

Official Transcript of Proceedings ACRST-3329

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control
Systems Subcommittee

Docket Number: (not applicable)

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005

SISP - REVIEW COMPLETE

Location: Rockville, Maryland

Date: Thursday, October 20, 2005

Work Order No.: NRC-663

Pages 1-191

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

**ACRS OFFICE COPY
RETAIN FOR THE LIFE OF THE COMMITTEE**

TR04

DISCLAIMER

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

October 20, 2005

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on October 20, 2005, as reported herein, is a record of the discussions recorded at the meeting held on the above date.

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

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

+ + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS
SUBCOMMITTEE MEETING

+ + + + +

THURSDAY, OCTOBER 20, 2005

+ + + + +

OPEN SESSION

+ + + + +

The Committee met in Room T2 B3 of the Nuclear
Regulatory Commission headquarters, Two White Flint
North, Rockville, MD, at 1:30 p.m., George
Apostolakis, Chair, presiding.

PRESENT:

GEORGE E. APOSTOLAKIS ACRS Member

MARIO V. BONACA ACRS Member

THOMAS S. KRESS ACRS Member

JOHN D. SIEBER ACRS Member

SERGIO B. GUARRO ACRS Consultant

ERIC A. THORNSBURY ACRS Staff

1 STAFF PRESENT:

2	CHRISTINA ANTONESCU	RES/DET/ERAB
3	STEVEN ARNDT	RES/DET/ERAB
4	FRED BURROWS	NMSS/FCSS/TSG
5	MATT CHIRAMAL	NRR/DE/EEIB
6	CLIFF DOVTT	NRR/DSSA/SPSB
7	MICHELE EVANS	RES/DET/ERAB
8	HOSSEN HAMZEHEE	RES/DRAA
9	ALLEN HOWE	NRR/DE/EEIB
10	WILLIAM E. KEMPER	RES/DET/ERAB/IVC
11	T. KOSHY	EEIB/NRR
12	ERIC LEE	NSIR/DNS/RSS
13	PAUL LOESER	RES/DET/ERAB
14	SCOTT MORRIS	NSIR/DNS/RSS
15	PAUL REBSTOCK	NRC/NRR/DE/EEIB-I&C
16	ROMAN SHAFFER	RES/DET/ERAB
17	GEORGE TARTAL	RES/DET/ERAB
18	MICHAEL WATERMAN	RES/DET/ERAB

19 ALSO PRESENT:

20	DAVID BLANCHARD	AREI
21	ROBERT CONTRATTO	Consultant
22	PAUL EWING	ORNL
23	TONY HARRIS	NEI
24	WES ITINES	Univ. TN
25	ROGER KISHER	ORNL

1 ALSO PRESENT: (CONT.)

2 KOFI KORSAH ORNL

3 GLENN LANG Consultant

4 JERRY MAUCK FANP

5 PETE MORRIS Westinghouse

6 BRUCE MROWOS ISC

7 THUY NGUYEN EPRI

8 DAVID SHARP Westinghouse/Consultant

9 NORMAN STRINGFELLOW Southern Nuclear

10 RAY TOROK EPRI

11 RICHARD WOOD ORNL

12

13

14

15

16

17

18

19

20

21

22

23

24

25

A-G-E-N-D-A

Opening Remarks	5
EPRI Guidance for Performing Defense in Depth and	
Diversity Assessment for Digital Upgrades: . . .	6
System Aspects of Digital Technology Overview .	124
Environmental Stressors	155

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

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

1:34 p.m.

CHAIRMAN APOSTOLAKIS: The meeting of the Advisory Committee on Reactor Safeguard Subcommittee on Digital Instrumentation and Control System.

I'm George Apostolakis, Chairman of the Subcommittee.

Members in attendance are Mario Bonaca, Jack Sieber and Tom Kress. Also in attendance is one of consultants Dr. Sergio Guarro.

The purpose of this meeting is to discuss three sections of the NRC Staff's draft digital systems research plan and to hear a presentation from EPRI on their guidance for performing defense-in-depth and diversity assessments for digital upgrades.

During this portion of the meeting we will hear from EPRI regarding their guidance document and from the NRC staff regarding Section 3.1 of the Digital Systems Research Plan, the system aspects of digital technology.

The Subcommittee will gather information, analyze relevant issues and facts and formulate proposed positions and actions as appropriate for deliberation by the full Committee. Eric Thornsby is the designated federal official for this meeting.

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 The rules for participation in today's
2 meeting have been announced as part of the notice of
3 this meeting previously published in the *Federal*
4 *Register* on September 29, 2005.

5 A transcript of the meeting is being kept
6 and will be made available as stated in the *Federal*
7 *Register* notice.

8 It is requested that speakers first
9 identify themselves and speak with sufficient clarity
10 and volume so that they can be readily heard.

11 We have received no written comments or
12 requests for time to make oral statements from members
13 of the public regarding today's meeting. We now
14 proceed with the meeting and I call upon Mr. A. Torok
15 of EPRI to begin the presentation.

16 MR. TOROK: I'm Ray Torok from EPRI. And
17 has already been said, we're here to talk about an
18 EPRI project that we call Defense-in Depth and
19 Diversity Assessments to Digital Upgrades. I guess i
20 can skip ahead.

21 And what I'd like to do before going
22 anywhere is introduce the Chairman of our Industry
23 Working Group who has guided this effort to talk about
24 the first few slides.

25 We're going to do sort of a tag team

NEAL R. GROSS

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

1 presentation. Our intent is to do a tag team
2 presentation to go through various areas of it, and we
3 were going to lead off with our Utility Chairman of
4 our Industry Working Group, that's Jack Stringfellow
5 from Southern Nuclear.

6 Jack, please.

7 CHAIRMAN APOSTOLAKIS: It's better to sit
8 there.

9 You don't have to leave. Stay there.
10 There are two chairs, aren't there?

11 MR. TOROK: Okay. I got your back, Jack.

12 MR. STRINGFELLOW: All right, Ray. Thank
13 you very much.

14 As Ray said, I'm Jack Stringfellow. I'm an
15 employee of Southern Nuclear Operating Company. It's
16 licensing manager for the Vogtle Electric Generating
17 Plant. I'm also the Chairman of this EPRI working
18 group that's been tasked to apply risk insights to the
19 process of performing a diversity and defense-in-depth
20 analysis for digital upgrades for nuclear power
21 plants.

22 And the first thing I want to say is
23 express our appreciation for the opportunity to make
24 this presentation. Thank you very much. We feel very
25 strongly about this program and we feel like we have

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 something that is worth considering and can certainly
2 enhance the process of performing a decubed analysis.

3 We want to talk for just a few moments in
4 our presentation, to being with, just to provide a
5 little background for the project, why we thought this
6 was a good thing to do, the impetus for this effort.
7 And how it relates to the current regulatory guidance
8 and make some key propositions with respect to how we
9 would envision moving forward with this effort. We're
10 going to give you a high level view of the guideline
11 approach. And then we want to spend most of our time
12 discussing the technical issues; the digital common
13 cause failure. We want to talk about susceptibility
14 to common cause failure. We want to talk bout
15 defensive measures. We want to address the issue of
16 estimating the probability of failure as well. And we
17 want to talk about what our risk insights have been as
18 a result of making this effort; what we found with
19 respect to the impact of diversity on safety and risk
20 and also conclusions that we've been able to come to
21 with respect to modeling digital equipment and PRA.

22 Then we'd like to offer some
23 recommendations for the ongoing activities of Research
24 and NRR, if we may be so bold as to do that.

25 You've already heard from Ray Torok. Oh,

NEAL R. GROSS

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

1 thank you, Ray.

2 MR. TOROK: I'm here to help.

3 MR. STRINGFELLOW: Thank you. What do you
4 do just hit the button to advance that?

5 MR. TOROK: Yes.

6 MR. STRINGFELLOW: Or the space bar?

7 CHAIRMAN APOSTOLAKIS: This is advanced
8 technology. Advanced digital.

9 MR. STRINGFELLOW: I just want to make
10 sure I don't screw up. Thank you.

11 CHAIRMAN APOSTOLAKIS: We have a project
12 involving human error also.

13 MEMBER SIEBER: You hit the wrong button
14 you trip the reactor.

15 MR. STRINGFELLOW: There you go. There you
16 go. So that tells me to keep my hands off, huh? All
17 right.

18 Our other presented will be Thuy Nguyen,
19 who is on loan to EPRI. And also Dave Blanchard,
20 Applied Reliability.

21 Our group represents ten utilities. We
22 have design experience, PRA experience and licensing
23 experience on the group. We also represent four
24 equipment suppliers as well as consultants and
25 integrators in NEI and EPRI. So we're a diverse group

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 and I think we've been able to bring a great deal of
2 varied experience to this effort.

3 We started our work back in early 2002.
4 And we have invited the NRC Staff to attend working
5 group meetings, and they have both in 2002, 2003 and
6 2004 in an effort to keep the NRC apprised of what we
7 were doing and the direction that we're headed in.

8 CHAIRMAN APOSTOLAKIS: But they were not
9 allowed to speak?

10 MR. STRINGFELLOW: Well, they were there
11 on their term. What am I trying to say?

12 MR. TOROK: Yes. I guess they weren't
13 there--

14 CHAIRMAN APOSTOLAKIS: Speak to the
15 microphone, please.

16 MR. TOROK: I'm sorry. They could probably
17 explain it better than I. My understanding --

18 CHAIRMAN APOSTOLAKIS: No, you explain.

19 MR. TOROK: My understanding was, yes,
20 they were not I guess free to offer NRC positions,
21 although to offer their opinions was fine. And because
22 they were EPRI working group meetings and not noticed
23 NRC meetings.

24 CHAIRMAN APOSTOLAKIS: So basically they
25 were observers?

NEAL R. GROSS

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

1 MR. STRINGFELLOW: That's correct, they
2 were observers.

3 MR. TOROK: That's right.

4 MR. STRINGFELLOW: That's correct.

5 CHAIRMAN APOSTOLAKIS: Okay.

6 MR. STRINGFELLOW: But we wanted them to
7 be able to be aware of what we were trying to do.

8 CHAIRMAN APOSTOLAKIS: Absolutely.

9 MR. STRINGFELLOW: Okay. We published a
10 final product in December of 2004, and that was
11 submitted to the NRC on February 22 of 2005 asking for
12 -- yes, I got my own copy, too.

13 And then we met with the Staff on April of
14 2005 to discuss status of the review and also to get
15 first impressions from the Staff with respect to the
16 document.

17 This last bullet says we are still
18 awaiting an NRC letter on a path forward. We did
19 receive some comments. Tony Pietrangelo received some
20 comments from Herb Berkow on October 18th. Due to
21 these late breaking comments, we haven't had a chance
22 to sit down and look at them in detail. So we're
23 really not prepared to talk about these comments line-
24 by-line today, but we appreciate the comments. And we
25 hope to use them as a basis for constructive dialogue

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 and moving forward with the review of this document.
2 So thank you very much.

3 CHAIRMAN APOSTOLAKIS: What is it that you
4 want the NRC to do?

5 MR. STRINGFELLOW: Well, what we
6 envisioned is we have a similar document, our
7 guidelines for licensing digital upgrades that we went
8 back -- when was it first published, Ray?

9 MR. TOROK: This goes back to 1993,
10 actually the first version of this.

11 MR. STRINGFELLOW: Yes.

12 MR. TOROK: And what we wanted to do was
13 establish a rough framework, basically, for licensing
14 digital upgrades that established a common
15 understanding between the Staff and the utilities.
16 Then that was revised more recently in a revision that
17 was published just a few years ago. We hope to do the
18 same --

19 MR. STRINGFELLOW: Excuse me, Ray, for
20 interrupting. But it was revised to update it to
21 reflect the rule change on 10 CFR 50.59.

22 MR. TOROK: Exactly.

23 MR. STRINGFELLOW: Okay. So we set about
24 to revise it for that purpose. And we submitted that
25 to the Staff for review, and it was subsequently

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 endorsed by regulatory information summary, a RIS.
2 And we would hope to be able to accomplish the same
3 thing with this guideline.

4 CHAIRMAN APOSTOLAKIS: Do you usually
5 incorporate documents like this one in a regulatory
6 guide?

7 MR. KEMPER: You mean EPRI's?

8 CHAIRMAN APOSTOLAKIS: Yes. Let's say that
9 you want to approve it?

10 MR. KEMPER: Exactly. Right. We would --

11 CHAIRMAN APOSTOLAKIS: You don't just say
12 we approve. I mean there is a regulatory guide --

13 MR. KEMPER: Well, there's a couple of
14 paths we could take. One is a safety evaluation report
15 could be written. That's been done in many cases in
16 the past.

17 CHAIRMAN APOSTOLAKIS: Sure.

18 MR. KEMPER: Or we could possibly endorse
19 this as a regulatory guide on this topic.

20 CHAIRMAN APOSTOLAKIS: Okay. But it has
21 to be a regulatory guide at the end?

22 MR. KEMPER: Well, no. Actually an SER
23 works sufficiently as well. Licensees can refer to
24 that.

25 CHAIRMAN APOSTOLAKIS: I thought you could

1 just say the SER, this is good enough and --

2 MR. KEMPER: Right. Correct.

3 MR. TOROK: And may I add to that? There
4 was a similar guideline we produced on evaluation of
5 commercial grade digital equipment for use in safety
6 related applications. And in that case NRC reviewed
7 and approved it and actually referenced it in the
8 standard review plan.

9 CHAIRMAN APOSTOLAKIS: Correct. Right.

10 MR. TOROK: So if you look at the standard
11 review plan now it refers you to the EPRI document.

12 CHAIRMAN APOSTOLAKIS: Bill, regardless of
13 whether you go the SER route or regulatory guide, will
14 you come to us before you issue whatever decision you
15 are --

16 MR. KEMPER: Oh, absolutely, yes. Well,
17 we have--

18 CHAIRMAN APOSTOLAKIS: -- SER and go more
19 deeply into the document itself.

20 MR. KEMPER: Well, as you know, we have a
21 risk program ourselves, right, which we presented back
22 in June to this Committee. So we're kind of trying to
23 accomplish the same thing in parallel here, if you
24 will; the agency as EPRI is. So at some point I
25 expect that we're going to probably converge, that's

NEAL R. GROSS

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

1 just Bill Kemper's idea or estimation of the work. So
2 hopefully the two programs will come together and we
3 will end up with one way to deal with a risk-informed
4 diversity and defense-in-depth process for licensing
5 digital.

6 CHAIRMAN APOSTOLAKIS: So you don't see
7 the Agency approving this before your particular
8 project is done?

9 MR. KEMPER: I can't speak directly for
10 NRR. But my thinking at this time is I would lobby
11 hard that we work together so that we come up with one
12 consistent approach on this.

13 CHAIRMAN APOSTOLAKIS: What are the plans?

14 MR. HOWE: Good afternoon. This is Allen
15 Howe. I'm with NRR.

16 And just to try to clarify this. If this
17 report is submitted to the NRC for review as a topical
18 report, we would treat it under our topical report
19 process. We would review it, we would write a safety
20 evaluation. Part of that process would be that the
21 applicant for the topical report would then supplement
22 their topical report with the safety evaluation to
23 designate that this has been reviewed and approved by
24 the NRC. Then licensees that came in with
25 applications could reference that topical report as a

NEAL R. GROSS

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

1 part of their application. So that's the topical
2 report process.

3 CHAIRMAN APOSTOLAKIS: And this is what's
4 happening now?

5 MR. HOWE: No. We have not accepted this
6 as a topical report for review?

7 CHAIRMAN APOSTOLAKIS: But EPRI is
8 requesting that you do that, is that what it is?

9 MR. HOWE: Yes.

10 CHAIRMAN APOSTOLAKIS: Okay. And you have
11 issued the SER or --

12 MR. HOWE: No. We have not issued an SER.
13 We have not even commenced a review on it. We have
14 been given a draft copy of the topical report. As was
15 indicated in one of the bullets, we provided some
16 comments back but the report has not been submitted
17 formally as a topical report.

18 CHAIRMAN APOSTOLAKIS: Okay. Thank you.

19 Oh, one last question. Can you explain a
20 little bit what you mean by expends NRC approach.

21 MR. TOROK: We'll get into that?

22 CHAIRMAN APOSTOLAKIS: What does that
23 mean? Oh, you will get into that?

24 MR. TOROK: Oh, yes.

25 MR. STRINGFELLOW: Yes. We're going to

NEAL R. GROSS

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

1 expand on that in the later slides here very shortly.
2 Very shortly.

3 CHAIRMAN APOSTOLAKIS: Okay.

4 MR. STRINGFELLOW: Okay. I guess there's
5 one thing, Ray, I would like to follow up on the
6 comment by Mr. Howe that we had not formally submitted
7 this for review. Because I believe we have.

8 CHAIRMAN APOSTOLAKIS: See, that's the
9 advantage of coming to the Advisory Committee to find
10 out.

11 MEMBER SIEBER: It's in the mail.

12 MR. HOWE: This is Allen Howe again.

13 Not to belabor the point, but we indicated
14 in a letter to you in March that we were considering
15 the subject topical report as a draft. And we had a
16 presubmittal meeting with you and we were waiting for
17 the formal submittal of your topical report.

18 MR. STRINGFELLOW: Did we identify this as
19 a draft. Okay.

20 CHAIRMAN APOSTOLAKIS: It may be a
21 formality anyway.

22 MR. STRINGFELLOW: Okay. All right. Fine.

23 CHAIRMAN APOSTOLAKIS: But ultimately, Mr.
24 Howe, you will come to this Committee after you have
25 your SER?

1 MR. HOWE: I'm sorry, I didn't hear the
2 question.

3 CHAIRMAN APOSTOLAKIS: After they submit
4 it formally, you issue an SER. And do you expect to
5 come before us for a letter?

6 MR. HOWE: We evaluate that on a case-by-
7 case basis. But I understand that your interest is in
8 hearing from the staff before we go forward with this.

9 CHAIRMAN APOSTOLAKIS: Yes. This is an
10 area where there is great interest on the part of the
11 Committee. I would appreciate it.

12 MR. HOWE: Okay.

13 CHAIRMAN APOSTOLAKIS: Okay.

14 MR. STRINGFELLOW: Okay. I want to spend
15 just a minute talking about regulatory environment and
16 why we think that this report can help. I think the
17 industry and the NRC have been struggling somewhat
18 with respect to digital upgrades. For example,
19 upgrades that involve rapid protection system and
20 engineered safety features actuation system.

21 We feel that it's been our experience that
22 the current guidance in the form of branch technical
23 position HICB-19 and NUREG/CR-6303 can be difficult to
24 implement. It is void of risk insights, certainly --

25 CHAIRMAN APOSTOLAKIS: Difficult to

NEAL R. GROSS

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

1 implement means it's vague or what? Why is it
2 difficult?

3 MR. STRINGFELLOW: Well, you know, one of
4 the examples there is with respect to large break
5 LOCA, for example. If you are postulating a digital
6 common cause failure and then trying to address the
7 large break LOCA in light of a digital common cause
8 failure given the guidance and the acceptance criteria
9 that are in HICB-19, it's difficult to address that
10 event, for example, without designing and adding onto
11 the system some sort of diverse actuation system for
12 example. And I guess we're going to get into that
13 later on and in a little more detail, I think. But I
14 think that would be an example.

15 Ray, can you --

16 MR. TOROK: Well, yes. Well, there's some
17 other things that requires revisiting FSAR analyses,
18 using different types of assumptions, best estimate
19 analysis that most utilities aren't used to because
20 they haven't done it that way before. And, in fact, it
21 appears that those analyses have very limited value as
22 well.

23 So, we'll get into some of these other
24 things in a few minutes. So you'll see --

25 MR. STRINGFELLOW: And that's where we

NEAL R. GROSS

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

1 came - I'm sorry I'm stepping on you, Ray. I
2 apologize.

3 MR. TOROK: No, no problem. We'll add a
4 lot of detail to that later I think.

5 MR. STRINGFELLOW: Right. You know, some
6 of the insights that we found is that revisiting many
7 of these Chapter 15 analyses provides a safety benefit
8 from a risk perspective. And so the deterministic
9 focus of the branch technical position I think is
10 where at least part of the difficulty arises in the
11 implementation.

12 And then we found that some things that
13 had been previously accepted in the past by the Staff
14 are now being questioned.

15 CHAIRMAN APOSTOLAKIS: Are you going to
16 come to this, too?

17 MR. TOROK: Some of that.

18 MR. STRINGFELLOW: Yes. We're going to
19 come to it.

20 MR. TOROK: Some of it, yes. And the idea
21 here really of what Jack's talking about now is to
22 make the point that there's a lot of problems with the
23 current process for doing this and we think there are
24 ways to improve them. And we think we should be doing
25 that.

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 MR. STRINGFELLOW: Yes. And don't take
2 this I'm not trying to throw rocks. I'm not trying to
3 throw rocks with this slide. What I'm trying to say
4 is we understand that the review of this systems is
5 evolving. And what we're trying to do with this
6 product is help that and help provide some stability
7 and provide those risk insights.

8 CHAIRMAN APOSTOLAKIS: Well, just that
9 bullet doesn't really read very well, "NRC Staff not
10 honoring SERs." Is it because the Staff is
11 capricious?

12 MR. TOROK: There's a specific example of
13 one review that's in progress now where the utility's
14 using a platform, a digital platform that had already
15 been reviewed and approved by NRC in the form of an
16 SER. And now the utility is receiving additional
17 questions on that. And, in fact, the Staff has taken
18 the position, as I understand it, that they may have
19 to go back and reopen that evaluation and start over
20 again. And, of course, that from the utility
21 standpoint, that has a tremendous impact on their
22 schedule for what they're planning to do. So for them
23 the process isn't working very well right now. So
24 that's the example there.

25 CHAIRMAN APOSTOLAKIS: There probably was

NEAL R. GROSS

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

1 a reason for it.

2 MR. TOROK: Yes. But, at any rate, the
3 problem from the utility perspective is it makes the
4 process unpredictable. And, of course, it makes it
5 difficult to them to estimate cost and schedule and
6 whatnot. So it puts them in a real rough position.

7 CHAIRMAN APOSTOLAKIS: Yes. And if it's an
8 issue of adequate protection, it makes the process
9 difficult from the Staff point of view?

10 MR. TOROK: That's right.

11 CHAIRMAN APOSTOLAKIS: Okay.

12 MR. STRINGFELLOW: And then finally, one
13 of the comments we got in our meeting in April on our
14 report that Research is doing some work with respect
15 to modeling digital systems in PRA and working on the
16 question of the failure probability of digital
17 systems. But, unfortunately, the timing of that
18 research doesn't support the near term submittals. And
19 so, again, that's another impetus for our work here.

20 Many utilities are in the process of
21 planning and trying to make digital upgrades today.
22 Many of us are operating our fleet on analog systems
23 that were designed and built many, many years ago.
24 Operating reliably and safely, I may add, but
25 nevertheless these systems are aging. And when we

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 look for replacements they are digital in nature. All
2 the way from things as simple as temperature
3 controllers on chilled water systems all the way up to
4 feedwater control systems and protection systems; the
5 replacements are digital in nature. And so we are
6 having to deal with these digital upgrades on a day-
7 to-day basis. And planning an across the board
8 protection system upgrade that takes a great deal of
9 resources and scheduling. So anything that we can do
10 to help move that process along we feel like in
11 everybody's best interests from both a reliability
12 standpoint and a safety standpoint.

13 The issue of software common mode failure
14 is still unsettled. You know, we recognize certainly
15 the need to ensure adequate coping capability or
16 diversity, but as I mentioned that the regulatory
17 issues and our experience has been protracted reviews.

18 As I mentioned before, we've found the
19 current NRC guidance to be problematic. I've already
20 mentioned that it can require backups that add
21 complexity and costs without necessarily improving
22 safety. It may not fully address events that are risk
23 significant, could actually discourage plant upgrades
24 that would enhance safety.

25 CHAIRMAN APOSTOLAKIS: Do you have an

NEAL R. GROSS

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

1 example of an event that may be risk significant in a
2 current review process?

3 MR. TOROK: Yes. We'll get to that in a
4 little.

5 I'm sorry.

6 MR. STRINGFELLOW: That's all. These are
7 the background slides. We're trying to set the stage
8 for this presentation.

9 CHAIRMAN APOSTOLAKIS: Yes. You are doing
10 that very well.

11 MR. TOROK: Work with us here.

12 CHAIRMAN APOSTOLAKIS: You've made a few
13 provocative statements that keeps us awake.

14 MR. STRINGFELLOW: We don't want you to go
15 asleep, okay?

16 CHAIRMAN APOSTOLAKIS: You are succeeding.

17 MR. STRINGFELLOW: Okay. All right. And
18 I've already mentioned that it can require analysis of
19 events that aren't safety significant from a risk
20 perspective.

21 Ray?

22 MR. TOROK: Yes. And we have examples of
23 those.

24 MR. STRINGFELLOW: We have examples of
25 those, too.

NEAL R. GROSS

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

1 CHAIRMAN APOSTOLAKIS: This is pretty
2 serious stuff there.

3 MR. TOROK: It's my turn, huh?

4 MR. STRINGFELLOW: It's your turn, Ray?
5 You want to sit here?

6 CHAIRMAN APOSTOLAKIS: Okay.

7 MR. TOROK: Okay. So we wanted to briefly
8 explain the current regulatory guidance that's out
9 there right now. Jack already mentioned BTP-19 which
10 is tied Chapter 7 of NUREG-0800, the standard review
11 plan. And that document references NUREG/CR-6303,
12 which is a contractor report developed by Lawrence
13 Livermore some years ago.

14 The vintage on these things, I believe
15 BTP-19 came out officially in 1994, but really the
16 work behind it dates back to the late '80s and early
17 '90s when it was put together primarily, I believe,
18 for the advanced reactor program to address diversity
19 and defense-in-depth there.

20 What it involves here is the idea is to
21 demonstrate that you have adequate coping capability
22 in the event of a common cause failure. I believe they
23 refer to it as software common mode failure. We're
24 quibbling over words here. We call it now digital
25 common cause failure or digital CCF; that's the

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 language here.

2 BTP-10 NUREG CR-6303 process involves 15
3 steps where you take your digital systems and break
4 them into blocks, identify blocks. And a block is,
5 let's see, the maximum size -- the maximum section of
6 the system for which a failure inside the system can't
7 propagate outside the block. That's the definition.

8 And then now you look for blocks that
9 contain common software and you postulate the
10 simultaneous failure of those blocks.

11 BTP-19 calls special attention to ESFAS
12 and reactor trip system for the purposes of D3
13 evaluations.

14 So having identified these blocks that
15 have common software now you go to your FSAR events
16 and reanalyze them with the postulated software common
17 cause failure. And you best estimate assumptions,
18 that's a little different from an FSAR analysis. And
19 the acceptance criteria is based on radiation release
20 criteria from 10 CFR 100.

21 If the results of the analyses are
22 unacceptable, then you add diverse backups as needed
23 for particular events.

24 The issue here --

25 CHAIRMAN APOSTOLAKIS: Now wait.

1 MR. TOROK: I'm sorry.

2 CHAIRMAN APOSTOLAKIS: I don't understand
3 the best estimate business. What kinds of assumptions
4 are these? Are these assumptions regarding the plant
5 or assumptions or the behavior of the software?

6 MR. TOROK: Oh, no. The plant primarily I
7 believe. Yes, it's the plant. Because for example you
8 might use a best estimate decay heat model rather than
9 a conservative bounding decay heat model.

10 CHAIRMAN APOSTOLAKIS: I understand that.

11 MR. TOROK: That sort of thing.

12 CHAIRMAN APOSTOLAKIS: As long as you
13 don't make best estimate assumptions regarding the
14 behavior of the software.

15 MR. TOROK: Right.

16 CHAIRMAN APOSTOLAKIS: Because I don't
17 think there are any.

18 MR. TOROK: That's a difficult part of the
19 problem.

20 CHAIRMAN APOSTOLAKIS: Yes.

21 MR. TOROK: Yes. Well, in this case the
22 assumption you make regarding the software is that it
23 fails, that the probability of failure is one.

24 CHAIRMAN APOSTOLAKIS: Complete failure?

25 MR. TOROK: Yes. Well, or failure enough

NEAL R. GROSS

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

1 that it defeats the safety function that you care
2 about.

3 Now, this approach is deterministic --

4 CHAIRMAN APOSTOLAKIS: Now this failure,
5 again, this digital system does what? Just actuates
6 the safety --

7 MR. TOROK: It could trip the reactor, for
8 example.

9 CHAIRMAN APOSTOLAKIS: So actuates trip?

10 MR. TOROK: It could actuate trip, that
11 would be one thing. Actuates an emergency system, for
12 example a core spray system or aux feedwater on a PWR.

13 CHAIRMAN APOSTOLAKIS: But it doesn't do
14 anything after that? It doesn't control it in anyway?

15 MR. TOROK: Let's see, are there cases
16 where CCF systems control? Most of them are simply
17 turn it on. And, yes, I think there are a few examples
18 of control

19 MR. KEMPER: Yes. For example, engineered
20 safety features that actuates pumps, it repositions
21 valves, it control the flow of --

22 CHAIRMAN APOSTOLAKIS: It does control the
23 flow.

24 MR. KEMPER: Oh, yes. High pressure safety
25 and low pressure safety injection flows to reactor

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 coolant systems, that sort of thing. I mean, although
2 it's not modulating flow, but it sets the flow at a
3 certain predesign design basis value.

4 MR. STRINGFELLOW: It basically starts
5 pumps and open valves. It repositions valves as
6 necessary to establish flow paths. Operators are then
7 stepping through their emergency procedures and once
8 they reach a point where they can reset SI, for
9 example, they manually reset SI, they manually stop
10 pumps that sort of thing. Once everything fires off
11 automatically and the necessary pumps are running,
12 then the operators have to step in and take control.

13 CHAIRMAN APOSTOLAKIS: So the system is
14 out of the picture?

15 MR. STRINGFELLOW: The actuation system
16 is.

17 MR. TOROK: So for the most part it's just
18 switching logic. It's not like feedback control as you
19 would have in the feedwater system, for example.

20 CHAIRMAN APOSTOLAKIS: I thought it did
21 more than just actuate systems.

22 MR. WATERMAN: This is Mike Waterman.

23 With regard to reactor trip and ESFAS
24 that's, like Ray said, trips a relay and then the
25 safety has to go to completion. If you're tripping

NEAL R. GROSS

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

1 the reactor, it cuts the MCCs to the control rods, the
2 control rods drop into the core. It doesn't do
3 anything to stop that. If it's ESFAS, it turns on
4 HPI, LPI and all that and then it's up to the operator
5 to control and modulate that. There's nothing in
6 ESFAS that's going to modulate anything. It actuates
7 systems, they turn on, spray turns on, containments
8 isolate, ECCS gets going and things like that. And
9 those things have to go to completion per regulation.

10 MR. KEMPER: However, there are
11 computations as well. Like for example in the reactor
12 protection systems there's variable pressure
13 temperature, trip set points that are calculated by
14 this platform. There's flux flow, delta flow trips.
15 So there's some sophisticated --

16 MR. WATERMAN: Up to the point of trip and
17 then once the trip occurs, it really doesn't matter
18 what the system does --

19 MR. KEMPER: Right.

20 MR. WATERMAN: -- because the safety
21 function itself goes to completion.

22 CHAIRMAN APOSTOLAKIS: Right. So it does
23 a monitoring job and then --

24 MR. WATERMAN: Yes, it continuously tries
25 to trip the reactor and if everything is okay, it

NEAL R. GROSS

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

1 fails to trip the reactor. But once it trips the
2 reactor, it may continue to calculate but it has no
3 effect on your safety system because they've tripped.
4 They've gone off and done their thing. And
5 essentially your reactor trip system is disconnected.

6 MR. TOROK: So it's primarily monitoring
7 and reacting to a trip signal at trip level. Yes. A
8 preset level.

9 Anyway, now let's get back to the BTP-19
10 approach. What have I done? Sorry.

11 Now we're down toward the bottom there,
12 approach characteristics. And we characterize this as
13 a deterministic approach with a focus on reactor
14 protection and ESFAS and the FSAR events. And the
15 reason we say it's deterministic is because we say
16 that it says focus on that system and go reanalyze
17 your FSAR events. Don't worry about which events are
18 more safety significant than others or anything like
19 that. And what that has the impact of doing is
20 distorting the safety significance of the software
21 because effectively you're saying the software
22 probability of failure is one and under that
23 assumption if there are results to these analyses that
24 are unacceptable, then you put in a diverse backup.
25 Ignoring the fact that in many situations there are

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 much more significant contributors to system failure
2 than the instrumentation control in the software. So
3 in that sense it distorts the safety significance of
4 the software.

5 Now I should say this all came about about
6 15 years ago. And, you know, then I'm thinking it
7 wasn't such a bad approach. But what it effectively
8 does is it says, look, I don't understand what's
9 inside that box with the software, so I'm not sure
10 what it might do. So I'll assume it fails. So that's
11 fine, you know, as long as you don't know what's
12 inside the box and you have to be sure that it doesn't
13 do something bad. But I would say that at this point
14 we know a lot more now about how to look at a digital
15 system and understand the design features in it to be
16 much more comfortable with what it might do and what
17 it might not do. And that's really what this approach
18 is about.

19 Now, we believe that a risk-informed
20 method offers very significant advantages. It keeps
21 the focus on safety, and you guys know more about this
22 than I do. The object is to show where the software
23 has risk significance and where it doesn't and worry
24 about defense-in-depth and diversity where, for
25 software anyway, it is significant.

NEAL R. GROSS

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

1 This allows consideration of design
2 features that are built into the digital system. And
3 there are characteristics that protect against failure
4 and against common cause failure. For example, self-
5 testing, data validation and fault tolerance.

6 And as an example here the deal with the
7 software, as you know, is it doesn't randomly, it
8 fails deterministically. And what typically gets
9 software into trouble is when it sees conditions that
10 the designer didn't anticipate and didn't test. So
11 it's a surprise kind of condition or unanticipated
12 condition.

13 There are ways to protect yourself against
14 that. One of them is data validation. If the sensor
15 data that the system is looking at goes out of range,
16 you flag it and you don't just use it blindly and do
17 stupid things. Now in that sense there's a big
18 difference between a high quality real time digital
19 system and a not so high quality real time system.
20 And we'll have a lot more discussion on that later.

21 Also under risk-informed method you can
22 consider the fact that when you add diverse backups,
23 you actually add additional failure modes, possibly
24 additional unanticipated behaviors. Certainly the
25 potential for spurious actuation. And these can all

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 be bad things.

2 And if you think about it, if you have a
3 system that is not very reliable to start with and you
4 add a diverse backup, you're probably improving the
5 overall reliability of the system. But if you have a
6 highly reliable system to start with and you add
7 backups, now you're not on such firm ground. You can
8 actually make it worse, and we think you ought to
9 worry about that in doing these things.

10 The risk-informed method is also
11 consistent with the latest trends in terms of
12 technical and regulatory efforts. And there I'm
13 referring to the NRC Management position that risk-
14 informed methods should be used or encouraged where
15 they make sense in more and more areas.

16 MEMBER BONACA: Before you proceed. Just
17 because I don't want to get confused. I understand
18 you're proposing a risk-informed approach. But now
19 the FSAR for these power plants would have the old
20 deterministic analysis, right?

21 MR. TOROK: Yes. Yes.

22 MEMBER BONACA: So now you're proposing to
23 use the new set points or whatever, how are you
24 proposing to use this digital --

25 MR. TOROK: Oh, I see what you mean. I'm

NEAL R. GROSS

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

1 not proposing to use new set points or anything like
2 that. We're proposing to use risk insights to help
3 determine where extra defense-in-depth is of value.

4 MEMBER BONACA: Yes. I understand that.

5 MR. TOROK: That sort of thing.

6 MEMBER BONACA: What I'm trying to
7 understand is that ultimately you have to have a
8 consistency between your accident or you haven't
9 changed yet, I mean whether you believe or not that
10 this addressing risk or just the traditional safety
11 and this new digital system. You will have
12 consistency there?

13 MR. TOROK: Well, yes. I agree. And I
14 guess this is an area where I should say the PRA
15 approaches in general face the same issues, I think.
16 And I don't know that we want to get into it right
17 now, but there is a confirmatory review process. I'm
18 looking at Dave Blanchard because he's the expert on
19 this.

20 MEMBER BONACA: No. I'm trying to
21 understand what you end up with.

22 MR. STRINGFELLOW: Hang on. Let me try,
23 Ray.

24 MR. TOROK: Okay.

25 MR. STRINGFELLOW: Let me try. This is

NEAL R. GROSS

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

1 Jack Stringfellow again.

2 I may not fully understand your question,
3 but correct me if I go wrong here. We are not
4 proposing to change the Chapter 15 analysis. The
5 Chapter 15 analysis will continue to be met with the
6 design. We're not altering that.

7 What we're proposing here is the use of
8 risk insights with respect to the Chapter 15 analysis
9 to focus on those areas where diversity can be of the
10 most benefit from a risk perspective. So the Chapter
11 15 analysis will not be revised.

12 MEMBER BONACA: You wouldn't have a need
13 to do that? All right.

14 MR. STRINGFELLOW: That's right. Did that
15 answer your question?

16 MEMBER BONACA: Yes, I think it does. I
17 was just looking at the previous slide on page 8 --
18 it's 6 where you're talking about that current NRC
19 guidance is problematic and require backups that add
20 complexity and cost without improving safety. And I
21 got the impression when I was reading this that if you
22 used the current guidance, you would not be accepting
23 criteria. For example in LOCA, therefore you would
24 have to do something else that you don't think is
25 significant from a risk-informed --

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 MR. TOROK: Yes, the acceptance criteria
2 there. We're really focused on this one issue really
3 of digital common cause failure, which is considered
4 beyond design basis event.

5 MEMBER BONACA: Okay.

6 MR. TOROK: Right.

7 MEMBER BONACA: Okay. I think I
8 understand where you're going. Go ahead.

9 MR. TOROK: Thanks, Jack.

10 MEMBER BONACA: Again, I'll ask more
11 questions when you get there.

12 MR. TOROK: Okay. So let's get back.
13 We're right at the bottom of this thing now. So we
14 like the potential advantages of the risk-informed
15 methods, however there are some technical issues here
16 associated with this, and they're at the bottom there.
17 One is digital system failure probabilities, what do
18 you do with that. And the other is this issue of
19 modeling digital equipment in PRA. Everybody's two
20 favorite issues these days. And these are areas that
21 need to faced to be able to use risk insights.
22 They're also areas where at the present time there is
23 no consensus on the best way to handle these things,
24 right? We want to say that up front.

25 But keep in mind, however, in looking at

NEAL R. GROSS

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

1 this too that our goal here is not to establish
2 absolute knowledge of digital system failure
3 probabilities and not to establish absolute knowledge
4 of the best way to model digital equipment in PRA.
5 What we're trying to do is capture risk insights
6 associated with these things. For example, get a
7 handle on where does the diverse backup help, where is
8 it a bad idea; you know, those kinds of things. So
9 risk insights. And we'll probably say that over and
10 over again.

11 Let me give you an example. You were
12 asking about examples, so we're going to get that. So
13 the first one here is a large break LOCA. And this is
14 large break LOCA with a digital common cause failure
15 in the low pressure injection system. Under the
16 deterministic method, the BTP-19 when you redo the
17 analysis you find that this is a large break, there is
18 insufficient time for operator action to do something
19 now that he's lost low pressure injection. Now in
20 BTP-19 it says for this event it recommends crediting
21 leak detection as a backup.

22 CHAIRMAN APOSTOLAKIS: This is design
23 basis?

24 MR. TOROK: Yes, beyond design basis.

25 CHAIRMAN APOSTOLAKIS: So --

1 MR. STRINGFELLOW: The digital common
2 cause failure is beyond design basis?

3 MR. TOROK: Yes, right.

4 CHAIRMAN APOSTOLAKIS: So would the NRC
5 look at this?

6 MR. TOROK: Because of the issue of
7 software common cause failure. Now --

8 MR. STRINGFELLOW: This is what BTP-19
9 would have us do. It would have us postulate the
10 common cause failure and then look at the LBLOCA and
11 show how we can continue to meet the LBLOCA within the
12 acceptance of criteria of BTP-19, which is relaxed to
13 the current Chapter 15 acceptance criteria. But
14 nevertheless, that's what it would have us do.

15 CHAIRMAN APOSTOLAKIS: We're getting into
16 the severe accident --

17 MR. TOROK: No. What this goes back to is
18 that with traditional redundant trains of hardware as
19 a basis of your safety system, since the failures that
20 can disable the safety system are hardware based
21 failure, then you can say well the likelihood of
22 having all the trains fail at the same time due to a
23 common cause hardware failure is at sufficiently small
24 that we don't have to assume that and analyze that.
25 That's the way it's traditionally handled for

NEAL R. GROSS

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

1 hardware.

2 Then along comes software. We put software
3 based control system on each of the channels of the
4 safety system. And now we say well what if there's a
5 bug in the software that's going to prevent all of the
6 trains from acting together or all at the -- I'm
7 sorry. All of them acting correctly?

8 CHAIRMAN APOSTOLAKIS: So this is an
9 application of the single failure criterion for
10 digital systems?

11 MR. TOROK: It would be if common cause
12 failure were within the design basis, but --

13 CHAIRMAN APOSTOLAKIS: It is not.

14 MR. TOROK: Right, exactly. So the
15 position that was taken in BTP-19 was look, we
16 understand it is beyond design basis, however we still
17 think it's prudent to look at this and here are the
18 ground rules. And the ground rules are go reanalyze
19 the Chapter 15 events with best estimate assumptions
20 so there's a relaxation there. And then are acceptance
21 criteria based on radiation release. And that was sort
22 of the compromise that was struck for --

23 MEMBER BONACA: The basic thought I guess
24 behind this is that with digital system you may have
25 common cause failure more likely now that --

NEAL R. GROSS

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

1 MR. TOROK: Right.

2 MEMBER BONACA: Well, I'm trying to say
3 that's --

4 CHAIRMAN APOSTOLAKIS: First of all, we
5 don't know that the digital common cause failure is
6 more likely than not --

7 MEMBER BONACA: I'm not arguing that right
8 now. I'm only saying that --

9 CHAIRMAN APOSTOLAKIS: Yes, but I mean I'm
10 puzzled why in the case all of a sudden we're jumping
11 into severe accident.

12 MEMBER BONACA: Well, the question is the
13 point that he made is because of the way it was
14 designed it was presumed that there will be no common
15 cause. So that assumption was not made. Now I'm
16 trying to understand why there is an assumption that
17 common cause failure is more likely with digital
18 systems.

19 MR. TOROK: Well, here's the deal. When a
20 software system fails it's nearly always because
21 there's a design flawed and it manifests itself in the
22 form of a software bug, right, one way or another.

23 MEMBER BONACA: That's right.

24 MR. TOROK: And in that sense digital
25 systems operates with extremely high reliability; if

NEAL R. GROSS

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

1 one does it, the next one's going to do it probably.

2 MEMBER BONACA: Right.

3 MR. TOROK: And that's the assumption
4 that's built in there. And then there are further
5 assumptions. One is we don't know how to put a
6 failure probability on digital equipment and in
7 software, therefore let's conservatively use one and
8 assume that it does fail and then show that you can
9 deal with it.

10 CHAIRMAN APOSTOLAKIS: Is anybody from NRR
11 here who can shed some light on this?

12 MR. TOROK: That would help, wouldn't it?

13 MR. KEMPER: Yes. I'll get started and,
14 Matt, you can follow up if you like.

15 The Agency took a position on this, oh
16 gosh it's been what? '94/'92 time frame. They got,
17 I guess, the National Academy of Sciences to do some
18 work for them, to do some studies on this subject. And
19 made recommendations that we form a policy to address
20 this issue. A letter was prepared, SECY letter was
21 sent to the Commission. The Commission agreed that
22 since we can't determine the failure probability of
23 software, whether it's more or less likely to fail
24 than hardware, then we would treat it in the manner
25 that we do. That it's a realistic failure but it will

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 be design basis -- beyond design basis failure
2 scenario. And so that's what gave rise to BTP-19 and
3 then NUREG-6303 was further written to embellish the
4 specifics of how you actually do a D3 analysis.

5 MR. TOROK: Right. So that was the
6 position 15 years ago, roughly.

7 MR. KEMPER: Right. That's right.

8 MR. TOROK: Okay. And effectively we're
9 saying well now we can do better than that.

10 MR. WATERMAN: This is Mike Waterman on
11 Office or Research.

12 I went back to 1993 and started doing an
13 operator event report, Part 21 review of all the
14 digital safety system, Appendix B, according to Ray
15 highly reliable digital systems. And I found 24
16 separate incidents of common cause failure in highly
17 reliable safety systems. I don't think they're that
18 highly reliable when I can find that many over a 12
19 year period.

20 Secondly, credit for leak detection backup
21 for BTP-19 disallowed by NRC. If you read BTP-19
22 there was a for example in there. Leak detection for
23 the system 80 plus. System 80 plus had extensive use
24 of acoustic monitors for leakage detection. We had a
25 licensee come in and say well, leakage detection is

NEAL R. GROSS

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

1 highly reliable. In July and August that same
2 licensee was cited because their leakage detection
3 systems in two separate plants failed to detect a
4 gallon per minute over a one hour period.

5 Leakage backup is only allowed if you're
6 going to put in leakage detection equipment that's
7 reliable. So we've got digital systems that are
8 somehow, even though they're more simple than what's
9 coming down for Oconee, are failing. What's causing
10 the failures? All these things that make them highly
11 reliable; self-testing and data validation are two of
12 the things that cause those systems to fail.

13 So to say these are the things that make
14 these systems highly reliable when those are the
15 things that add complexity and cause them to fail is
16 really off the mark.

17 MR. TOROK: Well, you're getting way ahead
18 of our talk here.

19 MR. WATERMAN: Okay. I just want to
20 clarify the credit for leak detection backup
21 disallowed by NRC, highly reliable digital systems is
22 just not really what I've seen.

23 MR. TOROK: Okay. Shall I continue.

24 MR. WATERMAN: Okay. Continue to march.

25 MR. TOROK: I'm sorry. Okay. So large

NEAL R. GROSS

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

1 break LOCA here's an example, okay. With common cause
2 failure low pressure injection under the deterministic
3 method there's no time for operator action and you
4 can't credit leak detection for whatever, right, as
5 Mike explained. And therefore you need to diverse
6 actuation of low pressure injection and its supporting
7 systems.

8 Now, if you look at that from a risk
9 insight point of view you would say well, the
10 probability of the digital common cause failure is --
11 I don't know what it is perhaps, exactly. In fact, I
12 certainly don't know exactly what it is but I have
13 plenty of reason to believe it's much less than one.
14 So that's one factor.

15 Another is that the likelihood of the
16 large break LOCA itself is quite low. And when I look
17 at those two together I conclude that the overall
18 contribution to core damage frequency from the
19 combination is very low. Very small.

20 CHAIRMAN APOSTOLAKIS: Well, but you know
21 what you're doing here is you're going back to the
22 original assumption that digital CCF, we don't know
23 how likely they are so therefore we're going to be
24 conservative. And now essentially you're saying don't
25 be conservative. It's a low probability event. That's

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 really what you're saying. I mean, it's not this
2 concise.

3 MR. TOROK: Well, what I'm saying is I
4 don't know precisely what the number is, but I know
5 it's less than one. Let me pick a number and see what
6 ballpark I'm in in core damage frequency. Just get a
7 handle on where I am.

8 CHAIRMAN APOSTOLAKIS: Right.

9 MR. TOROK: I'm trying to capture a risk
10 insight here.

11 CHAIRMAN APOSTOLAKIS: Right.

12 MR. TOROK: So that's one thing. If I
13 look at it this way, my conclusion is this event is
14 not a large contributor to core damage frequency.

15 There's another important fact, though,
16 that comes out of the risk evaluation. And that's
17 that if you do add a diverse backup for the I&C in the
18 low pressure injection system, it turns out it
19 wouldn't reduce the core damage frequency because the
20 failure probability of that system is dominated by the
21 large rotating machinery, the big pumps and valves and
22 spinning things.

23 CHAIRMAN APOSTOLAKIS: What is their
24 common cause failure rate?

25 MR. TOROK: Off the top of my head, I

1 don't know.

2 MR. BLANCHARD: For a typical low pressure
3 injection --

4 CHAIRMAN APOSTOLAKIS: You have to come.

5 MR. BLANCHARD: My name is Dave Blanchard.

6 For a typical low pressure injection
7 system you would have a common cause factor on the
8 order of 10^{-3} to 10^{-4} per demand.

9 CHAIRMAN APOSTOLAKIS: And you're saying
10 that the digital system is better than that.

11 MR. BLANCHARD: On that order or better,
12 yes.

13 CHAIRMAN APOSTOLAKIS: And how do you know
14 that?

15 MR. BLANCHARD: We will be addressing that
16 in a few minutes.

17 MR. TOROK: Yes. We'll get there.

18 MR. BLANCHARD: Yes. Right. Thank you.

19 MR. TOROK: Okay.

20 CHAIRMAN APOSTOLAKIS: I don't know. I am
21 uncomfortable with this. I'm not sure you're using
22 any risk insights here. Am I the only one who feels
23 that way. You're just attacking the original
24 assumptions.

25 MR. TOROK: Well --

1 CHAIRMAN APOSTOLAKIS: The Staff say we
2 don't know the details, we'll have to assume one. Why
3 do you say no don't assume one? Is that risk
4 insights?

5 And also this being more useful after we
6 approve the rule 50.46(a) which allow you to do
7 certain things for break sizes greater than the
8 transition. And the other argument there, you know,
9 the first subbullet at the bottom, don't do anything
10 to this because something is riskier. Well, that's an
11 interesting thought, although in real life I mean we
12 do that all the time, I must admit.

13 MR. TOROK: Well, under these assumptions
14 the conclusion is that the BTP-19 method drives you at
15 hardware and increase the complexity but the safety
16 benefit is questionable at best. So is that good
17 engineering? That's the question. I'll leave that as
18 the question.

19 CHAIRMAN APOSTOLAKIS: Wait a minute. Now
20 there is always another hand, you know that. The
21 large break LOCA is supposed to be the limiting
22 accident.

23 MR. TOROK: Pardon me?

24 CHAIRMAN APOSTOLAKIS: The large break
25 LOCA is supposed to be the limiting accident. It's

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 supposed to protect us from all sorts of things that
2 we haven't even thought of. So just to say that it
3 has low probability of occurrence, ah, doesn't cut it.
4 Because you know it's the things unknown and knowns
5 that you're so conservative designing the thing using
6 large LOCA as a design basis accident that you are
7 covered, you know. So -- anyway we're getting into
8 territory now -- let's go on. Let's go on.

9 MR. TOROK: It's still, you know --

10 CHAIRMAN APOSTOLAKIS: I'm sorry, Jack?

11 MEMBER SIEBER: It's not clear to me how
12 not installing a diverse system has an impact on
13 overall system reliability. In other words if you
14 install a backup system, obviously you're going to
15 effect reliability as a positive way. And I think you
16 have to come up some real numbers to be able to
17 establish what that's worth.

18 CHAIRMAN APOSTOLAKIS: Is argument is
19 though that, yes, you are reducing risk but I mean the
20 rotating components are still the same and they have
21 a higher probability of failure, right? That's what
22 you mean by backup? It's a backup to the I&C.

23 MR. TOROK: Backup to the I&C only.

24 CHAIRMAN APOSTOLAKIS: Not to the system
25 itself?

1 MR. TOROK: That's right.

2 CHAIRMAN APOSTOLAKIS: So the system
3 failure probability is dominated by the failure of the
4 pumps?

5 MEMBER SIEBER: That's true.

6 CHAIRMAN APOSTOLAKIS: So by adding the
7 backup system you reduce something else, but this
8 probability is still high. That's their argument.

9 MR. TOROK: Yes.

10 MEMBER SIEBER: So don't bother. You
11 could eliminate half the stuff in the plant.

12 CHAIRMAN APOSTOLAKIS: That's the point.
13 That was my point earlier that you know just because
14 something dominates it, don't eliminate everything
15 else.

16 MR. STRINGFELLOW: If I might, this is
17 Jack Stringfellow again. If I might offer up a little
18 anecdote with respect to the comment that Mr. Sieber
19 made.

20 Vogtle recently replaced or we have been
21 in the process of replacing our diesel sequencers with
22 a digital system. And we did a decubed analysis for
23 this system and we identified as a result of the
24 decubed analysis, we added some hardware. Some
25 electronics to some analog hardware to mitigate a

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 potential common cause failure of the system to fail
2 shed load. We installed the first train of that
3 system. And during testing that device actually
4 underwent an infant mortality. There was a compositor
5 in that device that had an infant mortality. It
6 failed and actually caused a failure to shed load
7 during the test.

8 So, you know, to my mind that's an example
9 of where we added hardware that actually caused a
10 failure due to a random failure of a compositor.

11 MEMBER SIEBER: Well, since we're telling
12 war stories, I used to be site Vice President of
13 Beaver Valley. And we installed digital sequencers on
14 our diesels and when we went through all the post-
15 modification testing and everything and everything was
16 fine. When we tested them after 18 months both diesels
17 failed to sequence. And the reason was that it was
18 unable to sufficiently reject surges on the DC power
19 system to the extent that it reset the microprocessors
20 to zero and destroyed the timing in there. And it
21 would count out. I mean, it was difficult to
22 troubleshoot that.

23 So I believe that there are situations
24 that can occur in power plant on simple digital
25 systems that give you common cause failures. And,

NEAL R. GROSS

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

1 frankly, when both diesels failed to start and load,
2 that got me upset. It cost \$80,000 in enforcement
3 action.

4 MR. TOROK: Right. Okay. Yes, which is
5 an interesting example and we should talk about that
6 and maybe the software complications there, if there
7 are any. But okay, let's go on.

8 Now we have another example. In this case
9 we're not talking about a pipe break or an FSAR event,
10 we're talking about risk significant events that are
11 modeled in the PRA but not in the FSAR necessarily.
12 Now this is -- you don't need to read all the small
13 print here. This is an event --

14 CHAIRMAN APOSTOLAKIS: This is a large
15 LOCA tree -- oh, transient.

16 MR. TOROK: Yes, it's an event tree.

17 CHAIRMAN APOSTOLAKIS: No, but what's the
18 initiating. Yes, I know the shape I've seen before.

19 MR. BLANCHARD: This is a loss of
20 feedwater event tree for PWR.

21 CHAIRMAN APOSTOLAKIS: So it's really a
22 transient.

23 MR. BLANCHARD: Yes, it's a transient
24 event tree.

25 MR. TOROK: So it's a high frequency

NEAL R. GROSS

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

1 initiator. And in this case the PRA looks at the
2 number of paths coming over here and through the
3 bottom and every which way, and many of them result in
4 core damage frequency over there.

5 CHAIRMAN APOSTOLAKIS: Right.

6 MR. TOROK: Now the FSAR -- the PRA
7 addresses all those paths. The FSAR addresses that one
8 and this one, the dash lines on there, right?

9 CHAIRMAN APOSTOLAKIS: The design basis
10 accident you mean?

11 MR. TOROK: Yes.

12 CHAIRMAN APOSTOLAKIS: And so BTP-19 would
13 say look at that one and look at this one, don't worry
14 about all this stuff.

15 CHAIRMAN APOSTOLAKIS: Yes.

16 MR. TOROK: Well it turns out some of
17 these are significant contributors to core damage
18 frequency. And that's because the PRA routinely
19 considers beyond design basis events that are risk
20 significant.

21 CHAIRMAN APOSTOLAKIS: Now I'm confused.
22 I mean, the previous slide said the NRC Staff went
23 beyond design basis in BTP-19 and now you're saying
24 here no, no, no that was really bad. I mean, they're
25 staying within the design basis. Which one is true?

NEAL R. GROSS

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

1 Or is it again whatever --

2 MR. TOROK: No, no, no. In either case
3 the event is considered -- the common cause failure
4 event is considered beyond design basis. In the
5 previous example it's an example of where the BTP-19
6 method would cause you to put in a diverse backup and
7 that apparently -- or that seems to have little or no
8 safety benefit. In this case the BTP-19 approach
9 ignores some potentially safety significant sequences
10 that probably should be considered. So in a sense --
11 and this in one both ends.

12 CHAIRMAN APOSTOLAKIS: Wait. Wait. Wait.
13 What does it mean it missed the safety significance.
14 I mean, safety significance is a relative term.

15 MR. TOROK: Yes.

16 CHAIRMAN APOSTOLAKIS: So you're saying
17 that there are some beyond design basis sequences that
18 dominate core damage frequency.

19 MR. TOROK: Yes.

20 CHAIRMAN APOSTOLAKIS: But core damage
21 frequency is acceptable in this plan.

22 MR. TOROK: But if I add common cause --

23 CHAIRMAN APOSTOLAKIS: And there is always
24 something that dominates.

25 MR. TOROK: Please, Dave.

1 MR. BLANCHARD: This is Dave Blanchard
2 again.

3 The branch technical position reviews the
4 effects of common cause failure for design basis
5 events only. It does not consider the potential
6 introduction of common cause failure in beyond design
7 basis events that are evaluated in the accident
8 sequences of the PRA.

9 CHAIRMAN APOSTOLAKIS: That's correct.

10 MR. BLANCHARD: So we can actually
11 introduce a common cause failure from a digital system
12 that can increase the frequency of these accident
13 sequences and it will go unevaluated under branch
14 technical position 19. We won't know about it until
15 someday we update the PRA.

16 CHAIRMAN APOSTOLAKIS: But when you
17 increase that frequency how many failures do you have
18 to assume exists after the initiating events? Because
19 if you have to assume more than one, you are beyond
20 design basis.

21 MR. BLANCHARD: Oh, no question. You are
22 beyond design basis.

23 CHAIRMAN APOSTOLAKIS: So you are
24 increasing the core damage frequency but we don't
25 regulate on the basis of the core damage frequency.

NEAL R. GROSS

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

1 MR. BLANCHARD: What we're proposing here
2 with this guideline is that a risk informed method to
3 review --

4 CHAIRMAN APOSTOLAKIS: Ah, is more
5 coherent, is more production?

6 MR. BLANCHARD: Yes. Yes.

7 CHAIRMAN APOSTOLAKIS: That's different.

8 MEMBER SIEBER: You don't agree with that?

9 CHAIRMAN APOSTOLAKIS: Nobody disagrees
10 with that.

11 MR. TOROK: Okay. We can go on then.
12 Okay.

13 So there's the two contrasting examples --

14 CHAIRMAN APOSTOLAKIS: But you know -- go
15 back. Beyond design basis events are considered in
16 the PRA and they are unevaluated using BTP-19. They
17 unevaluated using the totality of the regulations.

18 MEMBER BONACA: That's the point I was
19 trying to make before.

20 CHAIRMAN APOSTOLAKIS: Yes.

21 MEMBER BONACA: Okay. We are killing--

22 CHAIRMAN APOSTOLAKIS: We are killing BTP-
23 19 as if it were --

24 MEMBER BONACA: We're beating the same
25 dead horse. And the point is -- but that's the basis

NEAL R. GROSS

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

1 of the licenses that the plants you're addressing
2 right now have. So that's the way it is.

3 CHAIRMAN APOSTOLAKIS: And that's why
4 we're moving to a risk-informed environment as fast as
5 we can. This argument we know.

6 MEMBER BONACA: Here more than anything
7 else I am trying to understand, you know, and you're
8 doing a good job of how you propose to intermingle
9 this --

10 CHAIRMAN APOSTOLAKIS: Yes.

11 MEMBER BONACA: -- deterministic and
12 probabilistic approach in a way that still preserves
13 the licensing basis of this plant because that's what
14 it is.

15 CHAIRMAN APOSTOLAKIS: Yes. I really --
16 oh, I'm sorry.

17 MEMBER BONACA: Yes. That's it.

18 CHAIRMAN APOSTOLAKIS: I'm really
19 interested in understanding better your three
20 methodologies.

21 MR. TOROK: Okay.

22 CHAIRMAN APOSTOLAKIS: Extended, standard
23 risk and simplified risk. That's where the action is.
24 We know this area.

25 MR. TOROK: Okay. Let's move on. We had

1 here some different views --

2 CHAIRMAN APOSTOLAKIS: No, I'm not telling
3 you to skip slides, I mean unless you want to. But
4 don't try to convince us that the risk-informed
5 approach is better than the --

6 MR. TOROK: Okay. Okay.

7 CHAIRMAN APOSTOLAKIS: All right. We're
8 with you on that.

9 MR. TOROK: Okay. Tell you what, I'll do
10 this quickly. We have a list here of ways of looking
11 at the digital reliability issues. The first two
12 questions here -- it's just interesting to look at
13 different ways to look at this.

14 How reliability is the software? That's
15 a question where we would say -- and it's probably
16 unfair to say focus here, maybe emphasis. But the NRC
17 research emphasis on establishing how reliable
18 software is whereas we're emphasizing how reliable
19 does it need to be. And this is a good example of
20 getting a handle on the second question can help you
21 figure out how far to go with the first question so
22 you don't spend a lot of money going way farther than
23 you really need to.

24 Now all the rest of the questions on that
25 page, which I don't know how to skip through quickly,

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 are kind of the same thing. It's the same thing over
2 and over again.

3 One thing that I should call attention to
4 that's a little different, though, is that Research,
5 or NRC let's say, emphasis has been on what process
6 attributes affect reliability. And a difference
7 between what they're pushing and what we're pushing is
8 we say what design attributes affect reliability. So
9 we want to look at the as-built device, not just the
10 process that built it. And we think it's more
11 important to look at the design attributes. And Thuy
12 is going to say a bunch more about that later.

13 I'm going to skip the rest of these and
14 you can read, I guess, at your --

15 CHAIRMAN APOSTOLAKIS: So do you really
16 want to send the message that you are disagreeing on
17 everything?

18 MR. TOROK: Well, no, no, no. That's not
19 the message at all.

20 CHAIRMAN APOSTOLAKIS: It's not the
21 message I'm getting --

22 MR. TOROK: The message is that there are
23 different ways to look at these things. And we said
24 "focus" here, and maybe that's too strong.

25 CHAIRMAN APOSTOLAKIS: Maybe you can

NEAL R. GROSS

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

1 remove RES and EPRI and say one approach is this, the
2 other approach is that. And we like the second one.

3 MR. TOROK: Well, some combination of them
4 is kind of nice.

5 MR. STRINGFELLOW: That's why we titled
6 the slide complimentary.

7 MR. TOROK: Yes. Right. We're saying --

8 MEMBER SIEBER: We're not fooled by that.

9 CHAIRMAN APOSTOLAKIS: You're saying that
10 you're interested in establishing reasonable assurance
11 and the Agency is not?

12 MR. TOROK: Well --

13 CHAIRMAN APOSTOLAKIS: This is our bread
14 and butter.

15 MR. TOROK: It's a difference in emphasis.
16 How do I prove my liability claims? That's a tougher
17 question than how do I establish reasonable assurance.

18 CHAIRMAN APOSTOLAKIS: I still think you
19 should change the headings.

20 MR. TOROK: Okay.

21 CHAIRMAN APOSTOLAKIS: And say there may
22 be two -- separate approaches and this is the one
23 we're talking about. Because every single one of
24 these can be challenged.

25 MR. TOROK: Okay.

NEAL R. GROSS

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

1 CHAIRMAN APOSTOLAKIS: There is no reason
2 to do that. I mean, you know that the Staff doesn't
3 do that.

4 Let's go on.

5 MEMBER SIEBER: Actually, you got to
6 answer all the questions if you look at them.

7 MR. TOROK: The main point was that the
8 right -- the two kind of help each other out if you
9 can fill in all the blanks; that's all.

10 Now --

11 MEMBER BONACA: Your question, the way you
12 pose it, how reliable does it need to be. It depends
13 on what criteria you're using. So you're saying well
14 I don't like the deterministic, I'm going
15 probabilistic and then this is that. I can understand
16 how you have to first of all establish a guideline on
17 a process which is acceptable enough to answer the
18 question; how reliable does it need to be? It depends
19 on what criteria you're using.

20 MR. TOROK: Well, and for example in that
21 one I would say I need to show that it's sufficiently
22 reliable, that it's not going to dominate the failure
23 probability in a system that it's in, right? Okay.
24 Now I can go to my PRA and in other words, probably I
25 can generate a number there. Now I go back to my

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 reliable is it and say hey, here's my target. You
2 know, my target's not 10^{-9} , it's just 10^{-3} . Right?
3 Makes a huge difference in what you would do to show
4 reliability.

5 MEMBER BONACA: I understand.

6 MR. TOROK: That's the whole point, right?

7 MEMBER BONACA: Understand.

8 MR. GUARRO: There are certain points one
9 could easily argue with. For example when you say
10 which failure facts are important to safety, I don't
11 think that can be contrasted with respect to the
12 previous question, which is I think what it's supposed
13 to contrast, which is how can digital systems fail.
14 If you do not know how they fail, it's pretty hard to
15 see what the effects are, right?

16 MR. TOROK: Yes. Right.

17 CHAIRMAN APOSTOLAKIS: I think that was
18 not the most successful slide.

19 MR. STRINGFELLOW: Well, we've had a
20 couple of those.

21 MR. TOROK: Yes, we have.

22 CHAIRMAN APOSTOLAKIS: Probably for other
23 audiences you didn't have the same problem you're
24 having today.

25 MR. TOROK: So you can be sure we won't

NEAL R. GROSS

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

1 use that slide again.

2 CHAIRMAN APOSTOLAKIS: That's called
3 learning from experience.

4 MEMBER SIEBER: Are we supposed to be
5 keeping track of slide quality?

6 MR. TOROK: I would call that --

7 CHAIRMAN APOSTOLAKIS: Okay. Let's move
8 on. I want to see the three methods.

9 MR. TOROK: Yes. I would characterize
10 that as an operating history failure, by the way.

11 Okay. Now here's the key points we're
12 trying to make it. You guys liked the first one, I
13 think. Use of risk insights helps us do a better job,
14 okay?

15 CHAIRMAN APOSTOLAKIS: Absolutely.

16 MR. TOROK: Great. That's one.

17 Okay. And we believe that it's possible
18 to derive useful risk insights for D3 evaluation, not
19 for general purpose PRA evaluation, but for D3
20 evaluations now. And we think that you can derive
21 those risk insights without precise knowledge of
22 failure probabilities and without detailed PRA
23 modeling of the digital I&C. And we'll talk about how
24 that works. Okay. And we say that for the purposes
25 of D3 evaluations, not general purpose PRA, we can get

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 a handle on the reliability of the digital equipment
2 based on deterministic evaluation of the equipment.
3 Deterministic evaluation, okay? And we're going to
4 talk more about that.

5 And we believe that the ongoing and future
6 work by NRC Research and others is just going to help
7 that. There's a framework here as methods to determine
8 software reliability become better and better, that's
9 great because they can be used within this framework.
10 Same thing for modeling digital systems in PRA.

11 Oh, that was fast.

12 CHAIRMAN APOSTOLAKIS: Now I want to take
13 a ten minute. Is this a good time?

14 MR. TOROK: Okay.

15 MEMBER SIEBER: Ten minutes.

16 CHAIRMAN APOSTOLAKIS: Yes, we're going to
17 have two breaks this afternoon, ten minutes each.
18 12½, Jack.

19 MEMBER SIEBER: That includes travel time.

20 CHAIRMAN APOSTOLAKIS: We'll 2:55 -- no.
21 Until 2:55.

22 (Whereupon, at 2:43 p.m. a recess until
23 2:56 p.m.)

24 CHAIRMAN APOSTOLAKIS: I can start without
25 some members, but not without the speakers.

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 MR. TOROK: Okay. Excellent.

2 Before we start, I have a request that we
3 heard from Mr. Waterman mentioned a number of software
4 common mode failure problems that he discovered.

5 CHAIRMAN APOSTOLAKIS: Yes.

6 MR. TOROK: We'd like to see a formal list
7 of those. That would be very helpful to us. You
8 know, we asked our group, but we don't have a good
9 knowledge of that. Thank you.

10 Now, here's the other thing. We know we
11 want to get through this as quickly as we can. We're
12 going to try and go through the general stuff.
13 Obviously, we're going to need some of your help on
14 that. And what we're really trying to get to is the
15 two technical issues that we have in one of the early
16 slides. All right. They are what we call defensive
17 measures and how we look at susceptibility for
18 software common cause failure and how we estimate
19 failure probability. That's one part. And the other
20 one is the modeling and PRA and the risk insights that
21 come out of that. So we have to get to those things.
22 Everything else builds up to that.

23 So, please, friend, let us get through the
24 next few slides pretty quickly.

25 Anyway, so you asked about guidelines

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 methods. There are three methods in the guide. I want
2 to describe them very briefly and at fairly high
3 level. That are papers that are published that we can
4 provide that give all the details of them. But I
5 think we can describe the methods fairly simply. And
6 since you guys are well versed on PRA, you'll
7 understand what we're talking about very quickly here.

8 Now the first one we call extended
9 deterministic method. And it basically is the BTP-19
10 approach, however for problematic events like large
11 break LOCA we would say take a risk-informed look at
12 it to see if that puts the event in a new focus.
13 That's basically what the method does, simple as that.

14 The second one we standard risk-informed.
15 That's where the idea is capture a risk focus with
16 realistic assumptions and what you're really trying to
17 do there is update your PRA to reflect the digital
18 equipment, which means you need to put in failure
19 probabilities and beta factors and so as it makes
20 sense, and then regenerate your results and look at
21 your core damage frequency. That's the basic idea.

22 And at some point if you're putting in
23 digital upgrades, regardless of the D3 issue, you'll
24 want the PRA model to be consistent with the plant and
25 you'll face this problem.

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 The last method is simplified risk-
2 informed. And this is where we take conservative
3 assumptions and use the PRA so you don't have to
4 update your PRA model to do this one. And what you
5 basically do is treat the software common cause
6 failure as a new failure mode and you say for each
7 event, you would say you have an event frequency from
8 the PRA model. And you multiple that by the failure
9 probability of the digital system or of the software.
10 And that gives you a delta core damage frequency for
11 that event. You do that over and over again to see
12 what the total change in core damage frequency is and
13 you also identify the large contributors to it, and
14 that tells you where to focus. That's what the
15 simplified risk-informed method is about.

16 Now for the risk-informed methods, the
17 acceptance guidance from Reg Guide 1174, which you're
18 all familiar with in looking at delta CDF and so on.

19 All three methods use what we call a
20 confirmatory defense-in-depth review which is where
21 you do a sanity check on your results to make sure you
22 didn't miss something important. And without getting
23 into the details, and then the idea there is if the
24 acceptance criteria aren't met, you've got some
25 options. You could refine the assumptions if you can

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 defend revisions to your assumptions or you could use
2 one of the other methods. Modify your design so that
3 the common cause failure issue goes away, you know it
4 doesn't exist anymore or add a backup function as you
5 would under BTP-19.

6 That in one page is what all our methods
7 do.

8 Now, regardless of which method you pick
9 the first thing you have to do is figure out where
10 you're susceptible to digital common cause failure.
11 And under BTP-19 we talked about this. You identify
12 blocks and if the blocks have the same software,
13 you're susceptible. We do something a little more
14 than that. We say well wait a second, that's not the
15 whole story. You can look inside those blocks and you
16 can identify design features and behaviors and whatnot
17 that are designed into the thing that help constrain
18 the failures that you have to worry about. And Thuy's
19 going to explain that in more detail momentarily.

20 There are a couple of things that I wanted
21 to mention here. One is that this is a deterministic
22 way to look at a digital device to understand what its
23 failure behaviors might be and how they might get you.
24 So it's deterministic in that respect. That's really
25 important.

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 Another is it gets beyond the process
2 based way of looking at software quality. A great
3 process does not guarantee a great product. It might
4 guarantee a well documented product. But what we
5 believe is more important for establishing reliability
6 and reasonable assurance that you have high
7 reliability, is that you want to make sure the right
8 defensive measures or the right design attributes are
9 built into the device. You want to understand the
10 final as-built device, and that's what this is about.

11 MEMBER SIEBER: How do you examine the
12 software to predict all the failure modes that might
13 occur.

14 MR. TOROK: We'll get to that in a minute.

15 And I said this already, the defensive
16 measures provides a deterministic basis for estimating
17 likelihoods of failure and digital common cause
18 failure. And we're going to talk about that.

19 Now still, we want to acknowledge again
20 that this is different from standard PRA treatment of
21 hardware because software fails deterministically in
22 the sense that when it sees the right set of
23 condition, it'll do the same thing every time, or
24 nearly every time. I guess Microsoft may not agree
25 with that statement. Anyway, but what you really have

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 to get a handle on here is the likelihood that the
2 system will encounter unanticipated conditions; that's
3 one thing. And the likelihood that those anticipated
4 conditions will get you into trouble in your plant
5 context.

6 To do this evaluation where you're looking
7 inside the box is not something that you can do using
8 a handbook of failure probabilities that might be
9 great for modeling pumps and valves and PRA. In this
10 case it requires specific expertise in software and
11 detailed knowledge how a digital device works.

12 And with that, I want to introduce Thuy
13 Nguyen who is our expert on this.

14 MR. NGUYEN: So good afternoon.

15 I'm a software expert, and my job is to
16 analyze -- one of my job is to analyze the software
17 systems at EDF that are safety critical for the EDF
18 plants.

19 So, in fact --

20 CHAIRMAN APOSTOLAKIS: So how come you're
21 here? Are you spending time at EPRI?

22 MR. NGUYEN: Yes. Because EDF and EPRI
23 have cooperation agreements. We would like to share
24 research effort.

25 CHAIRMAN APOSTOLAKIS: Okay.

NEAL R. GROSS

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

1 MR. NGUYEN: So I'm spending a few years
2 at EPRI in Palo Alto.

3 CHAIRMAN APOSTOLAKIS: A few years?

4 MR. NGUYEN: Yes. This is a certain
5 number of important projects where we prefer to have
6 a much tighter cooperation than just phone and email.

7 CHAIRMAN APOSTOLAKIS: The first ten years
8 are difficult ones.

9 MR. NGUYEN: In California it's fairly
10 easy.

11 So I will start by very obvious things
12 first and introduce my terms.

13 First, the notion of digital faults. A
14 digital fault is a software bug, mostly. And by
15 itself it does nothing.

16 A digital fault if it's not activated by
17 particular conditions in the digital system will
18 remain latent and have no effect.

19 And I think we have heard recently of a
20 software bug found at Palo Verde. This is typically
21 the case of a software bug that exist permanently in
22 the software but is activated only when a hardware
23 fault occurs, a particular hardware fault occurs. And
24 as long as this hardware fault doesn't occur, the
25 software fault is dormant.

NEAL R. GROSS

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

1 When there is an activating condition
2 occurs, then you can have a digital failure. If this
3 activating condition effects only one channel of a
4 redundant system, only this channel will fail. So a
5 digital fault does not mean that we had digital
6 failures. This fault in Palo Verde has not been
7 activated in operation.

8 Now a failure of a channel is not yet a
9 common cause failure. A common cause failure occurs
10 when the activating condition effects multiple
11 channels concurrently. And this is very important
12 because I would say the analysis approach that I will
13 be presenting in the following slides is based on
14 this, I would say, vision of how digital CCF only.

15 I have also a small remark saying that
16 there are some digital faults that are activated but
17 do not result in failures. And there are failures that
18 are not risk significant. So we here are focused on
19 risk significant failures.

20 So in order to explain how software
21 systems work and fail, I have taken the metaphor which
22 is a mine field metaphor. I have a very large mine
23 field that I spent a lot of effort to remove the
24 mines, but I'll never be able to say there are no
25 mines left. So if I walk in this mine field without

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 specific pattern or randomly, at every step I might
2 step on a mine.

3 Now, this is not the case of certain types
4 of systems. Certain types of systems in fact are
5 designed to function cyclically. They follow again and
6 again the same path. So if I think, I'm going back to
7 mine field, if I walk along this path of course the
8 first cycles I will be quite worried that I might step
9 on a mine. But after a certain number of iterations
10 provided that my path is not too wide, I will grow a
11 higher level of confidence that even though there
12 might be still some mines left in the mine field, they
13 will not on my path.

14 And what is important to understand is
15 what's the width of my path. If it's very large like
16 a highway, I will need quite a number of iterations
17 It's very narrow, after a certain number of iterations
18 I can say, yes, it's quite unlikely that if I stay on
19 this path, I will step on a mine.

20 And here we're dealing with software that
21 are designed to be what we call deterministic. Of
22 course, totally in theories all software is
23 deterministic. But what I call deterministic is when
24 we understand and know what are the influence factors
25 that will effect the software trajectory. And in this

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 case the software is under the influence of a certain
2 number of factors that will effect the width of its
3 path.

4 I have listed here in these bullets a
5 number of influence factors. For example, you have
6 the input variables coming from the process.

7 You have the memory that the software
8 system keeps from one cycle to the next.

9 You have blocking interrupts. You might
10 have process-related interrupts. And you have also
11 internal resource management like memory allocation
12 and so on.

13 In most of the -- in all of the systems
14 that I know there are certain number of measures that
15 have been taken to narrow the path of the cycle. For
16 example, all resource management is static. There is
17 no dynamic memory location, for example.

18 The process interrupts -- rated interrupts
19 are not allowed.

20 There are clock interrupts in certain
21 systems that occur every millisecond. And there are,
22 I would say in software terms, represented a small
23 amount of curve that can be verified very thoroughly.

24 Short-term memory is also kept to a
25 minimum. That usually represents only a few variables

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 that can be very formally identified.

2 The number of processing inputs come from
3 the process and they can be validated before used, and
4 we will see how we will deal with that.

5 So as long as things stay, I would say, in
6 the nominal conditions the system will ge on this
7 green path and typically a number of situation per
8 year in a single channel in about a billion.

9 So after a number of situations I think my
10 engineering judgment is that it's very unlikely that
11 it will fail in this condition.

12 Now, of course, my system must be able to
13 react to a number of, I would say, conditions
14 occurring so that it some use. So I have listed here
15 a number of what I have called infrequent influence
16 factors, influence factors that could take the
17 software system out of its green path on which I am so
18 comfortable.

19 For example, there is initialization. But
20 this executed only once.

21 The operator request. For example, every
22 month the operator changes some set points. This can
23 be done channel-by-channel so I do not say that
24 operator request cannot activate a software fault.
25 What I say that we can take measures in the operation

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 and the maintenance of the system so that this does
2 not effect concurrently all the channels of my
3 redundant system.

4 There are hardware failures like the Palo
5 Verde example. But the hardware failures usually
6 effect a single channel.

7 There are exceptions. For example loss of
8 power or the operator has pushed the reset button.
9 The reaction of a protection system to an exception
10 is usually to stop the processor. So it's a very,
11 very simple action.

12 There are particular date and times like
13 the Y2K date, for example. And the usual approach to
14 avoid these kind of parameters is to say we will not
15 manage dates and times in this kind of system

16 So what is left? Ah, the plant
17 transients. Because the plant transients effect
18 concurrently all the channels and these are, I would
19 say, the main events that could trigger potentially a
20 software common cause failure. And of course if that
21 appears and if it leads me to an unforeseen, untested
22 condition, then there is a possibility that I might
23 step on the mine and that my system fails all its
24 channels concurrently. So that is an important
25 element to take into consideration.

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 So now let's look at the internals of a
2 software system used for reactor protection. Usually
3 it's composed of an operating system and of
4 application software. The application software is
5 usually subdivided into two main parts: Standard
6 elementary functions and application specific
7 software. So the operating system and the standard
8 elementary function usually are bundled with the I&C
9 platform.

10 Now, an important design feature of I
11 would say a well designed operating systems for
12 applications is that the operating system is
13 independent from the application software and that it
14 is transparent to plant condition. The operating
15 system will read inputs and give them to the
16 application software. But whatever the values of the
17 input, it's not effected. The operating system does
18 not react to interrupts coming from the plant
19 processes. So it's in its own circular path. The
20 application software is in its own circular path.

21 Now, if I have a plant transient, since
22 the operating system is blind to the plant condition,
23 it will remain on its green path. Only the application
24 software will be taken out of its own green path and
25 follow a different execution path.

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 So what I'm saying here it is quite
2 important. It's that provided that my operating system
3 has the appropriate properties, and that's a very big
4 if that needs to be substantiated and proven by
5 appropriate argument and evidence, the operating
6 system will not fail or is very unlikely to fail
7 during plant transients. It will stay in its
8 repetitive path.

9 And that is, I would say, something that
10 is difficult to accept by most people. We have
11 talking in our work group since quite a long time, and
12 it took me quite a number of discussions just to feel
13 that.

14 The second part of the platform software
15 is the standard elementary functions. There I will
16 take another type of argument. These functions are
17 usually very small and/or assign a delay. They are
18 very small functions but usually independent from one
19 another. They have no internal memory. They're based
20 usually on very well mastered algorithms. You can
21 perform very, very thorough V&V. So on engineering
22 terms the digital faults in the functions of the
23 standard library are quite unlikely.

24 So this is the basis for my statement.
25 And, of course, again that will need to be supported

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 by a very argument and evidence.

2 So our last part that we have not
3 addressed in the previous slide is the application
4 specific software. And I have put here, I would say,
5 the two main sources of potential faults of the
6 application software. We have, of course, the software
7 implementation faults, but we have also the
8 specification faults. And in my experience it has
9 always been the specification that has been the
10 undoing the application software.

11 In the software implementation you can
12 take very, very strong measures to make sure that it's
13 reliable and as fault free as it can be.

14 I have signs from Ray to go faster, so I
15 will not go very deep here.

16 I will try to speak a little more on
17 specification faults. There are two main types of
18 specification faults. What I call the expression
19 faults in the functional specification and the fault
20 that results in an incorrect understanding of the
21 plant and its systems by the specifiers.

22 You can take means to avoid expression
23 faults. But the lack of understanding is quite
24 difficult to address and they are usually in my
25 experience all the faults that I've seen are faults of

1 these types.

2 And now if we look at the notion of common
3 cause failure. The main source of common cause
4 failures in a redundant system are here. And if I
5 make a redundant system based on four channels, each
6 channel using a different platform but implementing
7 the same application, I would still say that the beta
8 factor is wrong because of he --

9 CHAIRMAN APOSTOLAKIS: Software failure.

10 MEMBER SIEBER: Need we say more?

11 MR. NGUYEN: Okay. So that's again a
12 very, very strong claim. And I have insisted here
13 that it needs very good argument and evidence.

14 EDF will be building a new power plant in
15 the years to come based on the Framatome design. And
16 my team has been in charge to provide this type of
17 argument for the analysis for the -- and I had one
18 year or one year and a half to do that.

19 So now if we try to give some figures on
20 the probability of digital failure, I would say the
21 probability of digital failure resides mainly in the
22 evaluation of the likelihood of a fault in the
23 specification. And the lack of understanding are I
24 would say quite similar for digital or for analog
25 systems. So my point would be to say probability of

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 systematic failure of a digital system should be in
2 the same range as an analog system. After that, we
3 have the probability of failure due to hardware and I
4 think that there are appropriate methods to do that.

5 So, again, later one we will take beta
6 factors between digital systems. But the beta factors
7 have nothing to do with the I&C platform, again
8 provided the fact that the I&C platform has the
9 appropriate defensive measures.

10 MR. TOROK: Okay. You know, yesterday we
11 had this problem when the computer was unplugged. Do
12 we know that this is okay?

13 CHAIRMAN APOSTOLAKIS: It's working.

14 MR. TOROK: Well, the computer will go for
15 a while.

16 Okay. So our next guy Dave. Now we're
17 moving it to transitioning from defensive measures to
18 risk insights; how do we get from here to there,
19 right? And Dave Blanchard is our next speaker.

20 MR. BLANCHARD: My Dave Blanchard. I'm
21 from Applied Reliability Engineering. And I've been
22 working with Ray and the rest of the working group for
23 the last several years in developing the guideline.

24 Early in the presentation we saw our two
25 major questions were where do the numbers come from in

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 terms of digital common cause failures. But a second
2 question was how do we incorporate the effects of
3 digital common cause failures into risk assessment.
4 And what's my presentation will be on, using the
5 defensive measures approach that Thuy just introduced.
6 He has provided us with methods to show that the
7 potential for failure of a digital channel even is on
8 the same order of that as a similar analog channel.
9 And in addition to that his defensive measures
10 approach as outlined in the guideline allow us also to
11 take a look at the potential for common cause beta
12 factors between redundant channels of instrumentation
13 and control.

14 Now, where these redundant channels exists
15 has an effect on the probability of common cause
16 failure. Identical trains in the same system, as an
17 example, using the same inputs, using the same signal
18 processing and voting logic will probably have a very
19 high common cause factor just because software behaves
20 deterministically. Between different systems that may
21 use different inputs, different signal processing,
22 different voting logic the common cause factor can be
23 less than one and the guidance document provides
24 information as to how to go about determining the
25 numbers.

1 We now have to incorporate those common
2 cause failures into the PRA. And the way we do that
3 according to the guideline, is to take a look the
4 defense-in-depth and the diversity that exists in the
5 plant as modeled in the PRA with the existing
6 mechanical and electrical mitigating systems. And in
7 a minute I'll illustrate how that's done.

8 We'll incorporate those potential effects
9 of digital CCF into the PRA and reevaluate a core
10 damage frequency using one of the three methods that
11 are in the guideline.

12 And then on completion of that we'll
13 perform sensitivity study to help develop insights
14 with respect to, well several things. Under what
15 accident sequence conditions does I&C diversity have
16 value? Under what conditions does it appear that the
17 risk is insensitive to digital common cause failures?
18 And as important as those first two questions, why are
19 the results sensitive or insensitive to the
20 introduction of digital common cause failures? What
21 design features and operating characteristics of the
22 plant and of the I&C system itself cause those
23 results?

24 Now, as we developed the guideline we in
25 fact incorporated insights, accepted data, manipulated

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 models from quite a number of PRAs to make sure we
2 understood the nature of the kinds of insights that we
3 could develop. There were some five PRAs that
4 ultimately ended up being used as a part of the
5 development of the guideline. There were three
6 Westinghouse PWRs, differing vintage from a two loop
7 Westinghouse plant up to a four loop. We had a
8 combustion engineering PRA that we were allowed to use
9 for some of these sensitivity studies. And then we
10 also had a BWR 4 who volunteered their PRA for this
11 effort.

12 And we began pretty simply just looking at
13 some of the mitigating systems and imposing the
14 effects of common cause failures into each of these
15 systems and then varying the likelihood of the common
16 cause failures to try and determine what the effects
17 of introducing digital common cause failure would be
18 on each of these systems.

19 Recognizing that the systems themselves
20 don't work in isolation to provide adequate core
21 cooling, we then moved on to selecting a few accident
22 sequences and performed some very similar sensitivity
23 studies that we had with the systems to see where
24 digital common cause failure has a most significant
25 impact and where the results are insensitive.

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 CHAIRMAN APOSTOLAKIS: Now let me
2 understand what you did here.

3 MR. BLANCHARD: Sure.

4 CHAIRMAN APOSTOLAKIS: When you say you
5 varied the common cause failure, you varied beta?

6 MR. BLANCHARD: We varied both the
7 probability and the beta factor.

8 CHAIRMAN APOSTOLAKIS: Okay. And did you
9 do it on the individual system or cut across systems?

10 MR. BLANCHARD: In the beginning we
11 defined a fairly simple problem. We just simply took
12 an individual system and imposed on that system the
13 instrumentation of the common cause failure of a
14 presumed digital system to see what effect it would
15 have on the reliability of the system.

16 Some of the insights we found from that
17 type of a sensitivity study were that if we had a
18 system with multiple trains where the mechanical and
19 electrical equipment within those trains, most of it
20 was active rotating equipment or valves that had to
21 move, that those types of systems were not very
22 sensitive to changes in the common cause failure
23 probability. We could vary the potential for digital
24 common cause failure between the trains of those
25 systems by an order of magnitude or more and have very

NEAL R. GROSS

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

1 little effect on the overall failure probability of
2 the systems.

3 We did find some systems that were fairly
4 sensitive to the introduction of digital common cause
5 failure. Those were systems which contained a lot of
6 passive components. The AC distribution system is an
7 example of buses and breakers and cables that don't
8 necessarily have to change position in order to
9 provide their function during an accident. In
10 addition to that, the AC power system has two very
11 diverse sources of power, off site and the diesel
12 generators. And when we encountered passive systems
13 and systems with that kind of diversity we found it
14 was very easy for the instrumentation and control to
15 dominate. And if a failure of the instrumentation and
16 control were due to common cause where multiple
17 divisions of the system failed, we found the I&C to
18 dominate in those situations.

19 CHAIRMAN APOSTOLAKIS: The systems that
20 were presented earlier to us by the Staff, the
21 Framatome and Westinghouse, these are supposed to
22 control all the safety systems, aren't they?

23 MR. KEMPER: This is Bill Kemper again.

24 With regard to the RPS and ESFAS, they
25 could also be deployed with other system applications

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 as well.

2 CHAIRMAN APOSTOLAKIS: The ESFAS is all
3 these, safety injection --

4 MR. KEMPER: Right. Right. Safety
5 injection. Exactly. Contained in isolation.

6 CHAIRMAN APOSTOLAKIS: So is it then
7 reasonable to do the traditional common cause failure
8 analysis and do it on individual systems? Is it
9 possible that you will have a digital system fault
10 that would effect the actuation of all the safety
11 systems?

12 MR. BLANCHARD: Yes. And, in fact, again
13 we recognize these systems don't work in isolation.

14 CHAIRMAN APOSTOLAKIS: So did you
15 analysis--

16 MR. BLANCHARD: Some are -- each other,
17 and our next step then was to expand the analysis into
18 looking at entire accidents --

19 CHAIRMAN APOSTOLAKIS: To multiple
20 systems? So you did that?

21 MR. BLANCHARD: Yes.

22 CHAIRMAN APOSTOLAKIS: So that's in slide
23 23?

24 MR. BLANCHARD: That is coming up next,
25 yes.

1 CHAIRMAN APOSTOLAKIS: Okay.

2 MR. BLANCHARD: All right. And in fact,
3 I will get into some examples of the results in
4 subsequent slides.

5 Just briefly, we didn't limit ourselves
6 just to looking at selected systems and a few accident
7 sequences from some of these PRAs. We did take a one
8 full scope level one PRA for a PWR and looked at all
9 the accident sequences in posing a plant wide digital
10 upgrade into these models and then performing some of
11 the same sensitivity studies to find out which
12 accident sequences were most sensitive to the
13 introduction of digital common cause failures.

14 This slide happens to describe the
15 mitigating systems that were in the accident sequences
16 for this particular PRA.

17 But the way we did the sensitivity study
18 was in line with how the guidelines are written. And
19 what our guidelines suggest that you do when you're
20 trying to get insights from your PRA with respect to
21 common cause failure effects is to view digital common
22 cause failures with three factors: F i r s t t h e
23 individual channel reliability; second the fact that
24 redundant channels can fail due to common cause
25 reasons, and; thirdly to take a look at the existing

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 diversity in the mechanical and electrical systems
2 into which the instrumentation and control is being
3 installed.

4 It needs to be kept in mind that when we
5 install this instrumentation and control it is
6 controlling an integrated set of mechanical and
7 electrical systems. And those mechanical and
8 electrical systems have their own inherent defense-in-
9 depth and diversity associated with them, and that's
10 probably not going to change as a result of installing
11 instrumentation and control. So there's some clues
12 from how the plant is designed and the defense-in-
13 depth and diversity that already exists in the
14 mechanical and electrical systems as to where defense-
15 in-depth and diversity may be important in the
16 instrumentation and control.

17 Now to install or to incorporate the
18 effects of digital common cause failure in the PRAs,
19 I'll use this reliability block diagram, the simple
20 reliability block diagram to illustrate that.

21 What I have here is an initiating event,
22 say, a PWR loss of feedwater. Several mitigating
23 systems are available to cope with that event, one of
24 them is aux feedwater, another is safety injection in
25 the pores for feed and bleed purposes. And I can have

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 operator actions to initiate some of these systems in
2 addition to the instrumentation and control.

3 Now, for an individual system, say the top
4 mitigating system, it has automatic actuation system
5 that may be digitally controlled. And for the purpose
6 of performing my defense-in-depth and diversity
7 analysis using this PRA, I will insert an event, a
8 super component if you will, into the model that would
9 reflect failure of the instrumentation and control
10 from common cause failure effects that would
11 simultaneously effect both trains.

12 Now to assign the failure probabilities to
13 that common cause event I would use the defensive
14 measures approach that are in the guideline, first to
15 evaluate what I believe the failure probability would
16 be of a digital channel and then to come up with the
17 common cause failure probability. And the product of
18 those two then would be the value that I would assign
19 to the digital common cause event that would fail both
20 trains of that system.

21 Now because it is an individual system and
22 because the instrumentation and the control for each
23 train likely gets signals from the same sensors, same
24 signal processing, same voting logic for an individual
25 system the common cause beta factor is likely to be

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 very high. Probably one. And that kind of guidance is
2 provided in the EPRI guideline when we're talking
3 about an individual system.

4 Now when we start looking at the second
5 system it may also have digital equipment that is not
6 diverse from the first system. In this case we'd be
7 talking about the safety injection system as a means
8 of doing feed and bleed, which is redundant to the aux
9 feedwater system. In that particular case, again, I
10 would insert a common cause factor in between the two
11 system representing digital common cause failure of
12 both the I&C for both systems. And again I would go
13 back to my defensive measures approach to estimate a
14 failure probability for an individual channel and a
15 common cause beta factor.

16 Now in this case I may be using different
17 instrumentation to actuate the system, different
18 methods of processing the signals, different voting
19 logic. And so the beta factor between two systems may
20 be less than one. But, again, the guideline line
21 provides guidance as to how to determine both the
22 failure probability of a channel as well as the common
23 cause beta factor.

24 And then towards the bottom of the diagram
25 you'll see an operator action is available to actuate

1 the second mitigating system. If in fact the operator
2 has to use instrumentation and controls that is not
3 diverse from the digital instrumentation and control
4 that actuates the mitigating systems, I will insert
5 into my PRA a common cause beta factor that represents
6 the failure of the operator to be able to take that
7 action.

8 And then finally between the initiating
9 event and some of the mitigating system, the
10 instrumentation and control may not be diverse. An
11 example of that is the turbine controls and the
12 feedwater system. If they do not happen to be
13 diverse, then I will again for the turbine trip
14 initiating event, I will insert for the feedwater
15 system a common cause beta factor that represents
16 failure of the feedwater system given a turbine trip.
17 And again I will go back to my defensive measures
18 approach in the guideline to determine a failure
19 probability for that common cause beta factor.

20 So with the super component type approach
21 we install some fairly simple logic into the PRA first
22 to represent digital common cause failures of
23 redundant trains of equipment within systems,
24 redundant systems and operator actions that may
25 actuate those redundant systems as well as between the

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 initiating event and the mitigating systems.

2 CHAIRMAN APOSTOLAKIS: What is the
3 definition of failure here? Failure to actuate?

4 MR. BLANCHARD: For the instrumentation
5 and control it would be failure to actuate, yes.
6 Right.

7 Now, to determine how well we could get
8 insights out of a process like this we performed a
9 series of sensitivity studies. For this particular PWR
10 PRA for all of its accident sequences we didn't happen
11 to have a particular digital I&C design. And so what
12 we did was to perform a series of sensitivity studies
13 to determine where we thought digital defense-in-depth
14 and diversity was a value. In the case of the channel
15 reliability we varied the failure probability of the
16 I&C channels from 10^{-2} per demand down to 10^{-6} per
17 demand. For the common cause beta factor we varied
18 that from all the way from one to zero. And then for
19 how the I&C system was installed in the mitigating
20 systems, we looked at several different designs or
21 architectures.

22 CHAIRMAN APOSTOLAKIS: Let me
23 understanding here what you're doing.

24 MR. BLANCHARD: Sure.

25 CHAIRMAN APOSTOLAKIS: The common cause

1 failure rate is beta times the probability of failure
2 of one channel, right?

3 MR. BLANCHARD: Yes.

4 CHAIRMAN APOSTOLAKIS: Now when you go to
5 two systems --

6 MR. BLANCHARD: Yes.

7 CHAIRMAN APOSTOLAKIS: -- what is one
8 channel?

9 MR. BLANCHARD: What is one channel?

10 CHAIRMAN APOSTOLAKIS: Yes.

11 MR. BLANCHARD: Is the --

12 CHAIRMAN APOSTOLAKIS: It's the system
13 itself?

14 MR. BLANCHARD: I'm sorry. I misunderstood
15 the question.

16 CHAIRMAN APOSTOLAKIS: Let's got to the
17 top then.

18 Is there a pointer that I can use from
19 here?

20 For this system you have the two trains.

21 MR. BLANCHARD: Yes.

22 CHAIRMAN APOSTOLAKIS: You got a
23 probability of failure of one, which can be varied
24 like this. And you have beta, so beta times that is
25 the probability of the common cause failure for that

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 system, right?

2 MR. BLANCHARD: Right.

3 CHAIRMAN APOSTOLAKIS: Right.

4 MR. BLANCHARD: And recognizing the train
5 is mechanical and electrical --

6 CHAIRMAN APOSTOLAKIS: I understand. You
7 have to put a microphone on or sit down. Sit down and
8 use your pointer.

9 Now if when I go to this beta and you have
10 two systems now, right? This beta couples the two
11 systems?

12 MR. BLANCHARD: Yes.

13 CHAIRMAN APOSTOLAKIS: How do I get the
14 common cause failure rate? Multiple this beta by
15 what?

16 MR. BLANCHARD: The failure probability of
17 a channel of one of the systems.

18 CHAIRMAN APOSTOLAKIS: One channel?

19 MR. BLANCHARD: One channel.

20 CHAIRMAN APOSTOLAKIS: One of these four
21 channels?

22 MR. BLANCHARD: Yes.

23 CHAIRMAN APOSTOLAKIS: And these two are
24 identical? These two are identical, so I pick the
25 largest one?

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 MR. BLANCHARD: Yes.

2 CHAIRMAN APOSTOLAKIS: The largest
3 probability or whatever.

4 MR. BLANCHARD: They may be similar, yes.

5 CHAIRMAN APOSTOLAKIS: Yes. Or may be
6 similar.

7 So it's beta times the probability of
8 failure of this?

9 MR. BLANCHARD: Yes.

10 CHAIRMAN APOSTOLAKIS: And when I go here
11 I don't understand how I multiple --

12 MR. BLANCHARD: Well, let's say I am
13 talking about a turbine trip which has a frequency of
14 about one a year. About a quarter of turbine trips
15 turn out to be I&C related.

16 CHAIRMAN APOSTOLAKIS: Okay.

17 MR. BLANCHARD: So with a .25 per year
18 initiating event frequency I will find a beta factor
19 that I can associate between the main feedwater system
20 and the turbine controls. If I find there's
21 functional diversity between the sensors used to
22 control the feedwater system and what's used to
23 control the turbine, then I might assign a beta factor
24 of .1 or .01 --

25 CHAIRMAN APOSTOLAKIS: But what is the

1 rate of common cause failure or coupling of the
2 initiating event and the failure of the system? I
3 mean, you're talking about two different things now.
4 One is a frequency.

5 MR. BLANCHARD: Yes.

6 CHAIRMAN APOSTOLAKIS: The other is a
7 probability.

8 MR. BLANCHARD: The probability would
9 essentially be .1.

10 CHAIRMAN APOSTOLAKIS: Yes.

11 MR. BLANCHARD: If I picked a beta factor
12 of .1 for the conditional probability of the feedwater
13 system given my turbine trip due to instrumentation
14 and control.

15 CHAIRMAN APOSTOLAKIS: So you would go the
16 accident sequence and say .25 --

17 MR. BLANCHARD: Yes.

18 CHAIRMAN APOSTOLAKIS: -- a year
19 occurrence of the turbine trip because of malfunction
20 of the instrumentation control and then times -- times
21 what?

22 MR. BLANCHARD: Point one.

23 CHAIRMAN APOSTOLAKIS: Times .1 and that's
24 it?

25 MR. BLANCHARD: Yes.

1 CHAIRMAN APOSTOLAKIS: And the system is
2 out.

3 MR. BLANCHARD: Yes.

4 CHAIRMAN APOSTOLAKIS: I see. I see. So
5 the individual probability of the train is not used in
6 this case?

7 MR. BLANCHARD: It would not be used in
8 this case.

9 CHAIRMAN APOSTOLAKIS: Because the --

10 MR. BLANCHARD: Each one of these common
11 cause factors fails the entire system.

12 CHAIRMAN APOSTOLAKIS: Okay. Okay. Okay.

13 MR. BLANCHARD: This common cause failure
14 fails these two systems.

15 CHAIRMAN APOSTOLAKIS: Yes. Okay. So
16 then I can have also a beta that couples this system,
17 this system and they operator action?

18 MR. BLANCHARD: That's correct.

19 CHAIRMAN APOSTOLAKIS: And what are the
20 results of all of this?

21 MR. BLANCHARD: If I can set up the
22 problem, I'll show you the results.

23 CHAIRMAN APOSTOLAKIS: You can set it up
24 already.

25 MR. BLANCHARD: All right. I need to set

1 up one more thing.

2 CHAIRMAN APOSTOLAKIS: Okay.

3 MR. BLANCHARD: Okay. Besides just
4 looking at changes in the failure probabilities I
5 looked at different I&C architectures. I looked at
6 different levels of defense-in-depth and diversity
7 within the instrumentation and control system itself.
8 As an example, I could assume all these systems were
9 not diverse from each other or the initiator with the
10 exception of one system, perhaps the auxiliary
11 feedwater system. It would have a beta factor of zero
12 in terms of common cause given failure of
13 instrumentation and control on these other systems in
14 that case.

15 CHAIRMAN APOSTOLAKIS: Are these
16 assumptions on your part? Are you working with a real
17 PRA?

18 MR. BLANCHARD: I'm working with a real
19 PRA and I'm assuming a plant wide digital upgrade, but
20 I don't happen to have an actual digital system so I'm
21 performing sensitivity studies to decide where in all
22 the accident sequences do I believe defense-in-depth
23 and diversity in the instrumentation and control is of
24 most value.

25 CHAIRMAN APOSTOLAKIS: I see. And these

NEAL R. GROSS

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

1 are sensitivity studies here, right?

2 MR. BLANCHARD: These are going to be
3 sensitivity studies.

4 CHAIRMAN APOSTOLAKIS: Is there one of
5 them where it says everything is identical to each
6 other and --

7 MR. BLANCHARD: I skipped over that one
8 because that's a really bad answer. Yes. I started
9 with --

10 CHAIRMAN APOSTOLAKIS: You're surprised
11 we're looking for it?

12 MR. BLANCHARD: Yes, actually I am. They
13 asked me not to mention that one yesterday when --

14 CHAIRMAN APOSTOLAKIS: So even if I ask
15 you, you will not tell me?

16 MR. BLANCHARD: Oh, no. I can probably go
17 back and find --

18 CHAIRMAN APOSTOLAKIS: So what was the
19 probability of the frequency of the accident
20 sequencing if none of these things had defense-in-
21 depth?

22 MR. BLANCHARD: Oh, I would have to go
23 back and look on the analysis that I did.

24 CHAIRMAN APOSTOLAKIS: So you're not
25 telling?

1 MR. BLANCHARD: Basically it's an
2 frequency of the initiating event.

3 CHAIRMAN APOSTOLAKIS: No, for the one you
4 analyzed. You have a table in the next slide.

5 MR. BLANCHARD: Oh, I'll show you. Yes.
6 I'm sorry.

7 CHAIRMAN APOSTOLAKIS: Yes, let's look at
8 the next slide.

9 MR. BLANCHARD: I'm sorry. I thought you
10 were asking for the one where everything was not
11 diverse.

12 CHAIRMAN APOSTOLAKIS: Yes. That's what
13 I'm asking for. The next table doesn't have that on
14 it?

15 MR. BLANCHARD: The next table does not
16 have that one.

17 CHAIRMAN APOSTOLAKIS: Right.

18 MR. BLANCHARD: Right. But basically it's
19 the initiating event frequency.

20 CHAIRMAN APOSTOLAKIS: Oh, in 25?

21 MR. BLANCHARD: Yes.

22 CHAIRMAN APOSTOLAKIS: Times .1, perhaps?

23 MR. BLANCHARD: Well, if you want to
24 assume some diversity between feedwater and -- yes.

25 CHAIRMAN APOSTOLAKIS: Yes. So in the

1 worst case, worst, worst, worst case --

2 MR. BLANCHARD: Yes.

3 CHAIRMAN APOSTOLAKIS: -- I will have a
4 pretty significant sequence?

5 MR. BLANCHARD: Yes.

6 CHAIRMAN APOSTOLAKIS: And you are arguing
7 that this worst, worst case is not really realistic?
8 That's really what you're arguing, aren't you?

9 MR. BLANCHARD: That's right. And so left
10 it out of the presentation. But I think we are
11 interested in looking at the imposing diversity on
12 single systems with respect to everything else, and
13 maybe more than one system and then maybe more than
14 one system plus a diverse actuation system for one
15 other system.

16 CHAIRMAN APOSTOLAKIS: Now when you say
17 diverse actuation system, can you explain it a little
18 bit?

19 MR. BLANCHARD: Similar to what is
20 required in the ATWAS rule for aux feedwater.

21 CHAIRMAN APOSTOLAKIS: Yes.

22 MR. BLANCHARD: Maybe an analog system
23 that's diverse from the digital system.

24 CHAIRMAN APOSTOLAKIS: But I thought we
25 couldn't find analog components anymore?

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 MR. BLANCHARD: Some of the ATWAS systems
2 are very simple and, yes, they are analog. Some of
3 them are analog.

4 CHAIRMAN APOSTOLAKIS: They are now. But
5 if you want to replace those will you be able to find
6 other analog components? Isn't that one of the prime
7 reasons why we're working on this?

8 MR. STRINGFELLOW: Yes. This is Jack
9 Stringfellow again.

10 This is not to say that analog components
11 no longer exist. I mean many of us are currently
12 maintaining our protection systems, our analog
13 protection systems with parts that we -- cards, for
14 example. ASIC cards that were developed for just for
15 the purpose of maintaining those systems. But we have
16 the capability in specific cases to maintain these
17 analog systems, and many of us are doing that.

18 MR. BLANCHARD: Otherwise you would have
19 to go to a diverse digital system.

20 CHAIRMAN APOSTOLAKIS: And what would that
21 be?

22 MR. BLANCHARD: I'm sorry?

23 CHAIRMAN APOSTOLAKIS: What would that be?
24 A diverse digital systems means what? Different
25 parameter?

1 MR. BLANCHARD: Different manufacturer,
2 different symptoms, different signals.

3 CHAIRMAN APOSTOLAKIS: Look at that
4 results now.

5 MR. BLANCHARD: Okay. All right. Well,
6 one last thing, if you don't mind. What I've done
7 here is essentially build a three dimensional matrix
8 where I'm going to vary all three of these factors and
9 then look at the final core damage frequency to
10 identify which combinations of these factors get me
11 back to a core damage frequency close to what I
12 started with. That was the purpose of these
13 sensitivity studies.

14 And I will show you the results for two of
15 the initiators. First is loss of feedwater for this
16 PRA. It happens to have a 8 times 10^{-2} per year
17 frequency. It's core damage frequency is five times
18 10^{-7} per year.

19 CHAIRMAN APOSTOLAKIS: You meant the
20 contributing of this sequence is five times to minus
21 seven?

22 MR. BLANCHARD: This is all the sequences
23 associated with loss of feedwater.

24 CHAIRMAN APOSTOLAKIS: Okay.

25 MR. BLANCHARD: All of them.

1 CHAIRMAN APOSTOLAKIS: Yes, that's what
2 I'm saying. This initiator?

3 MR. BLANCHARD: This initiator, yes.

4 CHAIRMAN APOSTOLAKIS: Okay.

5 MR. BLANCHARD: Now I'm just going to show
6 you a slice of three dimensional matrix. It happens
7 to be the slice where I've assumed the probability of
8 a failure of a single channel is 10^{-4} --

9 CHAIRMAN APOSTOLAKIS: On what basis?

10 MR. BLANCHARD: Well, my defensive
11 measures will get me to that basis.

12 CHAIRMAN APOSTOLAKIS: Yes. But one of
13 the slides earlier said that a strict process doesn't
14 necessarily lead to a highly reliable software.
15 That's a result of a very stringent process
16 controlling the process of developing the software,
17 10^{-4} or --

18 MR. TOROK: Plus good defensive measures.

19 I'm sorry. This is Ray Torok.

20 Yes. It's a good process plus good
21 defensive measures to justify a number in that range.

22 CHAIRMAN APOSTOLAKIS: Defensive measures
23 on a single channel?

24 MR. TOROK: Yes.

25 CHAIRMAN APOSTOLAKIS: Like what?

NEAL R. GROSS

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

1 MR. TOROK: You apply the defensive
2 measures evaluation that Thuy described --

3 CHAIRMAN APOSTOLAKIS: So that's the
4 process?

5 MR. TOROK: No. I'm sorry. I understand.
6 When we refer to process, we usually talk about the
7 software development process.

8 CHAIRMAN APOSTOLAKIS: Okay. So what
9 defensive -- remind me what defensive measures would
10 apply to a single channel.

11 MR. NGUYEN: This is Thuy.

12 CHAIRMAN APOSTOLAKIS: Yes.

13 MR. NGUYEN: For example, cyclic behavior
14 and a very strict identification of all the factors
15 that could take the software out of this cyclic
16 functioning.

17 CHAIRMAN APOSTOLAKIS: I'm having a
18 problem with that. I mean, come on. We've had, what
19 is it, Appendix B is it, the quality assurance. Yes.
20 That's as stringent as anything and still we've had
21 failures. So there is nothing unique about what you
22 are doing here, is it?

23 MR. NGUYEN: Oh.

24 CHAIRMAN APOSTOLAKIS: Oh.

25 MEMBER KRESS: What's the probability of

1 failure on demand for the analog system that this
2 replaced?

3 MR. BLANCHARD: Well, as it turns out we
4 have built a small model of the two out of four taken
5 twice system made of relays, contacts and relays.

6 MEMBER KRESS: Yes.

7 MR. BLANCHARD: And for a single channel
8 it happens to be right on the order of 10^{-4} --

9 MEMBER KRESS: That might be a
10 justification to that, because we heard earlier that
11 you could almost assume that the replacement system
12 has a failure probability of at least as good as the
13 analog.

14 MR. BLANCHARD: It was better than an
15 assumption. We believe we can justify that.

16 MEMBER KRESS: Right. You believed you
17 could justify that.

18 CHAIRMAN APOSTOLAKIS: I'm at a loss here.
19 I don't even know whether the beta factor model
20 applies.

21 MR. BLANCHARD: Whether the --

22 CHAIRMAN APOSTOLAKIS: Yes. The beta
23 factor model for common cause failures, why would it
24 apply to a system where the common cause failure may
25 be a specification error? I don't know. Does anybody

NEAL R. GROSS

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

1 know? And still, the 10^{-4} , I mean there is nothing
2 unique -- wait.

3 Mr. Nguyen?

4 MR. NGUYEN: Yes.

5 CHAIRMAN APOSTOLAKIS: There is unique
6 about the quality control you are putting here because
7 this business from day one has very strange in quality
8 control processes. And yet things fail. So what's so
9 unique about this? You're giving me a metaphor with
10 a circle, that's very illuminating, you know, for
11 educational purposes. But don't tell me that it's 10^{-4}
12 because you do a circle.

13 MR. NGUYEN: Well, it's -- no. But what
14 I'm saying is that because I'm working a cyclic
15 behavior, I can identify where are the most likely
16 points that could cause failures.

17 CHAIRMAN APOSTOLAKIS: And why can't I do
18 that with pumps so the pumps will never fail?

19 MR. NGUYEN: I'm not a mechanical
20 engineer.

21 CHAIRMAN APOSTOLAKIS: I know.

22 MR. NGUYEN: So I don't know.

23 MR. TOROK: Because pumps wear out is a
24 easy answer.

25 MR. GUARRO: But in the analogy between the

1 analog and digital systems so that was back on --
2 let's see, I think it was slide 20 there is the
3 statement "The likelihood of specification errors is
4 comparable for equivalent analog and digital systems."
5 I'm personally not convinced that that's true.

6 CHAIRMAN APOSTOLAKIS: No. I mean, there
7 are so many assumptions in all this.

8 MR. GUARRO: Because, I mean, I think that
9 the design process for an analog system is quite
10 different from the design process of something that
11 involves software. And having worked both with
12 engineers and software programmers, they behave very
13 differently. So to say that the specification error
14 would be the same, I think that's a big jump in faith.

15 CHAIRMAN APOSTOLAKIS: And also, I'd like
16 somebody to convince me why the beta factor model
17 applies here.

18 MR. TOROK: May I offer a couple of
19 clarifications. This is Ray Torok again.

20 You mentioned the Appendix B quality
21 assurance process. And that is a process that tries
22 to insure that you end up with high quality software.
23 And for software development it would require that
24 certain documents be generated along the way of
25 software requirements specification and a requirements

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 transability matrix and so on, and you do all the
2 right testing on the software. It's all about process
3 for software development. That's not what was Thuy was
4 talking about when he said defensive measures.

5 Now some of those process elements do
6 constitute defensive measures. But what he's really
7 looking at is the end product and the design
8 attributes that end up built into it.

9 A good process does not guarantee a good
10 design. It gives you the well documents design, but
11 not a good design.

12 CHAIRMAN APOSTOLAKIS: I agree. But how
13 do you know the circle?

14 MR. NGUYEN: This is Thuy again.

15 CHAIRMAN APOSTOLAKIS: Yes.

16 MR. NGUYEN: I can give you the example of
17 what I will be doing for the Teleperm XS for EDF's
18 purposes. We have a requirement from Framatome to
19 have the source code and the design documents of the
20 Teleperm XS. And we'll have them in offices for
21 analysis by advanced tools by, I would say, the formal
22 verification methods that exist currently. And, of
23 course--

24 CHAIRMAN APOSTOLAKIS: You still don't
25 know the circle.

1 MR. NGUYEN: Sorry?

2 CHAIRMAN APOSTOLAKIS: I mean, you are
3 gaining confidence that the thing will not fail in
4 frequency, but you still don't know the circle.

5 MR. NGUYEN: I know the circle because --
6 I'm a software engineer. I can understand and read
7 what are the statement, the individual statements that
8 are put in the software programs that command the
9 behavior of the software. That has been the way we
10 have assessed safety particular software since many
11 years now. And that has been -- we have developed and
12 acquired tools to do that.

13 MR. TOROK: The other point I'd like to
14 make -- this is Ray again. Is that if you're going to
15 pick numbers for failure probabilities and beta
16 factors, and Dave used them in an evaluation. And
17 we're not trying to make claims about what the real
18 failure probabilities are. What we are trying to do
19 is make claims that we can identify the places where
20 a diversity is important, diversity in I&C is
21 important and where it isn't. Where it's more likely
22 to be important. And that's what the risk insights
23 here are about. I don't believe those specific
24 numbers anymore than you do. And if you want to say
25 well 10^{-4} , that's fine, you do it. Do it at 10^{-3} , and

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 Dave's done those sensitivities. And that's really
2 what the exercise is about in generating risk
3 insights.

4 CHAIRMAN APOSTOLAKIS: But an actuation
5 system, I'm not really difficult to convince that you
6 have a low probability of failure. I mean, all it
7 does is send a signal to start something. But if you
8 go to more advance platforms, I don't believe -- of
9 course I have to think about the beta factor.

10 First of all, if the individual channel
11 becomes 10^{-2} , now everything goes up by two orders of
12 magnitude, right? So what does that tell you? I
13 don't know what it tells me. It tells me that if I
14 have one diverse system it's $1.6 \cdot 10^{-3}$?

15 MR. BLANCHARD: If your goal is to keep
16 your core damage frequency where it was before you
17 installed the system and you install a 10^{-2} channel,
18 it says you're going to have to do a lot more in terms
19 of installing other diverse systems or justifying a
20 very low beta factor in order to maintain that core
21 damage frequency.

22 CHAIRMAN APOSTOLAKIS: Yes. By the way,
23 these numbers on the table refer to all the sequences
24 initiated by loss of feedwater?

25 MR. BLANCHARD: Yes.

NEAL R. GROSS

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

1 CHAIRMAN APOSTOLAKIS: So if I make the
2 individual channel 10^{-2} , I end up one 1.6×10^{-3} , which
3 is about four orders of magnitude greater than the
4 current. And I still don't know what that tells me.
5 Four orders of magnitude, you know, is a lot.

6 MR. BLANCHARD: Yes. Well, if it does get
7 you to 1.6×10^{-3} , what it says is we have to go--

8 CHAIRMAN APOSTOLAKIS: With two systems
9 diverse and so on?

10 MR. BLANCHARD: Yes. We have to go way
11 down on this list of diversity in the instrumentation
12 and control and way over to the right of the chart in
13 terms of the beta factor before we have an acceptable
14 side --

15 CHAIRMAN APOSTOLAKIS: Why, by the way,
16 have you shaded some of these dark shade?

17 MEMBER KRESS: The acceptable regions.

18 MR. BLANCHARD: These are what I am
19 calling acceptional regions.

20 CHAIRMAN APOSTOLAKIS: Oh, I see.

21 MR. BLANCHARD: These are core damage
22 frequencies that are close to what I started with.

23 CHAIRMAN APOSTOLAKIS: To the original.
24 Yes.

25 MEMBER KRESS: I would have been tempting

NEAL R. GROSS

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

1 to put the dark shading on the next round. You got it
2 lightly shaded I noticed.

3 MR. BLANCHARD: Yes, those were kind of in
4 between numbers where I wasn't quite comfortable.

5 MEMBER KRESS: Maybe you could have them,
6 maybe not. Yes.

7 MR. BLANCHARD: And I have 18 initiating
8 events to do this with. And when I get done my change
9 in core damage frequency has to be small for the sum
10 of them.

11 CHAIRMAN APOSTOLAKIS: Yes.

12 MR. BLANCHARD: And so that's what the
13 shading is. I could probably live with the slightly
14 shaded areas. But, again, I have to do a lot of work
15 on the other initiating events to make sure they're
16 small.

17 CHAIRMAN APOSTOLAKIS: Well, there's the
18 whole issue with bringing software into the PRA
19 becomes trivial the moment you are willing to accept
20 the probability of one channel failing is something
21 you can estimate. Then everything, of course, becomes
22 building on manipulations. It's that PDF of 10^{-4} for
23 demand that is a major problem. I mean, I don't know
24 how you get that.

25 On the other hand the argument that, look,

1 even if I assume -- because let's face, these things
2 are reliable. I mean, it's not that they're failing
3 every other week. Even if I assume a very high
4 number, I still get results that are reasonable, then
5 maybe you have a point. In other words, your
6 philosophical approach I think is pretty good. How
7 reliable do they have to be?

8 MR. BLANCHARD: And --

9 CHAIRMAN APOSTOLAKIS: And what?

10 MR. BLANCHARD: And the conclusion we come
11 to is the channel of digital reliancy need be no more
12 reliable than a similar channel of analog.

13 CHAIRMAN APOSTOLAKIS: I don't know. Does
14 everyone agree with that? I'm not sure.

15 MR. MORRIS: If I could speak to the
16 question of the reliability of a single channel?

17 My name is Pete Morris. I work for
18 Westinghouse. I'm a designer of reactor safety
19 systems.

20 And if we step back for a moment and think
21 what kind of equipment is being used for these kinds
22 of applications. In the process control industry, not
23 nuclear power but petroleum refineries, pharmaceutical
24 factories, all kinds of applications in the process
25 control field there are numerous vendors of now all

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 computer-based distributed control system.

2 The safety systems, and for that matter
3 nonsafety systems, that are being used in modern
4 nuclear power plant upgrades are all based on these
5 different existing platforms that have been dedicated
6 for class 1E service.

7 If there were no nuclear power industry,
8 there is an overwhelming emphasis on the reliable
9 operation of these process control systems for all
10 kinds of things. Product liability is very important
11 to the maker of pharmaceuticals. Public safety related
12 issues for someone in a high energy industry is very
13 important. And the process control industry is
14 demanding that -- or the process control requirements
15 for many industries are demanding that very reliable
16 platforms must be available for all kinds of safety,
17 and I don't mean nuclear safety, but practical
18 everyday public safety anyway. And so by starting
19 with these kinds of system you know that you are
20 getting systems that have basic reliability
21 characteristics that approach or, frankly, even exceed
22 that of the historical analog-based systems of long
23 ago. Because modern safety and liability issues
24 demand that this equipment, that these systems, that
25 these platforms must be that reliable.

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 CHAIRMAN APOSTOLAKIS: I guess our problem
2 here is not just that they have to be reliable. I
3 mean, we have to be able to demonstrate that one way
4 or another. That's part of the issue here. It's not
5 just -- I mean, again, you know I have no doubt that
6 they're pretty systems. The question is how reliable
7 are they.

8 What do we do with our time now? Are you
9 near the end or you still --

10 MR. BLANCHARD: We are approaching the end
11 here. If I could just summarize this slide.

12 CHAIRMAN APOSTOLAKIS: Yes. Can you do
13 that?

14 MR. BLANCHARD: Yes. The conclusion w
15 came to with respect to the loss of feedwater
16 initiator is that if I can show that the I&C for two
17 systems are diverse from the control system that may
18 have caused the initiating event, plus either have a
19 diverse actuation system or allow the operator to be
20 able to initiate the systems, then that is sufficient
21 to bring my core damage frequency back close to where
22 it was originally. All right. And that is with a
23 probability failure of 10^4 --

24 MEMBER KRESS: If you have 18 sequences,
25 why don't you do divide that number by 18 or by 10?

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 MR. BLANCHARD: Well, I know that --

2 MEMBER KRESS: Because these are dominate
3 is what --

4 MR. BLANCHARD: I happen to know that some
5 of the initiating event frequencies are low to begin
6 with.

7 MEMBER KRESS: Okay.

8 MR. BLANCHARD: And I can --

9 MEMBER KRESS: You have prior knowledge
10 that allows you to say that they're not going to
11 contribute as much as these?

12 MR. BLANCHARD: Right. But in the end we
13 did all 18 initiating events. We did look at the
14 change in core damage frequency for all 200 sequences,
15 some together --

16 MEMBER KRESS: Yes. You could make a
17 matrix like this for all 18 of them, that would
18 include all 18 of them.

19 MR. BLANCHARD: In fact, we did.

20 MEMBER KRESS: Okay.

21 MR. BLANCHARD: In fact, we did. And for
22 different values of failure of a channel. And the
23 results were that with multiple mitigating systems
24 diverse from the cause of the initiating event and the
25 ability of the operator to actuate those systems we

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 could get very close to a change in core damage
2 frequency of 10^{-6} per year, even assuming very high
3 beta factors.

4 MEMBER KRESS: What constitutes a diverse
5 system in your mind? Is that manufactured by a
6 different company or a different programmers or what?

7 MR. TOROK: Technically, I suppose, you
8 can establish reasonable assurance that they won't be
9 subject to the same common cause failure. So --

10 MEMBER KRESS: So that's just another way
11 of saying you're diverse.

12 MR. TOROK: Well, yes. And the real answer
13 is you have to look inside the systems and the
14 applications to make that assumptions. Just because
15 they're from different manufacturers or use different
16 shifts and whatnot is not the whole story. It's not
17 the whole story.

18 MEMBER KRESS: They have to have some sort
19 of different programming on them.

20 MR. TOROK: Yes. Well, there need to be --
21 Thuy, did you want to get your two cents worth in
22 here?

23 MR. NGUYEN: Yes. I've tried to
24 illustrate defensive measures that would ensure or
25 give a very high assurance that the same platform

NEAL R. GROSS

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

1 would not be a significant cause of common cause
2 failures. I know that it's -- I would say, something
3 that is difficult to swallow. But this is what we can
4 see from the history of these platforms which are used
5 quite heavily in other industries.

6 MR. TOROK: But it comes back to being
7 able to generate an argument and reasonable assurance
8 that they're not subject to the same common cause
9 failures. Now Thuy's saying when you do that you'll
10 find that just because you have the same platform in
11 two different systems doesn't necessarily mean you
12 have a problem. There are other things that you need
13 to look at that are going to be more important. But
14 that's -- you know, it's a different argument. But you
15 come back to reasonable assurance, whatever that
16 takes, to show that there won't be the same common
17 cause failure. That's what it really comes down to.

18 CHAIRMAN APOSTOLAKIS: Your conclusions?

19 MR. TOROK: Have we wrapped that up?

20 MR. BLANCHARD: Finally, for the medium
21 LOCA which we didn't have a chance to talk about. All
22 we needed was high reliability software. What we
23 assumed in terms of diversity among the mitigating
24 system or a beta factor between those systems that
25 were not diverse played very little role in driving

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 the risk of the medium LOCA. We just needed high
2 reliability channel of --

3 MR. TOROK: You want to contrast BTP-19
4 and --

5 MR. BLANCHARD: Do we want to do that?

6 MR. TOROK: Okay. That's good.

7 I think we ought to just skip to the
8 conclusions. You've already hit these things.

9 CHAIRMAN APOSTOLAKIS: You have a
10 conclusions slide?

11 MR. TOROK: Yes. We can do conclusions
12 real fast.

13 CHAIRMAN APOSTOLAKIS: Okay.

14 MR. TOROK: Okay. And the first one just
15 says we believe that now is the time to start looking
16 at factoring risk insights into defense-in-depth and
17 diversity evaluation.

18 Let's go to the next one without any
19 detail there. The other one is based on what we're
20 seeing in sensitivity studies and so on, we would
21 recommend, make certain recommendations in regards to
22 what NRC is pursuing. And we tried to list that here.
23 We'd say, yes, this is a good area to pursue,
24 reliability of digital equipment, modeling in PRA
25 that's great. However, the first thing here don't

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 start with the general case.

2 When I sat here in June and one of the
3 Staff presentations on the Research program, there was
4 a list of issues that can effect digital equipment.
5 And it was sort of a general case issues list. And
6 what you find when you look at systems that might
7 really go into safety applications is they're designed
8 in such a way that those issues are irrelevant for
9 them. So I say constrain the problems for starters.
10 Constrain the problem to a realistic system for a
11 safety related application. That's all.

12 The next thing there is to keep track of
13 where D3 is a value and what levels of reliability you
14 need. I think it's a big advantage to understand what
15 your target is before you try to get to it.

16 Let's see, the third one, oh yes. Address
17 designed in behaviors, defensive measures. You know,
18 what the system is actually designed to do and ways to
19 look at the product, to evaluate the product because
20 that is more important in determining reliability than
21 the process elements like whether or not you got a
22 software requirements specification.

23 So we would say find a way to get that
24 into the NRC program. Now, actually some of the
25 presentations in June did touch on that, but the

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 emphasis was going in a different direction as far as
2 I could tell.

3 The other thing is let's just coordinate
4 with industry to make sure that we cover all the
5 important issues and that we don't duplicate effort
6 anymore than we have to. But I'd say it's certainly
7 an important area to keep working on.

8 The only other thing I would like to do is
9 thank you very much for letting us take all this time
10 to talk with you about these. And we'd be happy to
11 come back again if you think it would be helpful.

12 CHAIRMAN APOSTOLAKIS: Thank you very
13 much, gentlemen.

14 Any questions from the people sitting at
15 the table?

16 We do appreciate your coming here and
17 explaining this to us. Thank you. And I hope you are
18 taking our comments the way they were intended, in a
19 constructive way.

20 MR. STRINGFELLOW: I'd just like to say I
21 think we had a very constructive conversation and I
22 really appreciate the depth of the questions and the
23 challenging that we got here today. And we're going
24 to take this back and I hope we can move forward with
25 the review of this document.

1 Thanks.

2 CHAIRMAN APOSTOLAKIS: Thank you.

3 I propose we take ten minutes break and
4 then come back to the NRC presentation.

5 (Whereupon, at 4:13 p.m. a recess until
6 4:28 p.m.)

7 CHAIRMAN APOSTOLAKIS: Okay. We're back
8 to the Staff presentations.

9 Bill?

10 MR. KEMPER: Thank you.

11 Yes, again, I'm Bill Kemper. I'm with my
12 colleague Steve Arndt who will provide most of the
13 presentation.

14 This discussion will focus on the systems
15 aspects of digital technology, which is Section 3.1 in
16 the Research Plan.

17 CHAIRMAN APOSTOLAKIS: Yes.

18 MR. KEMPER: Current issues. As we all
19 know, there is an ever increasing use of digital
20 systems that requires new information and continuous
21 improvements to the NRC review process. Digital
22 systems will take on an ever increasing role in the
23 protection and control systems of nuclear power plants
24 and also fuel facilities, I might add, and even some
25 nonpower production facilities, you know, such as a

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 medical group.

2 New system challenges will continue to
3 emerge. For example, tin whiskers has become an issue
4 with us. Also INC instrumentation and control.
5 Circuit board aging has been a somewhat long issues
6 that we're dealing with, not only here but across the
7 world as well as to digital safety systems. So this
8 Research program will assist the Staff to develop a
9 fundamental understanding of how digital technologies
10 are used in safety systems and, again, develop review
11 guidance, tools, review procedures and training to the
12 staff to support NRC Staff reviews and evaluation of
13 the systems.

14 Now this next slide is an overview of the
15 various components of this area. We're going to talk
16 about environmental stresses in detail in just a
17 little bit. I believe that's next on the agenda. Ms.
18 Christina Antonescu will talk about that. And so
19 we'll give you a brief overview of the rest of these
20 systems, the COTS digital safety systems, effective
21 total harmonic distortion on digital systems compared
22 to diversity and defense-in-depth, least ways what we
23 believe we intend to do from a research environment in
24 that area. Systems communications, power distribution
25 system interfaces with nuclear facilities and finally

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 operating systems.

2 So, with that I'll turn it over to Steve
3 to provide an overview of each of these sections.

4 CHAIRMAN APOSTOLAKIS: So there are two
5 presentations? One by Steven and one by Christina.

6 MR. KEMPER: Yes.

7 CHAIRMAN APOSTOLAKIS: Okay.

8 MR. KEMPER: Yes. This one is scheduled
9 to go until -- well, it's scheduled to last an hour.
10 We'll try to get through it quicker than that if we
11 can.

12 CHAIRMAN APOSTOLAKIS: Okay.

13 MR. ARNDT: Yes. What we thought we'd do
14 is go over very quickly all the different programs in
15 this program area. And in keeping with the
16 recommendations of the Subcommittee at our last
17 meeting, we're going to talk in more detail about the
18 ongoing program and give you some results that you can
19 understand.

20 CHAIRMAN APOSTOLAKIS: Good.

21 MR. ARNDT: And that's why the
22 environmental stressors is highlighted in green.
23 That's of these programs, that's the only ongoing
24 program we have. The rest of these will be started in
25 the future. Of the ones here, I will tell you when we

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 plan to start the work. The diversity and defense-in-
2 depth program is the next one to be started. That
3 will be started this year.

4 MR. KEMPER: Oh, and I did want to
5 highlight one thing, George. You asked a question
6 earlier today about the priority. In the Research
7 Plan back in section Table 4 there actually is a
8 priority assigned to each one of these in terms if
9 high, medium, low. Okay.

10 CHAIRMAN APOSTOLAKIS: Thank you.

11 MR. KEMPER: And that supports the
12 schedule, the associated schedule for the projects.

13 CHAIRMAN APOSTOLAKIS: Is the rational
14 given, too, or just -- it's performance based. We've
15 just got the result?

16 MR. KEMPER: It relates to the strategic
17 goals, the objectives and goals of the strategic plan
18 of the agency.

19 CHAIRMAN APOSTOLAKIS: I'll make sure I
20 read that. Thank you.

21 MR. ARNDT: Also before we go forward I
22 also want to highlight a couple of issues. Bill
23 mentioned that the program plan is not just an NRR
24 program plan, it's an agency program plan. Some of
25 the areas are more emphasis on reactor issues. For

NEAL R. GROSS

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

1 example, the defense-in-depth issue is a specific
2 reactor issue. But particularly in this section a lot
3 of these issues apply equally to field fabrication
4 facilities that have distributed control systems,
5 issues about individual components in a medical -- a
6 radiator and things like that for the operating system
7 that's in the THD and things like that are applicable
8 in many cases to nonpower reactor applications that
9 we're interested in.

10 CHAIRMAN APOSTOLAKIS: That will be
11 useful.

12 MR. ARNDT: Yes.

13 CHAIRMAN APOSTOLAKIS: We'll come back it.

14 MR. ARNDT: Okay. The systems aspect is
15 a set of projects that follow this category primarily
16 because they effect the system as a whole from either
17 internal or external factors, but are broad scoped.
18 So they're things like environmental stressors, the
19 interactions with the digital systems with the rest of
20 the support systems in the plant like power supplies
21 and things like that. The issue of operating systems
22 and systems architecture which are not specific to a
23 particular component but are generic across a system.
24 And, of course, the issues we're facing with the use
25 of COTS and things like that. So that's how this

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 particular group got grouped together.

2 CHAIRMAN APOSTOLAKIS: By the way, let's
3 go back to this. Isn't the identification or the
4 failure modes of software part of the system aspects?

5 MR. ARNDT: Yes, but that's really a
6 crosscutting issue. That's something that we have to
7 deal with in all the different programs.

8 CHAIRMAN APOSTOLAKIS: So where will it be
9 handled?

10 MR. KEMPER: Well, we have a section
11 Software Quality Assurance. And that's where that's
12 treated. That's where we're dealing with that.

13 CHAIRMAN APOSTOLAKIS: Really?

14 MR. KEMPER: Yes, I believe it is. What
15 is that?

16 MR. ARNDT: 3.2

17 MR. KEMPER: 3.2. Yes, we talked about
18 that at the last meeting as well.

19 MR. ARNDT: So the research is, and this
20 similar to slides you've seen before, designed to look
21 at improving the fundamental understanding of the
22 digital technology, understanding their strengths,
23 weaknesses, limitation, capabilities. Identifying
24 what technical information is needed by the reviewers
25 in developing more quantitative review criteria where

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 possible. Improving the licensing technologies, the
2 tools, the methodologies and acceptance criteria.

3 So in many cases, and actually most cases,
4 we already have a process by which to review these
5 systems. But either because of their ever increasing
6 complexity or because we want to do it better based on
7 newer information, we have research programs in these
8 areas.

9 I'm going to hit this very, very briefly
10 because we're going to have a full presentation on
11 this program, but this program is basically looking at
12 how the systems are maintained in the expected
13 environment. What are the issues associated with EMI,
14 with lightening, the environment in which they exist?
15 And as we mentioned earlier, Christina will have a
16 full section on that.

17 The systems communication issue, this was
18 discussed in detail this morning, but what we're
19 really looking at is the safety aspects associated
20 with how the systems communications are put together.
21 The internal and external architectures, the protocols
22 both proprietary and off-the-shelf protocols; what
23 makes a good safety system and what are the particular
24 aspects of communications and protocols that we need
25 to work at. So the idea is to look at these systems,

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 the complexity, and understand what that is.

2 CHAIRMAN APOSTOLAKIS: Now if what we are
3 talking about is actuation systems --

4 MR. ARNDT: Yes.

5 CHAIRMAN APOSTOLAKIS: -- systems that
6 actuation signals, how relevant is all this? In other
7 words, by just listening to what you are saying one
8 gets the impression that you're talking in very
9 general terms, general software systems. And I think
10 the EPRI guys also said something to that effect. And
11 I remember that, you know, when that Academy work came
12 out there were a lot of debates behind it and all
13 that. And one argument by the industry was that the
14 systems you're talking about are extremely simple.
15 They're not talking about controlling the space
16 shuttle where you have continuous feedback and control
17 and all that. So a lot of these general findings and,
18 you know, communication and this and that, may not
19 apply to the simpler systems that an industry is
20 thinking of employing.

21 Like actuation systems, do I really have
22 to worry about communications and all that? What do
23 they communicate?

24 MR. ARNDT: Okay. There is both an issue
25 with what you said and a lot of truth in what you

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 said. When you talk about general, general you're
2 exactly correct. When you talk about the fact that
3 there are lots and lots of different protocols out
4 there, there's lots and lots of different software
5 communication, the hardware communication bus
6 configurations and like that; you're absolutely
7 correct. That is not something that we are
8 particularly concerned about.

9 The kinds of systems that we regulate,
10 safety systems, and the kinds of systems that we're
11 interested in, nonsafety systems that are used in
12 actual nuclear power plants or could be in the future,
13 are the things that we're most interested in and we're
14 trying to direct our research toward. So in that case
15 what you're saying is correct. The research needs to
16 be focused on those kinds of things that could have
17 direct implications on our regulated systems or those
18 systems that are important to safety from a risk
19 standpoint.

20 CHAIRMAN APOSTOLAKIS: And not expected to
21 be implemented in the next several years

22 MR. ARNDT: Are either currently being
23 used.

24 CHAIRMAN APOSTOLAKIS: Yes.

25 MR. ARNDT: Or currently being proposed or

1 some reason to believe --

2 CHAIRMAN APOSTOLAKIS: Or in the near
3 term?

4 MR. ARNDT: -- will get into a plant.

5 CHAIRMAN APOSTOLAKIS: Yes.

6 MR. KEMPER: And if you'll recall that
7 diagram that we went over this morning during the
8 security program, we illustrated where some of those
9 interchannel communications were being deployed in
10 systems that were being proposed to us for safety
11 system applications.

12 So you know we have specific reg guide
13 guidelines. Regulatory requirements, excuse me, that
14 require separation and deal with communications. But
15 this research will explore that to ensure that we
16 fully appreciate the ramifications of this
17 communication protocols and establish review criteria,
18 again, that the Staff can use in reviewing and
19 accepting these types of applications.

20 MR. WATERMAN: This is Mike Waterman,
21 Research.

22 Anytime you have data moving from one
23 point to another you've got yourself a network by
24 definition. And the way you move that data is by
25 using some kind of a protocol, be it SINEC L2 or

1 something like that.

2 The issue that arose with me when I was
3 trying to review was is I really didn't have
4 acceptance criteria for what features of SINEC L2
5 protocol were good features and which features ought
6 the developer to stay away from. And what I
7 envisioned off of looking at these various protocols
8 was to come with guidance for the Staff so that when
9 they were looking at a digital system such as that
10 complicated diagram that we kept referring to this
11 morning, the reviewer would be able to look at that
12 and say okay, they're using SINEC L2. Let's dig in to
13 how they're using it to make sure that they're only
14 using those features of SINEC L2 that are safe. And
15 we don't have any guidance for that right now, but the
16 TSX system has a pretty complicated network structure.
17 They have an AMD K6 E2 microprocessor. That's a 266
18 megahertz microprocessor just to do the
19 communications.

20 So, you know, these systems need to be
21 reviewed. And right now our criteria for what
22 protocols are good and bad is sort of vague and it
23 depends on whoever is reviewing it and what they know
24 about protocols. So we're trying to develop some more
25 definitive information for the reviewer to use when

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 he's doing a safety evaluation.

2 I guess that was the point --

3 CHAIRMAN APOSTOLAKIS: Okay. Okay. Let's
4 go on.

5 MR. ARNDT: Let me rephrase that just
6 slightly before we go on. The issue is, as I said,
7 very general we're not that interested in because of
8 the application issues. But the simplicity issue is
9 something that we really need to be looking at now.
10 Because we're not just talking about simple ladder
11 logic anymore. There's a lot of fairly complicated
12 implementations of these trip functions and basic
13 control functions because of the kinds of issues that
14 Mike just pointed out.

15 MEMBER SIEBER: Let me ask probably a too
16 simple question. GDC 24 talks about separation
17 between protection and control. The way I read that it
18 doesn't necessarily say that you can't use a single
19 processors for both functions.

20 MR. ARNDT: That is a -- Bill, you want
21 to--

22 MEMBER SIEBER: Can you or can't you?

23 MR. KEMPER: I'm sorry?

24 MEMBER SIEBER: Can you or must you use
25 separate CPUs between control systems and protection

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 systems?

2 MR. KEMPER: Between the control system
3 and protection system?

4 MEMBER SIEBER: Yes. Can you run it all
5 through the same box?

6 MR. KEMPER: Well, typically you don't
7 have a control system and a protection system in the
8 same box. Typically they're not commingled, okay?
9 Just from a design strategy.

10 MEMBER SIEBER: Yes. The question is is it
11 outlawed? GDC 24 when I read it really doesn't tell
12 me that.

13 MR. KEMPER: Well, GDC 24 is specified as
14 a separation criteria, right, applicable to --

15 MEMBER SIEBER: Right. And it looks like
16 more transducers and cutout switches and stuff like
17 that.

18 MR. KEMPER: Right. Yes. That's the idea
19 so that faults are not promulgated, obviously, from
20 one channel to the other.

21 MEMBER SIEBER: Right.

22 MR. KEMPER: Communication strategies,
23 though, are different and the task here is to make
24 sure that the communication strategies don't interfere
25 with the electrical separation that's required by GDC

NEAL R. GROSS

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

1 24. So that's what we're trying to do here is
2 evaluate various means that the vendors are using for
3 communications between channels and understand the
4 ramifications of that. And, as we said, develop
5 acceptance criteria ourselves or if we find problems,
6 maybe establish some coping strategies on how to deal
7 with that.

8 Did that answer your question?

9 MEMBER SIEBER: No.

10 MR. KEMPER: I'm not sure I did.

11 MEMBER SIEBER: No, it didn't. It leads
12 me to another question. From one channel to another
13 do you need separate CPUs?

14 MR. KEMPER: Yes.

15 MEMBER SIEBER: Are they truly independent
16 or not?

17 MR. KEMPER: Yes. Yes, they typically are,
18 right. Each channel is typically implemented by its
19 own separate CPU.

20 MEMBER SIEBER: Okay.

21 MR. KEMPER: It's own box is separation.

22 MEMBER SIEBER: And "typically" means not
23 always or is there a regulation, a standard or a
24 requirement that says this is the way it's got to be?

25 MR. KEMPER: Well, to comply with the

1 separation requirements of GDC 24 it has to be that
2 way. At least, I don't know of any way to skin that
3 cat, put more than one channel into one box.

4 MEMBER SIEBER: That's the way I look at
5 it. CPUs are cheap.

6 MR. KEMPER: Well, safety related CPUs,
7 though, are not quite so cheap actually.

8 MEMBER SIEBER: They're more expensive?

9 MR. KEMPER: Yes.

10 MR. ARNDT: Paul?

11 MR. LOESER: Yes. I'm Paul Loeser. I'm
12 with NRR.

13 In your questions the safety system cannot
14 be commingled with the control system. They have to
15 have a number of degrees of separation as specified in
16 6308, the one that was talked about earlier where you
17 break it down into blocks where you have functional
18 diversity, equipment diversity, programming diversity,
19 language diversity. And if someone tried to use the
20 same, for example, Intel microprocessor, a 486, for
21 both systems, we would then have to do a fairly
22 intricate diversity and defense-in-depth analysis to
23 see if they were adequately diverse that they could be
24 considered not subject to the same common mode failure
25 or not.

1 MEMBER SIEBER: Okay. That answers the
2 question.

3 MR. LOESER: As far as the channels
4 themselves being separate, two channels in the same
5 system may be exactly identical but have to be
6 physically different. They use the same process and
7 the same software, but they have to be separated.

8 MEMBER SIEBER: Okay.

9 MR. LOESER: We run into problems when
10 people start putting multiple safety functions on the
11 same four channels. And then you have to, again, do a
12 diversity and defense-in-depth analysis to see if you
13 do have a particular kind of accident and combined
14 with that you have a common mode failure under the
15 provisions of branch technical position 19 do you
16 still have enough defense considering this is
17 considered beyond design basis, to adequately cope.

18 MEMBER SIEBER: Okay.

19 MR. LOESER: But those things are taken
20 into consideration when we do our reviews.

21 MEMBER SIEBER: That answers my question.
22 Thank you.

23 MR. KEMPER: Dr. Sieber, with regard to
24 your question about a control system and a safety
25 system on the same microprocessor, there's nothing

1 that specifically prohibits that. And indeed, we ran
2 into that question when we were doing Draft Guide 1130
3 which will eventually become the NUREG Guide 1.152.

4 At first we had a regulatory position in
5 there that said you couldn't do it because there was
6 no barrier that would separate the two. And then
7 somebody from the public mentioned well you could run
8 a safety system on the safe protected mode of a
9 microprocessor and run your control system in the
10 nonprotected mode. And that would be an adequate
11 barrier, to which I guess we conceded that that was a
12 possibility.

13 So you could conceivably do it on the same
14 microprocessor even though, you know, it's --

15 MEMBER SIEBER: Yes, that's sort of the
16 way I read it. And I could picture people trying to
17 jam everything into minimum amount of hardware.

18 MR. KEMPER: At the risk of cutting off
19 conversation, we need to kind of --

20 CHAIRMAN APOSTOLAKIS: Can you tell me the
21 GDC was again, Jack.

22 MEMBER SIEBER: Twenty-four. It's on page
23 23 of the plan.

24 MR. ARNDT: Yes. Right.

25 So basically what we're trying to do is

NEAL R. GROSS

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

1 understand and develop the issues and the procedures
2 and policies and acceptance criteria for these
3 particular kinds of issues. Use communication systems
4 that are most likely to be used for the safety
5 functions, the failures in areas that we're interested
6 in and these kind of issues. And develop realistic
7 ways of doing these kinds of analysis. This project
8 is currently scheduled to start in '07.

9 As we've heard several times today COTS
10 systems are a continuing challenge for us. They're
11 being used extensively in the retrofit and there are
12 both issues associated with the dedication of the
13 systems and how they're interconnected and things like
14 that.

15 Licensees typically qualify COTS systems
16 for nuclear applications through a combination of
17 special tests and inspections, supplier surveys,
18 source verification and performance history. We then
19 do a qualitative review of their dedication.

20 This project, which is going to start on
21 '07, is designed to try and improve that review
22 process. Make it easier, more quantitative, look at
23 the tools that are out there to assess these systems
24 in a box kind of way. Look at issues like model
25 checking, statistical testing these kinds of things

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 and understand what is adequate, what level of
2 information do you need, what kind of samples do you
3 need to take. Do you do a thread audit? If you do a
4 thread audit, how many threads do you have to look at?
5 Try and get better more efficient process for the
6 review of these systems.

7 Okay. The next two projects look at the
8 issues associated with the electrical power for
9 digital systems. In the plan you'll read a couple of
10 LER examples of challenges we've had to the operation
11 of digital systems due to intermediate power, loss of
12 power, voltage fluctuations and things like that that
13 digital systems behaved differently than the analog
14 systems that they replaced.

15 CHAIRMAN APOSTOLAKIS: Yes, they did.

16 MR. ARNDT: And there's been a number of
17 examples of these. So we really want to look at these
18 issues and see whether or not they're going to be a
19 problem. There's been some anecdotal experience that
20 says that there may be some problems. So we want to
21 look at the systems, understand the systems, develop
22 methods to analyze these systems and determine whether
23 or not we need to look at them harder when we do the
24 reviews.

25 Again, this is a relatively low priority

1 but it's scheduled to start in '08. Okay.

2 The next project is a project on a similar
3 line but looking at a different aspect. Digital
4 systems, particularly some of the newer high density
5 digital systems are very sensitive to power quality,
6 particularly issues like zero crossing and things like
7 that, timing issues associated with nuclear power
8 quality. As the systems become more and more
9 dependent on the low voltage memory states, high Cs
10 densities this is something we really want to look at.

11 One of the interesting --

12 CHAIRMAN APOSTOLAKIS: I --

13 MR. ARNDT: Go ahead.

14 CHAIRMAN APOSTOLAKIS: Go ahead. Go
15 ahead.

16 MR. ARNDT: One of the interesting
17 aspects, of course, is that this is not just switching
18 power supplies and things like this. This is
19 everything downstream of the power supplies. And one
20 of the big issues is nonlinear loads. Well, one of
21 the things that's a nonlinear load is digital systems
22 themselves. So for relatively simple systems it's not
23 a big deal. But when you start loading down a power
24 supply with a lot of nonlinear loads like digital
25 systems, you can actually end up with serious issues

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 associated with nonlinear loads.

2 So the research will look at what's
3 currently out there, what's being developed. There's
4 a new IEEE standard 519 that looks at this particular
5 kinds of issue. Again, try to develop methodologies
6 and acceptance criteria, what are the important
7 characteristics and what should we be directing the
8 reviews to look like.

9 CHAIRMAN APOSTOLAKIS: Now, again, one of
10 the issues that has been raised over and over again is
11 what will be the specific contributions of each of
12 these projects that can be used by the agency groups
13 that are actually making decisions?

14 MR. ARNDT: Right.

15 CHAIRMAN APOSTOLAKIS: And one of the
16 questions before you answer that question is how is
17 the agency handling this issue now? Okay. Because
18 we've heard there's a Chapter 7 -- is this issue of
19 THD handled in some way now?

20 MR. ARNDT: There is a power quality
21 requirement, and I don't remember the specific area in
22 Chapter 7. Maybe my NRR colleagues can refresh my
23 memory. But support system type issues are reviewed.

24 CHAIRMAN APOSTOLAKIS: Are reviewed or are
25 not?

1 MR. ARNDT: Are part of the review.

2 CHAIRMAN APOSTOLAKIS: Okay.

3 MR. ARNDT: Paul?

4 MR. LOESER: Paul Loeser from NRR again.

5 Yes, this is an issue now and has been for
6 some time. We have some requirements. For example,
7 we only allow a five percent total harmonic distortion
8 under worse case and items like this. The problem
9 we're beginning to see is that as voltages drop we're
10 now getting into 2.4 volt circuitry whereas in the
11 past it was also 5 volts. Some of it's getting to 1.6
12 and .8 volt. The line thicknesses are getting much
13 thinner. The loads are getting much greater on the
14 items.

15 So while we're handling now with exiting
16 equipment, we're worried that in the future the rules
17 we have in effect may not hold and we need some
18 research or some guidance from somebody to tell us
19 what kind of rules should we have for the future.

20 CHAIRMAN APOSTOLAKIS: Bill, I really
21 think that statements of this type should find their
22 way into the plan. I think it will strengthen it so
23 much. and I urge you when you come before the full
24 Committee in November to do that as much as you can.

25 MR. KEMPER: Okay.

1 CHAIRMAN APOSTOLAKIS: I realize it's
2 only, what, two or three weeks back and you have to
3 have your 15 reviews if you change anything. But it's
4 so important. I mean, judging from past experience
5 with other research plans, most notably the human
6 factors research plan that this Committee reviewed a
7 few years ago, what the members want to see is that
8 kind of motivation. They don't want to see -- I mean
9 this is not the National Science Foundation. We are
10 not trying to advance science for its own sake. We
11 have a regulatory objective. So by citing things like
12 that in all projects ideal even, you know --

13 MR. KEMPER: Right.

14 CHAIRMAN APOSTOLAKIS: -- within reason,
15 I think it's going to go a long way towards convincing
16 people that this is a solid research plan.

17 So please in the presentation, I mean
18 we're going to discuss this tomorrow again. But the
19 presentation in my view, this is one of the most
20 critical aspects.

21 Both of you have thought about it already.
22 I mean, it's not that it's new to you. It's just that
23 some criteria hasn't found its way in the written
24 documents and the slides. Because every time I ask
25 the question, there is an answer.

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 MR. KEMPER: Well, if you'll notice the
2 last three tick bodies embody really the issues that
3 Paul just spoke to. He just gave it a much more
4 passionate and heartfelt description --

5 CHAIRMAN APOSTOLAKIS: Put it in -- he
6 gave it a different spin.

7 MR. KEMPER: And you're absolutely right.
8 Because that's why we're doing this is to support NRR
9 and our stakeholders.

10 CHAIRMAN APOSTOLAKIS: Right.

11 MR. KEMPER: You know, we're not doing
12 research for the sake of just doing research.

13 So good comment. I agree with you.

14 CHAIRMAN APOSTOLAKIS: Yes. So let's make
15 sure that this is one of the top priorities in
16 preparing for the full Committee meeting. Because, as
17 you know, the letter will be written then.

18 MR. KEMPER: Right. Right.

19 CHAIRMAN APOSTOLAKIS: It's very important
20 to be sensitive.

21 Okay, Steve.

22 MR. ARNDT: Yes. And I want to point out
23 one other thing. At the bottom of all these I
24 basically say when the project is going to kick off,
25 if it hasn't already. And one of the things we're

1 trying to do in a very proactive way because we've
2 been less than successful in the past, is for all the
3 new programs we've got the general outline of what the
4 issue is and what we're trying to solve and how we're
5 basically planning on doing it in the research program
6 plan. But the real details will be developed in the
7 statement of work of the program for either in-house
8 work or contract work. And that's going to be done in
9 conjunction with our stakeholders, be it NRR, NMSS or
10 whatever.

11 Operating systems. I'm going to go
12 through this reasonably quickly, even though it's a
13 very complicated issue. And this is an area where
14 it's really a multiple stakeholder issues. There's
15 issues for operating systems in materials, issues in
16 medical devices and fuel fabrication issues in the
17 plant systems, both the safety systems and nonsafety
18 systems. So this is one of the ones that is pretty
19 broad based.

20 As we've been talking. The systems are a
21 lot more complex now than they were in the early days.
22 In the day of the National Academy study many systems
23 didn't have operating systems. They were very simple
24 systems. That's much less so today.

25 In most cases we can get access to the

1 operating system. Hardware less so in the COTS
2 environment. So understanding the characteristics of
3 systems and what potential problems with the
4 characteristics of the system become more and more an
5 issue as we have less information in COTS space. And
6 we really have to understand how this works. We've
7 looked at this in the past and we think we need to do
8 more work in this area.

9 So this program, which is also starting in
10 '08 depending on input from other stakeholders it may
11 get pushed up, but it depends. Right now it's
12 scheduled for '08. We're really looking at issues
13 associated with best practices and failure modes. Try
14 and understand what is an acceptable review standard
15 for these systems. And also looking at what tools are
16 available out there and what the fidelity of the tools
17 are. For example, if the licensee comes in and says
18 we really really looked at our operating system, we
19 understand it, it's not a problem. We've used these
20 tools, we've used this kind of assessment methodology.

21 As Thuy pointed out earlier, there are
22 methodologies out there to look at reliability and
23 availability of these kinds of systems. But until
24 you've looked at that it's very hard to give any real
25 credit to those kinds of systems. So we really need

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 to understand the characteristics of operating these
2 systems and how do you validate them, how do you
3 understand they really are performing properly? So
4 that's really what this project is all about.

5 And now for everyone's favorite issue. As
6 we told you in June, we have a very extensive research
7 program in the area of risk of digital systems and how
8 do you model them and what's in the important modeling
9 characteristics and things like that. And we won't go
10 into that in detail here because we've already talked
11 about it in other places and I don't want to digress
12 anymore than I have to. But the other part of that is
13 how good is our current deterministic process?

14 As EPRI mentioned earlier in the day,
15 there's a lot of issues associated with whether or not
16 that process which was developed a number of years ago
17 is a good process. Now it's a process we have and
18 there's nothing wrong with it. We haven't licensed
19 anything that is not going to be sufficiently diverse.
20 But there's a lot of issues that are being raised by
21 the nuclear industry. So one of the things we want to
22 do is understand whether or not this is the current
23 state of the art for deterministic analysis of
24 defense-in-depth.

25 So basically what we're proposing to do is

1 perform some case studies and look at the way the
2 deterministic analysis is laid out in 6303. Review
3 the risk insights, both our own risk insights and
4 EPRI's risk insights and verify from a deterministic
5 standpoint whether or not this is the best we can do.

6 So that's the primary aspect of this. And
7 as I mentioned, this project is going to start later
8 this year.

9 MR. KEMPER: Yes. For example, a licensee
10 right now has an application that NRR is reviewing
11 that they propose to a certain strategy for their
12 design configuration with regard to diversity and
13 defense-in-depth. That's kind of the baseline. That's
14 where we're starting from because we don't have any
15 other specific case studies, if you will, that we can
16 draw from to make judgments, if you will, and provide
17 that feedback to the licensee. So we're thinking for
18 at least the generically qualified platforms it would
19 be good to perform these studies and come up with some
20 numbers ourselves. You know, or some conclusions
21 ourself which what's the best fit, if you will, from
22 a topology an a design strategy of these I&C systems
23 for various safety applications.

24 MR. GUARRO: Just trying to understand. Is
25 essentially the intent to identify the improvements to

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 the deterministic approach that would seem to satisfy
2 some risk-informed criteria as well. Because you've
3 mentioned risk, so I'm' trying to understand what the
4 connection is.

5 MR. ARNDT: The objective of this is
6 simply that last bullet there, to verify from a
7 deterministic standpoint the existing criteria is the
8 best we can do in a deterministic space.

9 The bullet above that is basically just to
10 learn from whatever information is out there, both
11 what the licensees have submitted, what's been done in
12 foreign applications and what if any information is
13 available from risk insights. Things that people have
14 looked at, things that people have done that will help
15 us understanding whether or not the deterministic --

16 MR. GUARRO: Some of the objections that we
17 have heard are based on risk considerations of some
18 sort.

19 MR. ARNDT: Right.

20 MR. GUARRO: So trying to figure out if
21 that fits into the formulation of some other or
22 improved deterministic formula.

23 MR. ARNDT: As I stated a few minutes ago,
24 we haven't kicked this off so we don't have the exact
25 details yet. But the idea is simply to look at

1 everything that's out there that we are aware of that
2 we're knowledgeable about to try and understand if
3 what we're currently doing is the best we can do in
4 deterministic space.

5 So, for example, looking at the EPRI
6 study. They've pointed out that there are some issues
7 that may not be covered in a bounding Chapter 15 type
8 analysis. That's something that we want to know if
9 we're going to look at whether or not this is the best
10 deterministic way of doing the deterministic analysis.
11 If not capturing something that's important or if we
12 are worrying about things that are not important from
13 a deterministic standpoint, then we want to look and
14 see whether or not we can do better. That's truly the
15 point of having that there.

16 MR. KEMPER: Let me just try to run
17 through a case study for example just off the top of
18 my head.

19 A licensee could propose to deploy the
20 same hardware throughout his plant, primary and
21 secondary. Okay. If you assume common mode failures
22 of that equipment and then you run the thermal
23 hydraulic analysis using best estimate calculations
24 per BTP-19 -- we intend to go look at the effects of
25 plants in a deterministic role. Now it was not

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 written from a probabilistic perspective because
2 that's the program that we have right now to deal
3 with. You could choose a different strategy. You
4 could choose to combine the RPS and the ESFAS. You
5 could choose to combine the RPS, ESFAS and your post
6 monitoring system. Any number. You know, you can just
7 pick them. And the idea is we want to run through a
8 few of those case studies and see if we can establish
9 for ourselves what is the best fit in terms of a design
10 philosophy for using the same microprocessors, for
11 using the same software, that sort of thing.

12 MR. ARNDT: The other, if you go up one
13 tick mark, one of the real issues here is in 6303
14 there's a set of rules associated with how you put
15 together blocks, how you put together coping
16 strategies and things like that. When we review this,
17 we've got to make some assumptions about how that
18 makes sense and the licensee has got to make some
19 characteristics. You put a line around this block,
20 you put a line around that block. But one of the
21 things we want to do is as Bill just mentioned is do
22 some case studies. Do it ourselves to understand what
23 makes sense and what doesn't make sense so we can have
24 a definitive technical basis to go back and say no,
25 you really can't do that because if you do that, you

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 run into problems. And we're not willing to accept
2 that.

3 CHAIRMAN APOSTOLAKIS: Okay. Let's move
4 on.

5 MR. ARNDT: Okay. So those were the
6 programs that were highlighted in the research program
7 plan.

8 CHAIRMAN APOSTOLAKIS: Very good.

9 MR. ARNDT: As Bill mentioned, as things
10 change we get requests for additional programs from
11 NRR, MNSS, they'll get thrown into the budget
12 prioritization process and they may bubble to the top.
13 But that's currently where we are on those issues.
14 And we will continue to work these programs in
15 conjunction with our colleagues in MNSS and NRR to try
16 and get --

17 CHAIRMAN APOSTOLAKIS: Very good.

18 MR. ARNDT: -- the best product for our
19 customers.

20 MR. KEMPER: Okay. We'll we're getting
21 close to being back on track. All right.

22 Okay. Christina Antonescu is going to
23 provide a presentation of environmental stressors, as
24 we promised earlier, Section 3.1.1.

25 CHAIRMAN APOSTOLAKIS: Now, Christina, you

NEAL R. GROSS

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

1 have something that's against you before you even sit
2 down. It's 5:10 after a long day and you have 27
3 slides.

4 MS. ANTONESCU: No, they are backup.

5 CHAIRMAN APOSTOLAKIS: What, 20 of them
6 are backups?

7 MS. ANTONESCU: Yes.

8 MEMBER SIEBER: Yes, there's only one real
9 slide.

10 MS. ANTONESCU: Only 18 I believe are--

11 CHAIRMAN APOSTOLAKIS: Can you be nice?

12 MS. ANTONESCU: I will be nice.

13 MEMBER BONACA: You should be nice to her
14 and tell her we like what you do, and then she'll be
15 nice to us.

16 CHAIRMAN APOSTOLAKIS: And then we'll be
17 done in a minute, huh?

18 MEMBER BONACA: Right.

19 MS. ANTONESCU: All right.

20 CHAIRMAN APOSTOLAKIS: This is a very
21 unusual color for the heading. I mean that's nice.

22 Go ahead.

23 MS. ANTONESCU: So my name is Christina
24 Antonescu. I've been working in the I&C group for the
25 last 15 years. And I would like to discuss with you

NEAL R. GROSS

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

1 today the status of our research on environmental
2 stressors and the impact on instrumentation and
3 control technology.

4 I have with me Richard Wood from Oak Ridge
5 National Lab. He has been principal investigator for
6 our projects on environmental stresses. He has a
7 background in the nuclear engineering and he has over
8 20 years experience with the -- power plant.

9 And contributing on the discussion, I also
10 have Paul Ewing, he's somewhere in the back from Oak
11 Ridge National Lab. He is a principal investigator
12 for our electromagnetic compatibility and lightning
13 protection projects. His background is electrical
14 engineering. He has 25 years experience with EMC
15 radio frequency transmission.

16 So our research on the environmental
17 stressors it's currently addressing three main topics.
18 The lightning protection one. The Committee recently
19 reviewed DG-1137 on lightning protection, so I will
20 not repeat the details of the guide in this
21 presentation. But it was presented to ACRS on July
22 6th of this year and reviewed by the ACRS in July. And
23 we're ready to issue the draft guide as a final guide
24 by the end of this year sometime as Reg. Guide 1.204.

25 The second main topic on environmental

1 stressors is the environmental compatibility for mild
2 environments. DG-1077 was developed in response to a
3 user need from NRR. And the need for DG-1077 is to
4 provide an all in one roadmap for acceptable practices
5 for the applicant. Previously the reg guide on mild
6 environment qualification was distributed among
7 several documents. So the Committee has seen and
8 approved DG-1077 before, but its release was delayed
9 to allow the revised IEEE standard to be reviewed and
10 to address some scope consideration which is focused
11 on mild environment rather than harsh and mild
12 environment.

13 So I will discuss the status of the DG-
14 1077 in my presentation.

15 And the third main topic is the
16 electromagnetic compatibility. And EPRI has requested
17 that NRR consider relaxation of the text limit for
18 series 114 because it is substantially higher than the
19 limit in certain frequency ranges. So the reasons for
20 the higher limit in Reg. Guide 1.180 and past versions
21 of the EPRI guide is that some plant measurements
22 taken by EPRI were very high. And EPRI had committed
23 to bound those measurements with its susceptibility
24 limits, but now suggests that it's analysis of the
25 measurement was flawed. So my presentation will

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 describe the issue on what has been done so far.

2 So as stated, the Committee has seen the
3 DG-1077 before, however it's release was delayed to
4 permit updating endorsement of the most recent
5 standard and to enhance the guidance by sharpening its
6 focus.

7 DG-1077 was presented in February of 2003.
8 ACRS approved it for release and the final effective
9 guide was granted --

10 CHAIRMAN APOSTOLAKIS: What does that
11 mean, "final effective guide?" That's new terminology
12 to me.

13 MS. ANTONESCU: The final guide was
14 granted or --

15 CHAIRMAN APOSTOLAKIS: So we approved it
16 and now you guys say no we're not going to publish it,
17 we're going to go back and do some more work?

18 MS. ANTONESCU: Yes. And I'm going to let
19 you know what the reason is. One of the reasons is to
20 permit updated endorsement of IEEE standards 323,
21 which was released in 2003. And then we just -- the
22 scope of it was also changed from mild and harsh to
23 mild only.

24 CHAIRMAN APOSTOLAKIS: Okay.

25 MS. ANTONESCU: However, following the

1 ACRS review of DG-1077 NUGEQ, that's the Nuclear
2 Utility Group on Equipment Qualification, requested
3 that the pending update of IEEE 323 be considered for
4 endorsement. So that's the 2003 version. So in
5 response finalization of DG-1077 was delayed so that
6 the standard could be reviewed. And IEEE 323 was
7 released on September 11, 2003. A review was
8 conducted by our office with the help of Oak Ridge.
9 And DG-1077 has been revised and is now DG-1142.

10 So because of the scope reduction of this
11 DG-1077 we plan to release it for public comment
12 again. And it will be designed as DG-1142. For
13 simplicity I'll refer to it as DG-1077 in my
14 presentation.

15 So IEEE 323-2003 is very similar to IEEE
16 323-1983. The primary difference involves practices
17 for harsh environment qualification. Provisions were
18 added to IEEE 323-2003 to allow condition monitoring
19 to be used to support on-going qualification. Changes
20 were made to address previous NRC objections, in
21 particular of dual transient as part of the DBA test
22 profile. And some wording changes were introduced to
23 add clarity, but in some cases they have introduced or
24 exacerbated some issues regarding harsh environment
25 qualification.

NEAL R. GROSS

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

1 So the guidance on documentation for mild
2 environment remains the same in both versions. And is
3 consistent with regulatory practice.

4 The qualification practices in 323-2003
5 are appropriate for mild environments with some
6 clarification conditions which I'm going to cover in
7 a few minutes. And the technical basis for endorsing
8 IEC 60780 remains ineffective and are equivalent to
9 the practices in IEEE 32-2003. But with reduced scope
10 of DG-1077 which limits the endorsement to mild
11 environment application only.

12 So endorsement of both standards is
13 limited now for mild environment for safety related
14 computer-based I&C systems.

15 So let me remind you what DG-1077 is. What
16 does it do? It endorses qualification practices in
17 323-2003 and IEC 60780 as acceptable for application
18 to safety related computer-based I&C systems located
19 in mild environments.

20 And where does it apply? It applies for
21 new and modified --

22 CHAIRMAN APOSTOLAKIS: Excuse me, did I
23 miss, but what is a mild environment?

24 MR. WOOD: This is Richard Wood.

25 It's an environment that does not have a

1 design basis accident condition. So for harsh
2 environments there's a substantial change under an
3 accident condition. For a mild environment, the
4 environment doesn't change substantially under the
5 normal or abnormal conditions.

6 MEMBER SIEBER: It presumes that it is in
7 the containment during a LOCA?

8 MR. WOOD: Yes.

9 MEMBER SIEBER: So you have pressure
10 temperature radiation spray, chemical spray.

11 MS. ANTONESCU: EQ would be --

12 CHAIRMAN APOSTOLAKIS: That's mild?

13 MEMBER SIEBER: That's harsh.

14 CHAIRMAN APOSTOLAKIS: Oh, harsh.

15 MS. ANTONESCU: Harsh.

16 MEMBER SIEBER: Mild is like in here.

17 MR. WOOD: Normal operation.

18 CHAIRMAN APOSTOLAKIS: Less than that.

19 MS. ANTONESCU: Harsh would have to be --
20 the qualified language has to be established for DBA.

21 CHAIRMAN APOSTOLAKIS: Okay.

22 MS. ANTONESCU: So where does it apply?
23 I already said that.

24 What does it provide? It addresses unique
25 characteristics of computer-based I&C systems as well

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 as acceptable evidence for mild environment
2 qualification.

3 What has changed in DG-1077? The revision
4 of the draft guide involves endorsing, again, the
5 updated IEEE standard in 2003 and also the current
6 international standard.

7 The regulatory revise scope and provides
8 pointers to guidance on key related issues.

9 And the reduced scope to focus
10 specifically on mild environment qualification of
11 computer-based I&C systems. Thus since the revised
12 DG-1077 only applies to mild environment qualification
13 of computer-based I&C system, the standards are only
14 endorsed for mild environment application by this
15 guide. As a result, all previous positions related to
16 harsh environment qualification were deleted and
17 replaced by position to point to Reg. Guide 1.89 which
18 is for harsh environment as the prevailing guidance on
19 qualification on those environments.

20 So it was determined that harsh
21 environment qualification should remain the exclusive
22 domain of Reg. Guide 1.89.

23 So because of the revision we proposed
24 that the guide be released for another round of public
25 comments.

1 MEMBER SIEBER: Did you ask us to review
2 it before you released it?

3 MS. ANTONESCU: We will.

4 MEMBER SIEBER: Okay.

5 MS. ANTONESCU: That's our intent.

6 MR. KEMPER: That's coming. That's the
7 next step.

8 MEMBER SIEBER: Okay.

9 MR. KEMPER: We're going to send it to NRR
10 and let them review it and the next step will --

11 CHAIRMAN APOSTOLAKIS: That's you, right?

12 MR. KEMPER: Yes. Bill Kemper.

13 MEMBER SIEBER: Yes.

14 MS. ANTONESCU: So what are the position
15 of DG-1077? We have covered its endorsement of
16 standards, so now let's look at the enhancement
17 exceptions.

18 DG-1077 provides one enhancement to IEEE
19 323-2003 and IEC 60780 to address unique
20 characteristics of microprocessors. And the
21 enhancement is for computer that must be functioning
22 or the software has to be executing while being
23 tested.

24 The second, the system level effects must
25 be considered as a whole, and then test as parts and

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 confirm no acceptable cumulative effects. So that
2 what I mean is use analysis to supplement testing.

3 And the exception, we don't have enough
4 the exception -- at least one exception that we are
5 looking at is that enough documented evidence must be
6 available to show qualification. So we're taking
7 exception to clause 7.1. And 7.1 says that very
8 little evidence of qualification needs to be
9 documented for mild environments. And we're taking
10 exception to that, and that's why we're consistent now
11 with clause 7.2, which specifies full documentation of
12 qualification processes including test plans and
13 results. This documented evidence necessary for the
14 Staff to adequately confirm that the functioning
15 complex computer system is in fact qualified for the
16 environment in which it was operated.

17 So the pointers, there are two pointers
18 that we have. And one is to Reg. Guide 1.180 on my
19 guidance that we'd retained from our previous
20 revisions. And another pointer to Reg. Guide 1.89 on
21 harsh environment qualification guidance. And this
22 replaces all previous harsh environments qualification
23 position in DG-1077. We just point now everything to
24 Reg. Guide 1.89.

25 Now I'm going to look at the last topic on

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 electromagnetic compatibility and change the subject.

2 The industry response to NRC on its
3 regulatory guidance on EMC nuclear power plant has
4 been generally positive. Regulatory guidance on EMC
5 began with review and acceptance of EPRI TR-2323 with
6 stipulation in an SER in 1996. Reg. Guide 1.180 was
7 released in 2000 and recognized the SER and its
8 acceptance of TR-2323. Then Reg. Guide 1.180 was
9 updated in 2003 to incorporate changes in the
10 acceptable EMI/RFI practices. TR-2323 has been
11 updated over the years, but these updates have not
12 been endorsed by NRC since similar practices are
13 included in Reg. Guide 1.180.

14 So the industry response to regulatory
15 guidance on EMC has been generally positive. However,
16 there is one significant issue that concerns the
17 industry, and that is CS114 operating envelope and the
18 feeling that it's too harsh. So I'm going to tell you
19 the problems from EPRI's point of view.

20 EPRI has requested that NRC review CS114
21 operating envelope in Reg. Guide 1.180 Rev. 1 because
22 the envelope was based on EPRI's planned measurements
23 and the measurements were flawed. CS114 is a high
24 frequency conducted susceptibility test and it has
25 proven problematic for nearly all equipment tested to

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 date. And very few pieces of the equipment have
2 passed the test without being redesigned. This is a
3 very harsh test.

4 So CS114 operating envelope in Reg. Guide
5 1.180 actually incorporated plant data obtained from
6 EPRI and now EPRI says its measurement and the
7 original analysis of plant data were flawed.

8 So EPRI says that CS114 is a continuous
9 wave test and its operating envelope should be based
10 on continuous wave data, not the transient data. And
11 we do have separate power surge susceptibility testing
12 for that, which is IEEE 662.41.

13 So it then follows that CS114 operating
14 envelope in Reg. Guide 1.180 Rev. 1 is subsequently
15 flawed. The result is that EPRI wants to see the
16 operating envelope changed.

17 So to explain where we are, I'm just going
18 to give you some background.

19 EPRI collected its conducted emission data
20 in 1994 in seven plants and it captured power
21 transients. So the subsequent EPRI data profile then
22 showed high conducted emission levels in the plant.

23 So Research was only infrequently allowed
24 to make limited conducted emission measurements in
25 plants because of their intrusive nature and our data

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 profile showed lower levels. Because of the limited
2 measurements our data had a high degree of measurement
3 uncertainty.

4 And how does this effect Reg. Guide 1.180?
5 We incorporated the EPRI data into a development of
6 our CS114 operating envelope. We started with
7 operating envelope for the military ground facility in
8 461D and then addressed it to incorporate EPRI plant
9 data so that we could be consistent with the SER based
10 on EPRI's TR-102323 guide. Our goal was to ensure
11 that safety related equipment could withstand ambient
12 conducted emission in plants, and we assumed that EPRI
13 data was relevant. And we have documented the
14 technical basis in NUREG/CR-6431.

15 So of course EPRI is now revising its data
16 collection analysis rationale and they are now saying
17 their conducted emission data should not have included
18 captured power transients because we have a separate
19 test for that. Because they're addressed by power
20 surge susceptibility testing IEEE C62.41 and C62.45.
21 Their argument is that CS114 operating envelope was
22 not intended to be tested on conducted emission
23 measurements, but rather should be based on a radiated
24 emission environment. And this is to say that
25 radiated emissions will couple onto signal and power

1 leads and interference with the normal operation of
2 the piece of the equipment. Hence, EPRI is saying
3 that the original rationale was flawed and the SER
4 operating envelope based on 102323 was then also
5 flawed.

6 And I'm illustrating visually what the
7 issue is. And we have here a comparison of the
8 operating envelope for Reg. Guide 1.180 Rev. 1 and
9 EPRI TR-102323 and Rev. 3.

10 The NRC operating envelope is shown in
11 red. The EPRI envelope that have been accepted in
12 Rev. 0 are shown dark green. And the EPRI operating
13 envelope that they are recommending is showing blue.

14 So note that the power and signal
15 operating envelope is the same for 102323. This is
16 based on EPRI's assumption that the radiated emissions
17 will couple onto both power and signal leads in the
18 same manner. Thus, the operating envelope should not
19 be different.

20 Also note that Rev. 2 EPRI envelopes are
21 shown in black and actually separate the power and
22 signal lead envelopes.

23 Also you can see that the Reg. Guide and
24 EPRI Rev. 2 envelopes for power leads are very
25 similar.

1 So the problem area that we're looking at
2 is this triangle shown in light green. For most
3 equipment on this is the frequency range below --
4 where the existing operating envelopes have problem to
5 be stringent and hard to pass.

6 So in summary, we have agreed to look into
7 EPRI's request and we have reviewed the information
8 received from EPRI regarding the CS114 operating
9 envelope and in the TR-102323 guide. And we are now
10 investigating the rationale for EPRI CS114 operating
11 envelope and if justified, will develop a revised
12 position on CS114 operating envelope.

13 So we will update the Reg. Guide based on
14 the results of the investigation and the revised
15 position.

16 MEMBER SIEBER: Are you planning to get
17 more data or are you going to use EPRI's data?

18 MS. ANTONESCU: If necessary. I'm not
19 sure. Depending on how we're going to -- what we're
20 going to find out or what our rationale will be or
21 what we need to justify.

22 MR. WOOD: The real issue is whether or
23 not the argument that's presented is a compelling
24 technical argument. If not, then it may require some
25 more measurements.

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 MEMBER SIEBER: But you aren't really
2 contesting the data that became available at plants?
3 It's how it's applied?

4 MR. WOOD: We haven't had an opportunity
5 to look at the details of the EPRI data. So we're not
6 contesting their argument. What we're trying to do is
7 figure out whether their argument fully explains all
8 the potential sources.

9 MEMBER SIEBER: Okay. They're contesting,
10 your arguing?

11 MR. WOOD: Well, they're contesting their
12 previous argument.

13 MS. ANTONESCU: Because we have to take
14 theirs --

15 MEMBER SIEBER: If you have to argue, it's
16 best to argue with yourself.

17 MR. WOOD: I think so.

18 CHAIRMAN APOSTOLAKIS: Any other comments
19 or questions from people at the table?

20 Thank you Christina and Richard.

21 MEMBER SIEBER: Okay.

22 CHAIRMAN APOSTOLAKIS: Appreciate it.
23 We'll see you tomorrow, Christina, I suppose.

24 MS. ANTONESCU: Yes, see you tomorrow.

25 CHAIRMAN APOSTOLAKIS: With few slides.

NEAL R. GROSS

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

1 MS. ANTONESCU: Fewer slides. All right.
2 I'll try to shorten tonight.

3 MEMBER SIEBER: This was actually very
4 good. This was very good.

5 MS. ANTONESCU: Thank you.

6 CHAIRMAN APOSTOLAKIS: You raise
7 expectations by showing the backup slides, then you
8 use a topical list.

9 MS. ANTONESCU: Thank you.

10 CHAIRMAN APOSTOLAKIS: That was a good
11 move.

12 MS. ANTONESCU: Thank you.

13 CHAIRMAN APOSTOLAKIS: Okay. As I said
14 earlier, judging from the experiences we've had with
15 the human factors research plan where the developers
16 had to come back two or three times to us, and also
17 from some of the comments that we've heard here in the
18 last two or three meetings, a separate meeting, it is
19 extremely important to show how a research plan --
20 what's the rationale. How it relates to what we are
21 doing already and why do we need something new, you
22 know, to supplement or compliment or improve on what
23 we're doing already.

24 Every time I asked a question, you guys
25 have been answering. So you have thought about it. But

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 what has not happened is that that kind of argument is
2 not in the plan and in your presentations usually you
3 ignore it. So what I think you should do is really
4 focus on it and make a big deal out of it when you
5 come back in November. Because we'll write -- the
6 letter will be, as I understand it, on the plan not on
7 individual projects even though you guys described a
8 lot of them. We'll wait for that for the future after
9 you have reasonable progress.

10 So as I was thinking about this last
11 night, because I do think that there's a lot of good
12 stuff in the plan, I was trying to think how can one
13 show what you are doing and how what you are doing
14 fits in the bigger picture. And the bigger picture
15 that came to my mind was the reactor oversight
16 process.

17 Now, I want to say up front what follows
18 is not something that you must do. We are not
19 recommending that you do it. We ourselves, you know,
20 are not sure that everything there is on solid ground.
21 But it's a thought.

22 This diagram, by the way, do you have it
23 in front of you or can you look it?

24 MR. KEMPER: We can look at it. Yes.

25 CHAIRMAN APOSTOLAKIS: Well, you can have

1 copies. It's over there. They may want to take notes.

2 MR. KEMPER: We have a copy here.

3 CHAIRMAN APOSTOLAKIS: Yes. Mike, you
4 have a copy?

5 So the diagram was of tremendous value to
6 the people who developed the reactor oversight process
7 because they were able to communicate to the world at
8 large, in fact, what the agency cares about. So here
9 is some thought.

10 The overall mission of the agency is the
11 top box. Public health and safety. And I put as a
12 result of severe nuclear reactor operation with
13 different color in parenthesis because you probably
14 had to drop that because you are adding now an NMSS.
15 The strategic performance areas were reactor safety,
16 radiation safety workers, safeguards and then I put in
17 purple there NMSS.

18 Now the cornerstones are exactly the same
19 from the reactor oversight process. Now the purpose
20 of those is really to see, to help you communicate to
21 the reader or the viewer or the reviewer what kinds of
22 systems you're talking about and what parts of the
23 broader picture they're effecting. You will need some
24 cornerstones for the NMSS, I guess, and the safeguards
25 I'm not sure how much you can put there. But, again,

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 this is their idea. In fact, some of my colleagues
2 have doubts that even the cornerstones for reactor
3 safety are appropriate in your case.

4 So the message here is don't take this
5 literally, okay. Don't take it literally all by --
6 you know, he said mitigating systems, I have to have
7 something on there. No, no, it's the idea.

8 Then under each one, and I think this
9 comes really from the questions that have been raised,
10 let's say I'm giving as an example the mitigating
11 systems cornerstone, okay? But you can have arrows
12 going to barrier integrity and so on. What is the
13 function and the unique characteristics of the system
14 that we are dealing with in this project, this
15 particular 6.5.3.2? As an example, what was said
16 today. It's just a simple actuation system. That's
17 important to know that you are dealing with a simple
18 actuation system and not trying to control the area.

19 How is the agency reviewing it now? What
20 is the current state of the art, in other words, or
21 the practice? Are we reviewing them? Are we
22 approving these things, disapproving and so on.

23 The third bullet -- again, even these
24 bullets should be subject to revision and so on. Why
25 do you want to change it? I mean, you know, you

1 remember several months ago Mr. Calvert told and we
2 are happy with what we have. Well, if you are happy,
3 then why are we spending money doing anything, you
4 know. Today we got different responses from the NRR
5 representative. Okay. Every time I ask why you want
6 to do that -- I forget your name. I'm sorry.

7 MR. LOESER: Paul Loeser.

8 CHAIRMAN APOSTOLAKIS: Paul stood up and
9 said for such-and-such a reason and made perfect sense
10 to me. That kind of thing would be nice to
11 communicate.

12 Then the heart of the matter, and that was
13 really the fourth bullet is what killed the human
14 factors plan several times. If you are successful in
15 project X, how are you going to change the present
16 situation? Are you going to shorten the review time
17 and make it more efficient? Are you going to enhance
18 it and bring in more staff and make it more effective?
19 Are you anticipating what's going to happen, as we
20 said today, so you want to be prepared and understand
21 it better? Can you be a little bit specific in other
22 words. You know, this is really what we expect.

23 Now the last bullet was -- I'm not sure
24 that I could do that either. Would there be any
25 metrics for the previous staff? I find that very

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 difficult to do many times, most of the time. But
2 just in case.

3 But this again gives you the thrust of the
4 thing. I mean for each project you answer these or
5 similar questions and place them in the context of a
6 bigger picture, then it seems to me we are really well
7 on our way.

8 And then at the bottom, of course, the
9 cost cutting issues that you guys have a lot of. And
10 that's fine. You can say, look, what we're doing here
11 will effect, you know, detecting that an initiating
12 event has occurred. At the same time we will look at
13 the mitigating system. In fact, the beta factor
14 example from EPRI was one example of that. You know,
15 you have a loss of feedwater flow and then the
16 argument was that 25 percent of the time it's the
17 turban, and that may be coupled with the mitigating,
18 the safety system. Great. Okay. So we're doing this
19 project and we're affecting that.

20 I don't know. Is wireless technology
21 primarily related to emergency preparedness? Could
22 be, huh. I don't know about barrier integrity. But
23 that helps the reviewer understand a little better
24 what we're talking about and where.

25 MEMBER SIEBER: Part of this work is

1 already done. If you look at page 125 there's a lot of
2 pages like that. You already have which supported
3 strategies are for each project. They're already
4 listed.

5 MR. ARNDT: Yes. And some of that --

6 CHAIRMAN APOSTOLAKIS: If I under the
7 impression that you guys had not even thought about
8 it, I wouldn't raise it. Because I know you can't do
9 this in three weeks.

10 MR. ARNDT: Right.

11 CHAIRMAN APOSTOLAKIS: But I know you have
12 done it. It's just that you haven't documented it in
13 a way that other people can appreciate that you've
14 done it.

15 MR. ARNDT: Yes.

16 MR. KEMPER: Well, if I could -- Bill
17 Kemper here.

18 The supportive strategies, though, again,
19 is out of the strategic plan.

20 MEMBER SIEBER: Right.

21 MR. KEMPER: It's not a one-one mapping
22 that you can do to the IOP. But this is just a
23 different way of slicing the agency's mission.

24 CHAIRMAN APOSTOLAKIS: I'm sorry. Jack.

25 MEMBER SIEBER: I think the most important

1 thing is that fourth bullet.

2 CHAIRMAN APOSTOLAKIS: Yes.

3 MEMBER SIEBER: There's the direction of
4 the agency and here's how these programs fit in.

5 MR. ARNDT: Right. Okay. And that's a
6 very good comment. And we can certainly do that in
7 most, maybe not all, but most of the cases.

8 CHAIRMAN APOSTOLAKIS: Okay. But
9 especially in the presentation

10 MR. ARNDT: Right. Some of our programs
11 are quite -- are individual technology focused. How
12 do we get ready or do we do a better job of reviewing
13 a particular piece of hardware or piece of software.
14 And many of them are crosscutting type issues. How do
15 you model --

16 CHAIRMAN APOSTOLAKIS: But when you see a
17 better job, you must have something in your mind.

18 MR. ARNDT: Yes.

19 CHAIRMAN APOSTOLAKIS: Why do you need to
20 do a better job? I mean, in what sense? Do we need
21 to understand it better?

22 MR. ARNDT: Yes. And there's a set of
23 things that we hope to accomplish, and that's what you
24 want us to articulate better?

25 CHAIRMAN APOSTOLAKIS: And in many of

NEAL R. GROSS

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

1 these you are very explicit.

2 MR. ARNDT: Right.

3 CHAIRMAN APOSTOLAKIS: This project will
4 result in tools as follows: A, B, C, D. That's great.

5 MR. ARNDT: Right.

6 CHAIRMAN APOSTOLAKIS: In other places
7 you're not so explicit.

8 MR. ARNDT: Right. In some cases we simply
9 didn't articulate as well as we can. Some cases we
10 don't know --

11 CHAIRMAN APOSTOLAKIS: Well, this is a
12 document that is evolving.

13 MR. ARNDT: Right.

14 CHAIRMAN APOSTOLAKIS: I mean, this is
15 just an extra thought to help you --

16 MR. ARNDT: And I appreciate that.

17 CHAIRMAN APOSTOLAKIS: -- communicate
18 better what you have already done in my view.

19 MR. ARNDT: Right.

20 CHAIRMAN APOSTOLAKIS: Most of the time,
21 anyway, you have done it.

22 MR. ARNDT: Okay. Let me ask another
23 question that will hopefully help the presentation.

24 We're scheduled, I think, an hour and a
25 half --

1 CHAIRMAN APOSTOLAKIS: On what?

2 MR. ARNDT: Next --

3 MR. KEMPER: November.

4 MR. ARNDT: -- November.

5 MEMBER SIEBER: The full Committee.

6 MR. ARNDT: We can structure that anyway
7 that you think is going to be best for the Committee.
8 Obviously, there's some things we want to say. One
9 way we can do it is to review very quickly like I did
10 for environmental stressors this afternoon all the
11 programs. That may not be the most effective use of
12 time.

13 CHAIRMAN APOSTOLAKIS: In my view it is
14 not.

15 MR. ARNDT: Okay.

16 CHAIRMAN APOSTOLAKIS: I would structure
17 it around something like this. Here's the big
18 picture, we have six areas right around. This is how
19 they fit into this.

20 MR. ARNDT: Right.

21 CHAIRMAN APOSTOLAKIS: You know, this is
22 the way it's being done now. We need to better a job
23 because of A, B, C, D and here is what we're offering.

24 Now to go over all the projects will
25 probably -- I don't know. It's over kill.

NEAL R. GROSS

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

1 MR. ARNDT: Yes.

2 MR. KEMPER: We've already done that
3 anyway. In May that's what we did, right? That's why
4 we're here.

5 MEMBER BONACA: But you have those tables,
6 you know, in page 11 with all your programs, etcetera,
7 so you have really logical step.

8 MR. ARNDT: Sure. We can structure it in
9 that way and then maybe use a couple of examples

10 CHAIRMAN APOSTOLAKIS: Absolutely.

11 MR. ARNDT: That go to particular issues.

12 MEMBER BONACA: Because you do have a
13 series of tables with all the --

14 CHAIRMAN APOSTOLAKIS: And don't hesitate.
15 You know, this morning I noticed -- was it the
16 morning, or whatever? That -- and I appreciate that.
17 I mean, you really don't want to criticize what your
18 colleagues of NRR are doing now and say we need to do
19 this because you're not doing right. But at the same
20 time to say that what we're doing now is fine and
21 excellent and we're spending a million dollars to
22 improve it, I mean -- so it's okay. I mean, it's the
23 state of the art. How are we doing it now? Maybe we
24 are doing it overly conservative because that's what
25 you do if you're a regulatory, right?

NEAL R. GROSS

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

1 MR. ARNDT: Right. Well, and it's --

2 CHAIRMAN APOSTOLAKIS: But I think the
3 fundamental thing that this is a new technology, new
4 failure modes and we're all as a community trying to
5 understand it is a very powerful argument in my view.

6 MR. ARNDT: Yes. And it also has the
7 virtue of being true.

8 CHAIRMAN APOSTOLAKIS: Which sometimes
9 helps in my estimation.

10 MEMBER BONACA: You know one thing that
11 certainly struck me was well we were discussing common
12 mode failure, you know, because we're left to question
13 in our mind. And then I saw the table that you
14 developed, which is the events that took place.

15 MR. ARNDT: Right.

16 MEMBER BONACA: You know, to me is one of
17 the most convincing arguments. Here are the facts that
18 whatever the estimation is going to be right now,
19 etcetera, there are issues that we have to deal with
20 in advance out there in the field that have been
21 cropping up.

22 MR. ARNDT: Yes.

23 MEMBER BONACA: And that in and of itself
24 to me is justification for work, in a goal sense of
25 course. And I'm saying that which you can address

1 also the examples, of not giving examples to us, but
2 I think that gives justification to the plan.

3 I would like to add one thing that, you
4 know, that I am in general am quite impressed with the
5 plan because here we are now, you know, performing our
6 review of the RES research plan and here we're
7 scheduled to develop one. And I wish there was a
8 document like this for every area we're looking at.
9 And there isn't.

10 MR. ARNDT: Well, you're partially
11 responsible for it because as you recall the first
12 version of this was as a answer to the mass
13 recommendations that were part of this Committee's--

14 MR. KEMPER: But thank you. We appreciate
15 your help on that.

16 MEMBER BONACA: I think it's a good base
17 to start it and I think it's going to help you through
18 the next few years very years.

19 MR. KEMPER: Well, we've put a fair amount
20 of effort trying to vet this with our stakeholders.
21 You know, since we first met in May, quite honestly.
22 And I think it's a much better product now as a result
23 of that than it was when we started out four or five
24 months ago.

25 MR. ARNDT: Right.

1 CHAIRMAN APOSTOLAKIS: Jack?

2 MEMBER SIEBER: I'm curious about one
3 thing. Will you prepare the research plan in such
4 detail? Obviously you have to think about it. Did it
5 actually in preparing the plan change your conception
6 of what it is you should be doing or did you already
7 have fixed in your mind I'm going to do these things,
8 all I have to do is write it down?

9 MR. ARNDT: It's a little bit of both.

10 MEMBER SIEBER: Okay. I sort of sensed
11 that.

12 MR. KEMPER: It's an iterative process.

13 MR. ARNDT: It's very much an interactive
14 process. Because we get -- and I'll mention this a
15 little bit tomorrow morning when I talk about the
16 emerging technology section. But part of the process
17 of planning, particularly out year planning, is
18 figuring out where we want to be.

19 MEMBER SIEBER: Right.

20 MR. ARNDT: And that involves polling our
21 stakeholders, talking to ourselves, looking at the
22 research that's out there and all the other areas.
23 Some of us are involved in proposal reviews for DOE
24 and other areas. So you get a lot of different things
25 and you work through the issues. And some of them

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 come up as we look through the data and issues and
2 things like that.

3 And as unpleasant as putting one together
4 one of these things is, it's kind of useful to do it
5 every few years simply to force yourself to do that
6 kind of thinking.

7 As you know, we did our first one, this is
8 the second version. We're planning now in the future
9 to do yearly updates, which is a little less resource
10 intensive.

11 MEMBER SIEBER: Yes.

12 MR. ARNDT: But also having that continual
13 update both in terms of prioritization what's
14 important to do sooner rather than later as well as
15 what are the hot issues and things like that. You
16 need, to misuse an old adage, it doesn't do you a lot
17 of good to look under the street light when you
18 realize the wall across the street. But actually in
19 point of fact, it's important to look under the street
20 light the things that you know are important, it's
21 also important to look outside there the things you
22 don't know that are important and keep searching and
23 figuring out what may be coming down the pike.

24 MEMBER SIEBER: Yes. It seems to me that
25 this plan compared to the last plan is more practical.

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 MR. ARNDT: Yes.

2 MEMBER SIEBER: And is driven more toward
3 real needs.

4 MR. ARNDT: Yes.

5 MEMBER SIEBER: As opposed to this broad
6 research.

7 MR. ARNDT: Right. And that's been an
8 evolutionary process dealing with and working with our
9 stakeholders.

10 MEMBER SIEBER: Well, to me it's a good
11 trend.

12 MR. ARNDT: Yes.

13 MEMBER SIEBER: I like it.

14 MR. KEMPER: Thank you.

15 MR. ARNDT: It has a specific intent.

16 MR. KEMPER: That's on purpose. That's
17 not an accident.

18 MEMBER BONACA: The one thing that I add,
19 again the issues of operating experience. I mean
20 there is experience that is there I'm sure has been
21 pulled together theorizing certain events and whatever
22 specifics they're interested to, the some that are
23 common cause some may be other things. And, you know,
24 to the degree to which that information can be
25 provided, even in research important to this measure,

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 as an introduction, as a history, I think it's
2 helpful. I mean, certainly it would be helpful
3 probably to the whole Committee if you had synopsis of
4 it, you know, sometime in the presentation. This is
5 not talking about hypothetical situations. We have
6 had events.

7 CHAIRMAN APOSTOLAKIS: Tom, do you want to
8 say anything?

9 MEMBER KRESS: No. I agree.

10 CHAIRMAN APOSTOLAKIS: And we're meeting
11 tomorrow.

12 MR. ARNDT: And we welcome input after the
13 meeting, too.

14 MR. KEMPER: No. But this has been very
15 helpful and, please, let's continue to talk any ideas
16 you get. Because quite honestly, I've been kind of
17 scratching my head trying to figure out what do we
18 need to talk to you all about in November --

19 CHAIRMAN APOSTOLAKIS: Scratching you're
20 head trying to figure out why does the ACRS have such
21 a bad reputation? We're such nice people.

22 MR. KEMPER: Well, we've spent so much
23 time in front of you --

24 CHAIRMAN APOSTOLAKIS: Undeserved.
25 Undeserved.

1 MR. KEMPER: We've so much time.

2 CHAIRMAN APOSTOLAKIS: A lot of it is
3 unfair.

4 MR. KEMPER: You're right. It's unfair.
5 But anyway, we still have to live with it.

6 CHAIRMAN APOSTOLAKIS: And in fact, I was
7 telling Eric earlier it seems that, you know, the
8 magnitude of this and the interest in the kind of work
9 you guys are doing, we'll probably have to continue
10 these Subcommittee meetings, especially as you start
11 producing stuff.

12 MR. KEMPER: Absolutely.

13 CHAIRMAN APOSTOLAKIS: Because this is a
14 big project, very important and we are all trying to
15 learn here what is going on.

16 MR. KEMPER: Right.

17 MR. ARNDT: And that's actually one thing
18 not necessarily in the letter, but informally we would
19 be very interested in which areas you would be most
20 interested in hearing from us.

21 CHAIRMAN APOSTOLAKIS: Well, you know my
22 area.

23 MR. ARNDT: Yes.

24 MR. ARNDT: Now seriously for scheduling
25 purposes it helps us a lot. But we're always happy to

1 come and talk to folks like you.

2 CHAIRMAN APOSTOLAKIS: Any other comments
3 from our colleagues here?

4 MR. WATERMAN: This is Waterman.

5 The other thing I see in the research plan
6 since I bought so much into it is you talk about the
7 plan growing. One of the things I'd like to see the
8 plan start doing is as we finish those projects up, we
9 start a new section in that plan that gives a synopsis
10 of the products we developed. So when somebody picks
11 it up and says they can look at one plan and see where
12 were you, where are you and what are you going to do
13 all in one document. So that document is going to
14 continue to grow as new projects get added in at the
15 front and as the completed projects get added in down
16 at the bottom so you can say well this is what they
17 intended to and well, this is what came out of that.

18 CHAIRMAN APOSTOLAKIS: And another thing
19 for the major items here, one for example being how to
20 bring all this stuff into PRA, I would strongly
21 recommend that you don't come here at the very end of
22 the project. It would be better to brief the
23 Committee or the Subcommittee at least, as those
24 milestones are reached, so you get some feedback.

25 MR. ARNDT: Absolutely.

NEAL R. GROSS

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

1 CHAIRMAN APOSTOLAKIS: And possibly
2 valuable advise.

3 MR. ARNDT: Right. Right.

4 CHAIRMAN APOSTOLAKIS: All right. I think
5 we've had enough for today. Thank you, gentlemen and
6 lady. And we shall see you again in the morning at
7 8:30.

8 (Whereupon, at 5:52 p.m. the meeting was
9 adjourned.)

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

CERTIFICATE

This is to certify that the attached proceedings
before the United States Nuclear Regulatory Commission
in the matter of:

Name of Proceeding: Advisory Committee on
Reactor Safeguards
Digital Instrumentation and
Control Systems Subcommittee
Docket Number: n/a
Location: Rockville, MD

were held as herein appears, and that this is the
original transcript thereof for the file of the United
States Nuclear Regulatory Commission taken by me and,
thereafter reduced to typewriting by me or under the
direction of the court reporting company, and that the
transcript is a true and accurate record of the
foregoing proceedings.



Katherine Sykora
Official Reporter
Neal R. Gross & Co., Inc.

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

(202) 234-4433

www.nealrgross.com



Defense-in-Depth and Diversity for Digital Upgrades

Presented to the
**ACRS Subcommittee on
Instrumentation and Control**

Rockville, MD
October 20, 2005

Contents

- Background
 - Impetus for EPRI Defense-in-Depth and Diversity (D3) Project
 - Current regulatory guidance
 - Key propositions
- EPRI D3 Guideline approach
- Technical issues
 - Digital common cause failure
 - Susceptibility and defensive measures
 - Estimating probability of failure
 - Risk insights
 - Impact of diversity on safety/risk
 - Modeling digital equipment in PRAs
- Recommendations for RES, NRR activities

Presenters

- | | |
|---------------------|-----------------------------|
| • Jack Stringfellow | Working group chairman, SNC |
| • Ray Torok, | EPRI (rtorok@epri.com) |
| • Thuy Nguyen | EPRI/Electricite de France |
| • Dave Blanchard | Applied Reliability |

Presenters represent industry working group - 10 utilities – design, PRA and licensing engineers; 4 equipment suppliers; 4 consultants/integrators; NEI and EPRI

Background - EPRI D3 Project

- Industry working group started in early 2002
- NRC staff (I&C, PRA, RES) attended working group meetings in 2002, 2003 and 2004
- D3 Guideline (product #1002835) published December 2004 - offers alternative to NRC guidance
 - Extends NRC approach
 - Applies risk insights to improve focus on safety
- Submitted for NRC review February 22, 2005
- Met with staff April 2005
- Still awaiting NRC letter on path forward

Regulatory Environment

Industry and NRC staff need a stable, predictable, and practical licensing approach for integrated digital upgrades.

- Current guidance is "difficult to implement"
- Current guidance is void of risk insights
- Recent experience – NRC staff not honoring SERs for topical reports
- Regulatory positions are changing without changing the governing documents
- Timeliness of planned research does not support near-term submittals

Impetus for EPRI D3 Project

- Digital upgrades are in progress for many plants/systems
- Software common-mode failure issue is still unsettled
 - Need to ensure "adequate coping capability" or diversity & defense-in-depth (D3), but....
 - Regulatory uncertainty – utilities and staff
 - Protracted, unpredictable reviews
- Current NRC guidance is problematic
 - Can require backups that add complexity and cost without improving safety
 - May not address events that are risk-significant
 - Discourages plant upgrades that would enhance safety
 - Requires analysis of events that are not safety-significant

Current Regulatory Guidance –

**BTP-19 of Chapter 7 of NUREG 0800 (Standard Review Plan),
NUREG/CR-6303**

- Evaluation of plant coping capability during digital CCF
 - 15 step process
 - Break digital system into blocks
 - Identify blocks with common software
 - Determine effects of simultaneous failure of common blocks on ESFAS and RTS
 - Reanalyze events in FSAR
 - Best estimate assumptions
 - Acceptance criteria based on 10 CFR 100 (radiation release)
 - Add diverse backups for actuating RTS or ESFAS as needed
- Approach characteristics
 - Deterministic, with focus on RPS, ESFAS and FSAR events
 - Software safety significance distorted
 - Failure probability = 1.0
 - Other failure contributors in the system ignored

Risk-Informed Method Offers Advantages

- Keeps focus on safety – can show where software has risk significance, assess D3 accordingly
- Allows consideration of digital system design features and characteristics that protect against digital CCF, e.g.,
 - Self testing
 - Data validation
 - Fault-tolerance
- Allows consideration of risk associated with adding diverse backups (e.g., spurious actions)
- Consistent with updated technical and regulatory trends
- Technical issues can be addressed
 - Digital system failure probabilities
 - Modeling digital equipment in PRA

Deterministic versus Risk-Informed Example 1 – Large Break LOCA

LBLOCA with digital CCF in low pressure injection (LPI)

- Deterministic (BTP-19) method
 - Insufficient time for operator action
 - Credit for leak detection backup (per BTP-19) disallowed by NRC
 - Therefore, diverse actuation of LPI and supporting systems needed as backup
- Application of risk insights would:
 - Consider low probability of digital CCF in LPI system
 - Show LBLOCA concurrent with digital CCF is a negligible contributor to core damage frequency (CDF)
 - Show that a diverse backup for the I&C
 - Would not reduce risk (large rotating components dominate)
 - Will add complexity and increase probability of spurious actuation

BTP-19 method adds hardware and complexity, but questionable safety benefit

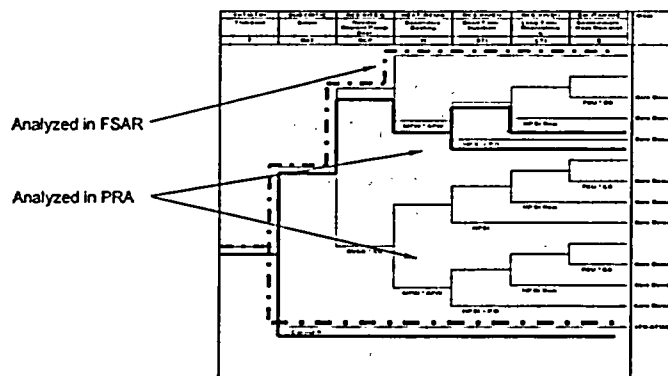
© 2005 Electric Power Research Institute, Inc. All rights reserved.

9

Deterministic versus Risk-Informed Example 2 – Risk-Significant Events from PRA

Beyond design basis events considered in PRA

- Are unevaluated using deterministic (BTP-19) method



- Risk-informed method addresses known risk significant accident sequences

© 2005 Electric Power Research Institute, Inc. All rights reserved.

10

Complementary Views of Digital Reliability Issues

	RES focus	EPRI focus
How reliable is the software?	X	
How reliable does it need to be?		X
How to prove reliability claim	X	
How to establish reasonable assurance		X
What process attributes affect reliability?	X	
What design attributes affect reliability?		X
How can digital systems fail?	X	
Which failure effects are important to safety?		X
How to accurately model digital in PRA	X	
Which behaviors need to be modeled in PRA		X
Solve problem for general purpose software	X	
Solve problem for high-integrity application software		X

© 2005 Electric Power Research Institute, Inc. All rights reserved.

11

Key Propositions of Today's Presentation

- Use of risk insights in D3 evaluations improves ability to manage safety issues associated with postulated digital CCFs
- It is possible to derive useful risk insights for D3 evaluations now
 - Without precise knowledge of failure probabilities
 - Without detailed PRA modeling of digital I&C
- It is possible to estimate reliability of digital equipment for D3 evaluations now, based on deterministic evaluation of the equipment
- Future research by RES and others will enhance methods and accuracy
 - Software reliability
 - Modeling digital systems in PRA

© 2005 Electric Power Research Institute, Inc. All rights reserved.

12

EPRI D3 Guideline Methods

- **Extended Deterministic** – based largely on BTP-19 approach
 - Use risk insights from PRA to address problematic events
- **Standard Risk-Informed** – risk focus with realistic assumptions
 - Update PRA and regenerate risk results
- **Simplified Risk-Informed** – risk focus with conservative assumptions
 - Use input from existing PRA to estimate change in risk
- Risk-informed methods use Regulatory Guide 1.174 acceptance guidance (based on ΔCDF , $\Delta LERF$)
- All three methods include confirmatory defense-in-depth review, similar to the Significance Determination Process (SDP)
- If acceptance criteria not met, can refine assumptions, use one of the other methods, modify the design, or add a backup function

First Step in D3 Evaluation is Identifying Susceptibilities to Digital CCF

- **BTP-19 (NUREG/CR 6303):**
 - Identify "blocks" such that internal failures don't propagate beyond block boundaries
 - Blocks that contain the same software modules are deemed susceptible
- **EPRI "defensive measures" approach looks "inside the block" to:**
 - Identify design features, behaviors, etc. that restrict digital failures / CCFs to small, manageable sets of potential failures
 - Constrain the "digital issues" problem to actual behaviors of realistic safety systems
 - Meet the intent of the NUREG and refine it to reflect more recent methods
 - Goes beyond process-based evaluation, considers as-built behaviors
 - Shows objectively why there is low potential for digital failure
 - Allows objective comparison of digital and analog systems
 - Improve susceptibility assessment for deterministic approach
 - Provide practical reliability treatment for risk-informed evaluations

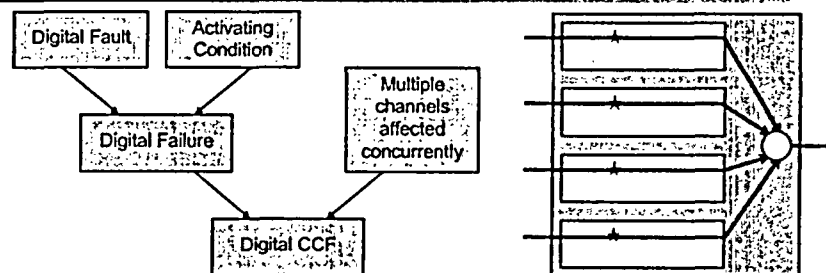
Susceptibilities to Digital CCF

- Evaluation of defensive measures provides a deterministic basis for estimating likelihoods of failure and CCF for digital equipment. However,
 - It is different from standard PRA treatment of hardware reliability - Digital failures are not random – they involve:
 - Likelihood that system will encounter unanticipated conditions
 - Likelihood that unanticipated conditions will cause unacceptable result in context of plant application
 - It requires
 - Expertise in software
 - Detailed knowledge of the design and functioning of the digital system

© 2004 Electric Power Research Institute Inc. All rights reserved.

15

Digital Failures and Digital CCFs: Necessary Ingredients



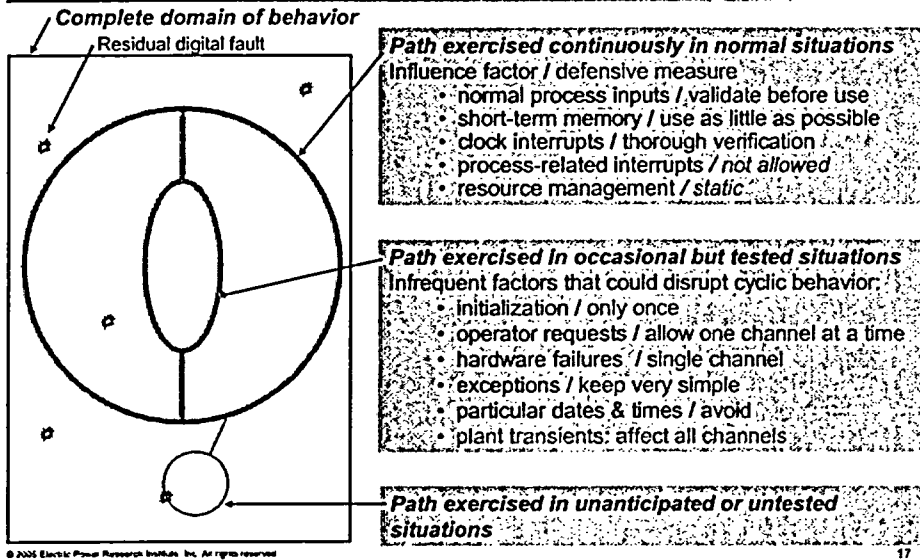
- In well-designed digital systems, defensive measures may be used to reduce and help evaluate:
 - The likelihood of the different types of residual digital faults
 - The possible activating conditions
 - The likelihood that an activating condition concurrently affects multiple channels
- Also
 - Not all activations of digital faults result in digital failure
 - Not all digital failures and digital CCFs are risk-significant

© 2004 Electric Power Research Institute Inc. All rights reserved.

16

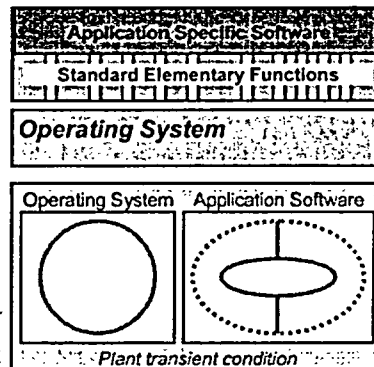
Example of Defensive Measures: the Minefield Metaphor - Cyclic Behavior with Well-Identified Influence Factors

Influence Factor: Anything that affects software trajectory



I&C Platform Software may not be a Dominant Cause of Digital CCF

- Main software modules
 - Operating System
 - Application Software
 - Standard Elementary Functions
 - Application Specific Software
- Operating System defensive measures
 - Independent from Application SW
 - Transparent to plant conditions
 - Postulated residual faults are unlikely to be activated during a plant transient
- Standard Elementary Function defensive measures
 - Small, simple, independent, usually stateless modules, well-mastered algorithms, very thorough V&V, operational experience
 - Digital faults are unlikely



© 2005 Electric Power Research Institute, Inc. All rights reserved.

18

Digital Faults in Application Specific Software

Specification Faults

Lack of understanding: specifiers do not fully understand or know the context of the I&C system

Expression faults: functional specification does not accurately reflect requirements or properly account for analog/digital differences

Software Implementation Faults

Automated code generation from formal functional specification

Simplicity facilitates high test coverage levels and software analysis

- In high quality software, digital failures tend to be predominantly caused by specification faults
 - The most likely failures usually have low risk significance
 - Channels implementing the same functional specification are likely to fail concurrently, regardless of other forms of diversity
 - Functionally diverse specifications are not necessarily immune from related understanding mistakes

© 2005 Electric Power Research Institute, Inc. All rights reserved.

19

Defensive Measures are Essential in Assessing Susceptibility and Reliability for D3 Evaluations

- Evaluation of defensive measures helps identify the dominant causes of digital failure and digital CCF on a deterministic basis
- A digital system with appropriate defensive measures can be shown to be at least as reliable as an equivalent analog system
 - Application specification (not the embedded software) dominates digital failure likelihood
 - Likelihood of specification errors is comparable for equivalent analog and digital systems
 - Digital hardware uses fewer components, is more reliable and more fault-tolerant
- Claims like this should be supported by appropriate evidence and documentation

© 2005 Electric Power Research Institute, Inc. All rights reserved.

20

From Defensive Measures to Risk Insights

- Using 'Defensive Measures' approach:
 - Provide evidence that probability of failure (on demand) for a digital I&C channel is on the same order as that for a similar analog channel
 - Select β for the I&C in:
 - Identical trains in same system (probably 1.0)
 - Different systems (between 0 and 1.0)
- Based on the diversity and defense-in-depth in the existing mechanical and electrical systems that is modeled in the PRA
 - Incorporate potential effects of digital CCF into the PRA
 - Evaluate change in core damage frequency
- Use sensitivity studies to develop insights
 - Under what accident sequence conditions does I&C diversity have value?
 - Under what conditions are the results insensitive to digital CCF?
 - Why?

Limited Scope PRA Studies

- Plant-specific PRA models for a PWR and BWR used to evaluate effects of digital CCF on:
 - Selected systems
 - PWR
 - Aux feedwater
 - Safety injection
 - Service water
 - AC power
 - BWR
 - HPCI & RCIC
 - Low pressure injection
 - Emergency depressurization
 - AC power
 - Selected accident sequences
 - PWR
 - Loss of feedwater with failure of secondary cooling and feed & bleed
 - Small LOCA with failure of high head safety injection
 - BWR
 - Turbine trip with failure of all injection
 - Large LOCA with failure of low pressure injection

Full Scope PRA Studies

- Full scope level 1 internal events PWR PRA used to evaluate effects of digital CCF on all accident sequences
 - 18 initiating events, ~200 accident sequences
 - Mitigating systems
 - 4 SGs
 - 2 turbine MFW pumps/
1 startup FW pump
 - 3 Condensate pumps
 - 2 motor AFW/
1 turbine AFW pump
 - 2 SI pumps/
2 charging pumps
 - 2 RHR pumps
 - 2 PORVs
 - 2 EDGs

© 2005 Electric Power Research Institute, Inc. All rights reserved.

23

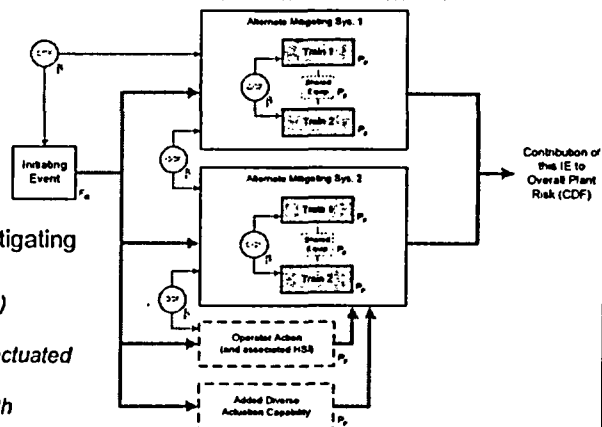
Digital CCF Effects in PRA

I&C channel reliability (P_{di})
• $10^{-2}/\text{dem}$ to $10^{-6}/\text{dem}$

I&C common cause (β)
• 1.0 to 0

Electrical and mechanical mitigating system I&C diversity

- 1 System diverse from IE ($\beta=0$)
- 2 Systems diverse from IE
- 2 Systems diverse from IE, 1 actuated by DAS
- 2 Systems diverse from IE, both actuated by operator
- 2 Systems diverse from IE and each other



© 2005 Electric Power Research Institute, Inc. All rights reserved.

24

Full Scope PRA Sensitivity Study - Example Results

Loss of FW

$$F_{IE} = 8.0E-2/\text{yr}$$

$$CDF = 5.1E-7/\text{yr}$$

CDF Results Summary

$$P_{\beta} = 10^{-4}/\text{dem}$$

Mitigating System Design	β		
	1.0	0.1	0.01
1 system diverse from IE	1.6E-05	1.0E-05	9.6E-06
2 systems diverse from IE (but not each other)	8.7E-06	1.5E-06	8.2E-07
2 Systems diverse from IE, 1 actuated by DAS	8.2E-07	7.5E-07	7.4E-07
2 Systems diverse from IE, both actuated by operator	7.4E-07	6.7E-07	6.6E-07
2 systems diverse from IE (and each other)	6.9E-07	6.9E-07	6.9E-07

Medium LOCA

$$F_{IE} = 4.0E-5/\text{yr}$$

$$CDF = 1.42E-7/\text{yr}$$

CDF Results Summary

$$P_{\beta} = 10^{-4}/\text{dem}$$

Mitigating System Design	β		
	1.0	0.1	0.01
2 systems diverse from IE	1.6E-07	1.3E-07	1.3E-07
2 Systems diverse from IE, 1 actuated by DAS	1.42E-07	1.42E-07	1.42E-07
2 systems diverse from IE (and each other)	1.43E-07	1.43E-07	1.43E-07

© 2005 Electric Power Research Institute, Inc. All rights reserved.

25

Risk Insights – When is D3 of value for a digital I&C system?

- Dictated by:
 - Frequency of the initiating event
 - Existing D3 of the mechanical and electrical mitigating systems
- Examples
 - High frequency events benefit from D3 in the I&C
 - Multiple, diverse mitigating systems
 - Want to preserve existing diversity of electrical / mechanical equipment
 - Low frequency events receive little benefit from the addition of diversity in the I&C
 - Single mitigating system with little diversity between redundant trains of electrical / mechanical equipment

© 2005 Electric Power Research Institute, Inc. All rights reserved.

26

Risk Insights - How reliable does a digital I&C system need to be?

- Dictated primarily by the frequency of the initiating event
 - High frequency events benefit the most from reliable digital I&C (e.g., Turbine Trip, Loss of FW)
 - Reliability of a channel of digital I&C need only be similar to a functionally similar channel of analog I&C ($P_{df} \sim 1E-4/\text{dem}$)
 - Some degree of diversity needed in actuating mitigating systems (ability of operator to implement EOPs independent of digital failure is generally sufficient)
 - Low frequency events are insensitive to the reliability of the digital I&C (e.g., LOCAs, MSLB)
 - Single mitigating system with reliability dominated by major rotating equipment ($P_{df} \sim 1E-2$ to $1E-3/\text{dem}$)
 - Also insensitive to potential for common cause failure of redundant channels ($\beta_{cc} \sim 1$)

© 2005 Electric Power Research Institute, Inc. All rights reserved.

27

Conclusions

- Utilities want to install digital upgrades now. An improved D3 approach is needed now
- New digital system evaluation techniques make it possible to improve on the assumption that software failure probability is 1 or 0
- Proposed methods in the EPRI D3 Guideline:
 - supplement and complement the BTP-19 approach, improving both practicality and safety focus
 - meet the intent of BTP-19 in that they are effective ways to "demonstrate vulnerabilities to common cause failure have been adequately addressed."
- Future research on digital reliability and PRA modeling will offer improvements in accuracy, modeling techniques and risk insights

© 2005 Electric Power Research Institute, Inc. All rights reserved.

28

Recommendation for Further Research

- Continue Work on Digital Reliability, but.....
 - Don't start with "general case" software (complex, multi-tasking, etc.)
 - It's too difficult
 - It's not relevant to NPP safety systems
 - Constrain the problem by starting with simple, high-quality software appropriate for safety applications
 - Keep track of where D3 is of value and what levels of reliability are actually needed
 - Include consideration of designed-in behaviors - they are more revealing, more deterministic, and more important than process-based criteria
 - Coordinate with industry to ensure that:
 - Important issues are addressed
 - Results are practical and useful



System Aspects of Digital Technology Overview

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

October 20, 2005

Steven A. Arndt

Division of Engineering Technology
Office of Nuclear Regulatory Research
301-415-6502, saa@nrc.gov

William E. Kemper

Division of Engineering Technology
Office of Nuclear Regulatory Research
301-415-7585, wek@nrc.gov

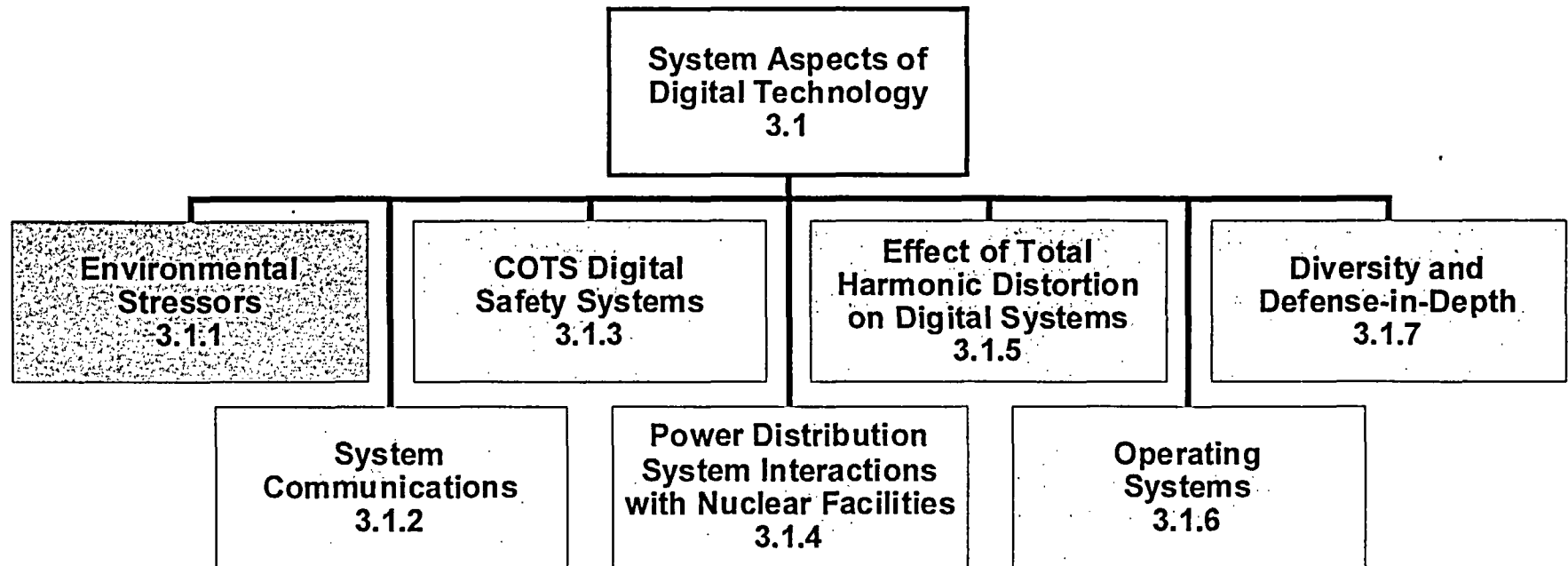


SYSTEM ASPECTS OF DIGITAL TECHNOLOGY

- Current issues
 - Ever increasing use of digital systems requires new information and continuous improvements to the review process
 - Digital systems will take on an ever increasing role in the protection and control systems in nuclear power plants
 - New system challenges will continue to emerge (tin whiskers, IC card aging, etc.)



SYSTEM ASPECTS OF DIGITAL TECHNOLOGY





SYSTEM ASPECTS OF DIGITAL TECHNOLOGY

- System aspects of digital technology involve those factors, both internal and external, that affect the performance of a digital system as a whole.
- This part of the research program will address aspects of digital systems that can adversely affect safety due to
 - Environmental stressors
 - Systems interactions associated with power distribution and total harmonic distortion effects
 - Operating systems and system communications
 - Diversity and defense-in-depth, and COTS systems



SYSTEM ASPECTS OF DIGITAL TECHNOLOGY

- This research program provides
 - Fundamental understanding of digital technologies used in safety systems including system strengths and weaknesses
 - Technical information needed to review development and installation issues for digital technologies in safety systems
 - Technical guidance for licensing digital technologies in safety systems
 - Tools, methodologies, and objective acceptance criteria for reviewing these systems
- Seven project areas are currently included in the NRC Digital System Research Plan



ENVIRONMENTAL STRESSORS PROJECTS 3.1.1

- Environmental compatibility for safety-related I&C systems depends on maintaining the expected environment in the nuclear power plant and qualifying the equipment to withstand that environment
- Current project includes enhancing the technical bases for conducted EMI/RFI, development of regulatory guidance for ensuring adequate lightning protection and development of qualification standards for computer-based equipment important to safety in mild environments



SYSTEM COMMUNICATIONS PROJECT 3.1.2

- The trend in digital safety systems is towards networked intrasystem architectures using dedicated communication microprocessors and proprietary communication protocols
- NRC needs detail information to evaluate these complex digital communication systems and the failure analysis techniques for these architectures



SYSTEM COMMUNICATIONS

- Research will identify
 - Communication systems likely to be used for safety functions
 - Features of safe protocols for data transfer
 - Failure scenarios and mitigation strategies
- These methods will be further refined using realistic safety-related COTS systems for incorporation into NRC review methodologies
- This project is projected to start in FY07



COTS DIGITAL SAFETY SYSTEMS PROJECT 3.1.3

- The nuclear industry is retrofitting existing analog systems with COTS-based digital systems
- Licensees typically use a combination of processes to dedicate COTS equipment for safety related applications
 - Special tests and inspections
 - Supplier surveys
 - Source verification
 - Performance history
- NRC performs qualitative assessments of COTS dedications



COTS DIGITAL SAFETY SYSTEMS

- This project will assess currently available methods for quantitatively determining the acceptability of COTS components.
- Perform case studies of possible quantitative safety assessment methods for reviewing COTS components including:
 - Hardware
 - Software
 - Interactions between safety system channels and between safety and non-safety systems
 - Human-machine interfaces
- This project is projected to start in FY07



ELECTRICAL POWER DISTRIBUTION SYSTEM INTERACTIONS PROJECT 3.1.4

- Nuclear power plant are subject to loss-of-off-site power due to grid disturbances, resulting in loss of power and voltage fluctuation internal to the nuclear power plant
- Loss of power and voltage fluctuations have the potential to cause digital systems to exhibit failures that may not have been seen in the analog components that they replace
- Digital systems are being deployed for control and protection systems in the plants as well as being integrated into other components (smart sensors, power supplies, etc.)



ELECTRICAL POWER DISTRIBUTION SYSTEM INTERACTIONS

- Research will support ongoing RES efforts to
 - Understand the effects of NPP digital component and system interactions and potential for CMF caused by electric transmission and distribution system disturbances
 - Develop methods capable of modeling the complex system interactions needed to determine the effect of power fluctuations on digital system in nuclear facilities
 - Review existing standards to determine their applicability for addressing these issues
- This project is projected to start in FY08



EFFECT OF THD ON DIGITAL SYSTEMS PROJECT 3.1.5

- Switching power supplies, non-linear loads, etc., cause harmonic distortion of electric power (commonly termed as THD) that may affect digital systems adversely
- Newer digital components are more sensitive to power quality disturbances
 - Higher IC circuit densities
 - Lower voltage requirements for memory states
 - Higher power requirements



EFFECT OF THD ON DIGITAL SYSTEMS

- The research will evaluate the effects of THD on digital component performance and safety and review existing standards (for example IEEE Std 519) to determine their applicability for addressing THD related effects on digital components
- This research will also identify methodologies for evaluating the effect of THD on digital systems and determining if existing power specifications are adequate
- This project is projected to start in FY08



OPERATING SYSTEMS PROJECT 3.1.6

- Operating systems used in nuclear safety applications continue to become more complex
- NRC and licensees may not be able to assess proprietary COTS operating systems adequately
- RES reviewed potential impacts of operating systems on the reliability and safety of digital systems in the past but the results were inconclusive



OPERATING SYSTEMS

- This research will:
 - Study design aspects, best practices and failure modes of operating systems
 - Identify safety-critical design aspects of operating systems
 - Acquire or develop tools and procedures for assessment of operating systems
 - Develop processes for performing safety assessments of operating systems
- This project is projected to start in FY08



DIVERSITY AND DEFENSE-IN-DEPTH PROJECT 3.1.7

- D3 position and guidance are deterministic
 - BTP HICB-19 is not risk-informed
 - NUREG/CR-6303 provides alternatives without identifying the most acceptable approach
- The nuclear power industry has proposed risk informed approaches to address the D3 issue
 - Leak before break
 - Risk contributed by CMF
- The nuclear power industry has proposed designs that would combine echelons of defense-in-depth, and operator actions for diversity



DIVERSITY AND DEFENSE-IN-DEPTH

- The project will
 - Perform case studies of digital safety system configurations to determine their susceptibility to CMF
 - Test NUREG/CR-6303 coping strategies to develop best practices, methodologies and acceptance criteria for D3 designs
 - Review insights from probabilistic analysis of CMF
 - Verify, from a deterministic standpoint, that existing guidance (SRP BTP HICB-19) is realistically conservative
- This project is projected to start in FY06



SYSTEM ASPECTS OF DIGITAL TECHNOLOGY SUMMARY

- The research area focus on system aspects of digital technology involve those factors, both internal and external, that affect the performance of a digital system as a whole
 - Environmental stressors
 - Systems interactions associated with power distribution and total harmonic distortion effects
 - Operating systems and system communications
 - Diversity and defense-in-depth, and COTS systems
 - New challenges to digital system will continue to emerge (tin whisker, IC card aging, etc.)
- These research projects will provide objective acceptance criteria and review procedures that augment and supplement existing SRP guidance for approving (or denying) digital safety system license applications



Environmental Stressors (3.1.1)

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

October 20, 2005

Christina E. Antonescu
Division of Engineering Technology
Office of Nuclear Regulatory Research
301-415-6792, cea1@nrc.gov

Richard T. Wood
Oak Ridge National Laboratory
865-574-5578, woodrt@ornl.gov

Effects of Environmental Stressors on Safety-Related I&C Systems Are Being Addressed in Regulatory Research

- Lightning Protection
 - DG-1137 presented to ACRS on July 6, 2005
 - Reviewed by ACRS on July 18, 2005
 - Will be issued as Regulatory Guide 1.204
- Environmental Qualification for Mild Environments
 - DG-1077 was developed in response to a User Need
 - It provides comprehensive guidance on mild environment qualification of safety-related computer-based I&C systems
 - DG-1077 was revised to endorse the recently updated IEEE standard
- Electromagnetic Compatibility
 - Industry proposal for relaxed susceptibility test limit under evaluation

DG-1077 Has Been Revised to Update and Enhance the Qualification Guidance It Provides

- DG-1077 was presented to ACRS on February 6, 2003
- ACRS approval for release as a final effective guide was granted on February 14, 2003
- DG-1077 was deferred pending consideration of new version of IEEE qualification standard (Letter from Mayfield to Horrion/NUGEQ, May 30, 2003)
- IEEE 323-2003 was released on September 11, 2003
- Review of IEEE 323-2003 has been conducted
- DG-1077 has been revised and is now DG-1142

Comparison of IEEE 323-1983 and IEEE 323-2003 Showed No Significant Differences for Mild Environment Qualification

- Primary differences involve practices for harsh environment qualification
 - IEEE 323-2003 added provisions for using condition monitoring as part of on-going qualification
 - Application of dual transients in DBA testing as a form of margin was deleted
 - Other wording changes raise some issues that must be considered before endorsement for harsh environment qualification
 - Guidance on documentation for mild environment qualification remains the same in both versions and is inconsistent with regulatory practice
- Qualification practices in IEEE 323-2003 are appropriate for mild environment application with clarifications and conditions
- Technical basis for endorsing IEC 60780 (1998) remains unaffected
 - Equivalent to practices in IEEE 323-2003
 - Reduced scope of DG-1077 limits endorsement to mild environment application only

DG-1077 Endorses Current Environmental Qualification Standards for Safety-Related Computer-Based I&C Systems in Mild Environments

- Qualification practices in IEEE 323-2003 and IEC 60780 (1998) endorsed as acceptable for application to safety-related computer-based I&C systems located in mild environments
- Guidance applies to new or modified safety-related I&C systems in existing and future nuclear power plants that employ computers
- Guidance addresses unique characteristics of computer-based I&C systems as well as acceptable evidence for mild environment qualification of complex technology

What has Changed in DG-1077

- Endorsement of domestic qualification standard updated to reflect most recent version of IEEE 323
- Regulatory positions reflect revised scope and provide pointers to guidance on key related issues
 - Practices in standards endorsed for application to safety-related computer-based I&C systems located in mild environments, subject to conditions and clarifications
 - Guidance on harsh environment qualification has been deleted and a pointer to RG 1.89 as prevailing guidance added
- DG-1077 is ready to proceed with release for a second round of public comments

DG-1077 Endorsement of Qualification Standards Includes Exceptions and Enhancements

- DG-1077 provides one enhancement to IEEE 323-2003 and IEC 60780 (1998)
 - Unique characteristics of microprocessors are addressed [Position 1]
 - ❖ Equipment must be operating and performing intended function during testing (consistent with Ch. 7, NUREG-0800 and IEEE 7-4.3.2)
 - ❖ Dynamic response of distributed system must be evaluated (consistent with Ch. 7, NUREG-0800)
- DG1077 provides one exception to IEEE 323-2003
 - Exception is taken to Clause 7.1 of IEEE 323-2003 [Position 4]
 - ❖ Documentation provided to show evidence of environmental qualification must be consistent with the guidance in clause 7.2
 - ❖ Design Specification/Certificate of Conformance is not sufficient documentation of qualification for mild environments (consistent with Chapter 7, NUREG-0800)

DG-1077 Provides Pointers to Acceptable Guidance on Key Related Issues

- EMI susceptibility testing guidance is provided in R.G. 1.180 Rev. 1 [Position 2]
- Harsh environment qualification guidance is provided in R.G. 1.89 Rev. 1 [Position 3]

Response Is Generally Positive to Regulatory Guidance on Electromagnetic Compatibility in Nuclear Power Plants

- EPRI TR-102323 — “Guidelines for Electromagnetic Interference Testing in Power Plants”
 - Originally issued in September 1994
 - Reviewed and accepted with stipulations in SER in April 1996
 - Rev.1 update in 1996; Rev. 2 in 2000; and Rev. 3 in 2005 (no revisions have been endorsed)
- RG-1.180 — Guidelines for Evaluating EMI/RFI in Safety-Related I&C Systems
 - Originally released in January 2000
 - Rev. 1 update in May 2003
 - Industry response is generally positive
 - One significant issue concerns industry – CS114 operating envelope

EPRI is Requesting that NRC Review the CS114 Operating Envelope in RG 1.180, Rev. 1 Citing that Its Previous Measurements Were Flawed

- CS114 is a high-frequency conducted susceptibility test that has proven problematic for nearly all equipment tested and most equipment requires redesign to pass or justification for exception
- CS114 operating envelope in RG 1.180, Rev. 1 incorporated plant data and analysis from EPRI
- EPRI cites that its measurements and analysis of plant data were flawed, i.e., it included transient data that could not be separated from continuous wave data
- EPRI cites that CS114 operating envelope in RG 1.180, Rev. 1 is subsequently flawed

Background — EPRI Collected Conducted Emissions Data in 1994

- ❑ Conducted emissions measurements were made in seven plants and included captured power transients
- ❑ Subsequent EPRI data profile showed high conducted emissions levels in plants
- ❑ RES made limited conducted emissions measurements in plants — infrequently allowed because of their intrusive nature
- ❑ RES data profile showed lower levels but had high degree of measurement uncertainty

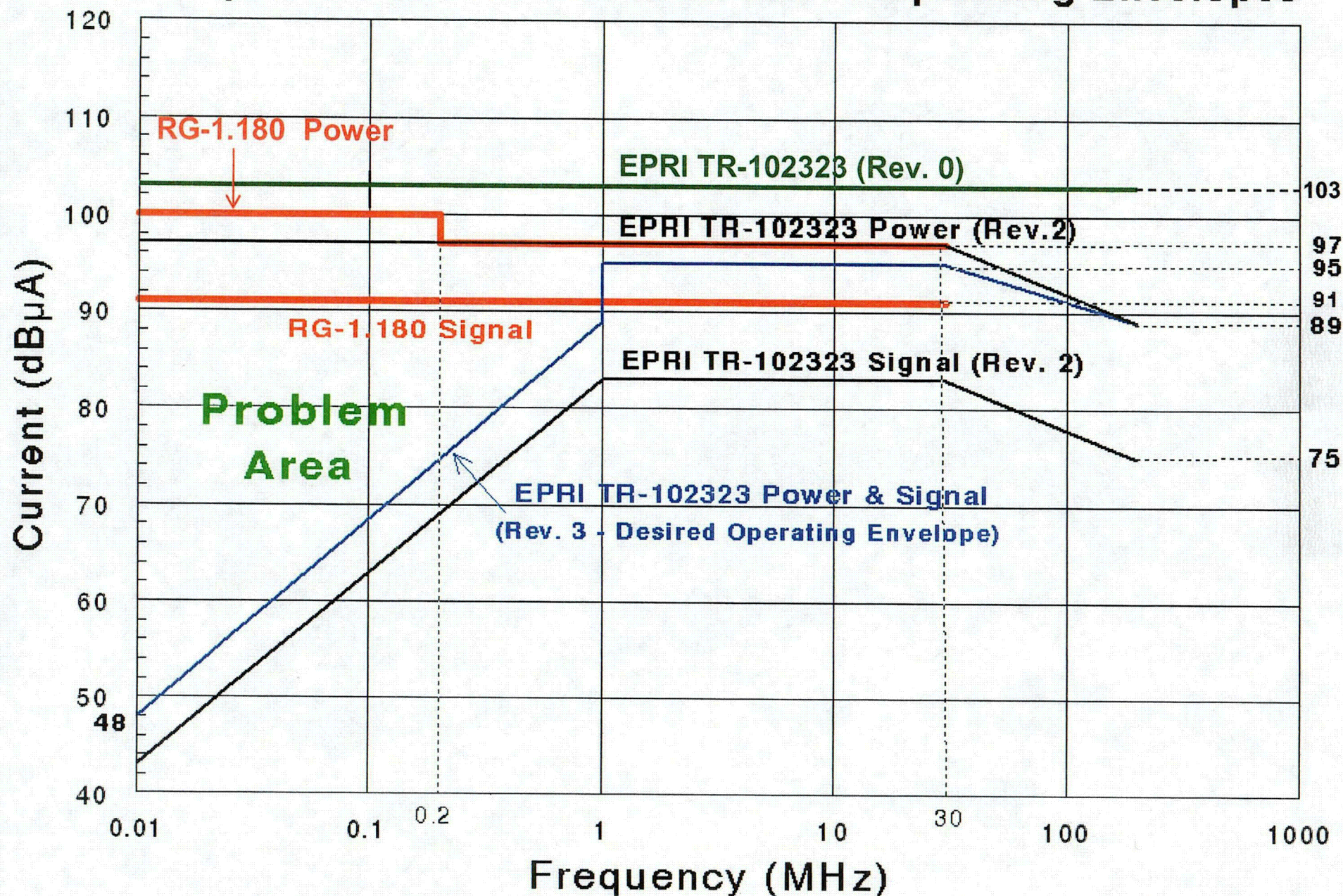
Background — RES Incorporated EPRI Data into Development of NRC CS114 Envelope

- ❑ Started with operating envelope for military ground facilities in MIL-STD 461D
- ❑ Adjusted operating envelope to incorporate EPRI plant data and be consistent with SER based on TR-102323
- ❑ Goal was to ensure that safety-related equipment could withstand ambient conducted emissions in plants
- ❑ Technical basis is documented in NUREG/CR-6431

EPRI is Now Revising Its Original Data Collection and Analysis Rationale

- ❑ EPRI cites that conducted emissions data should not have included captured power transients, as these are addressed by power surge susceptibility testing
- ❑ EPRI cites that the CS114 operating envelope was not intended to be based on conducted emissions measurements, but rather should be based on the radiated emissions environment — it's a coupling issue
- ❑ EPRI cites that its original rationale was flawed and hence the SER operating envelope based on TR-102323 was flawed

Comparison of NRC and EPRI CS114 Operating Envelopes



RES Is Looking Into EPRI's Rationale and Request

- RES has reviewed the information received from EPRI regarding the CS114 operating envelope in TR-102323
- RES is investigating the rationale for the EPRI proposed CS114 operating envelope
- RES will update RG 1.180, Rev. 1 if the results of the investigation justify

BACKUP

What Unique Characteristics of Microprocessor Technology Are Addressed?

- Need to operate the equipment as it is tested by performing full range of functions
 - Specified in IEEE 7-4.3.2
 - Results from complexity of functions that can be performed and the range of operational states assumed by computers
 - Confirms performance of software operating on hardware under environmental stress
- Need to evaluate dynamic response of distributed system under environmental stress
 - Consistent with Channel Integrity and System Integrity guidance in NUREG-0800 Sections 7.1-B 6 and 7.1-C 10
 - Confirmatory research showed that digital communication interfaces can be vulnerable to intermittent upsets that impede data flow and can interrupt function (NUREG/CR-6406)
 - Confirms that system design requirements for time response are met even under environmental stress (e.g., when full system testing is not practical) and addresses sequential execution and accumulated delay

Original DG-1077 Explicitly Addressed Harsh Environment Technical Issues

- Exceptions were taken to resolve issues
 - Dual transients without amplitude margin not acceptable for DBA testing
 - Aging to an end-of-life condition is necessary for Category A (harsh environment) qualification to meet 10 CFR 50.49 requirement
- Revised DG-1077 does not apply to harsh environment qualification so exceptions (and previous qualification location categories) were deleted

IEEE 323-2003 Poses “Issues” That Must be Considered

- Margin for age conditioning
 - Statement that suggested margin factors do not apply to aging still exists
 - Discussion of type testing specifies need for margin only for DBE testing (strengthening the implication that margin for aging is not necessary)
 - As with IEEE 323-1983, no explicit requirement for margin in age conditioning is present
- LOCA/HELB test profiles
 - No specification of dual transient with margin
 - Profile figure shows single transient with margin on magnitude
 - Time margin omitted without justification

IEEE 323-2003 Poses “Issues” That Must be Considered (cont)

- Radiation source
 - Unqualified permission to use a gamma source
 - Requirement to test against all significant types of radiation present in the service conditions is dropped
 - Requirement to subject equipment to radiation equivalent to or greater than that expected in service is dropped
- Operating experience
 - Change in qualification by experience from requiring that equipment differences do not affect the ability to perform the safety function to instead permit differences as long as they do not “unacceptably” reduce the capability to perform the safety function
- Analysis
 - As with IEEE 323-1983, the criteria that must be satisfied for the analytical technique to be considered valid are not explicitly stated

IEEE 323-2003 Poses “Issues” That Must be Considered (cont)

- Extension of qualified life
 - Methods similar to those in IEEE 323-1983 that address identification of conservatism as a basis for qualified life extension are present
 - Requirement that on-going qualification methods must be technically justified and documented is deleted
- Age conditioning
 - Requirement of conservatism in age conditioning eliminated with no comparable requirement of margin
- Documentation
 - As with IEEE 323-1983, design specifications and certificates of conformance are declared as sufficient documentation for equipment qualification in mild environments

Only One IEEE 323-2003 Issue Relevant For DG-1077 Endorsement

- All but one issue relevant to only harsh environment qualification
 - DG-1077 only addresses mild environment qualification for specific technology
 - Other issues must be addressed prior to endorsement of standard for harsh environment use
- Exception taken in DG-1077 to mild environment issue
 - Design specification/certificate of conformance not sufficient documentation for mild environment qualification of safety-related computer-based I&C systems
 - Provides acceptable evidence up front rather than through RAIs
 - Avoids implication that mild environment qualification not necessary

Is There a Conflict With Two Regulatory Guides Endorsing the Same Standard?

- The purpose of regulatory guides is not to give a blanket endorsement of a standard but rather to provide guidance on an acceptable method to address a particular issue related to satisfying the Commission's regulations
 - RG 1.89 describes an acceptable method for satisfying 10 CFR 50.49
 - DG-1077 describes acceptable methods for satisfying 10 CFR 50.55a(h) and GDC 4
 - Neither guide has endorsement of IEEE 323 as its fundamental purpose
- Two regulatory guides focus on different aspects of the environmental qualification issue
 - Harsh environment qualification for Class 1E electrical equipment in RG 1.89
 - Mild environment qualification for safety-related computer-based I&C systems in DG-1077
- Effectively, the two guides endorse IEEE 323 for distinct applications and there is no inconsistency or conflict
 - For continuity and stability, the focus of R.G. 1.89 should remain on qualification in harsh environment to satisfy 10 CFR 50.49
 - DG-1077 addresses specific considerations for unique technology by focusing on qualification of safety-related computer-based I&C systems in mild environments

Existing Regulatory Guidance on Environmental Qualification Distributed Among Several Resources

- Regulatory Guide 1.89
 - Addresses 10 CFR 50.49 for electrical equipment important to safety
 - Limits scope to harsh environments that are subject to Design Basis Accident (DBA) conditions
 - Endorses IEEE 323-1974
- NUREG-0588
 - Provides NRC staff position on environmental qualification of safety-related electrical equipment
 - Applies to qualification based on IEEE 323
 - Describes equipment categories that includes mild environment applications (equipment not subject to DBA)
 - States qualification for mild environment should be supported by test or test and analysis

Existing Regulatory Guidance on Environmental Qualification Distributed Among Several Resources (cont)

- NUREG-0800, Chapter 7
 - Provides review guidance to NRC staff on environmental qualification of safety-related I&C systems
 - References design criteria from IEEE 7-4.3.2
 - Specifies qualification for mild environments according to IEEE 323
 - States testing of channel or system “as a whole” is preferred but notes that licensee should confirm conservative design if testing not practical
- DG-1077 is intended to provide a roadmap for an effective and acceptable use of existing guidance

Regulatory Uncertainty Can Arise Without Explicit Comprehensive Guidance

- Is qualification for mild environments necessary and what is sufficient evidence?
 - Excluded from scope of 10 CFR 50.49 but implicitly required in 10 CFR 50.55a(h)
 - Guidance distributed over several sources
 - ❖ IEEE 603/279, IEEE 7-4.3.2
 - ❖ NUREG-0588
 - ❖ NUREG-0800 Chapters 3 and 7
 - ❖ SERs
 - When are certificates of conformance or conservative designs acceptable?
- Are existing national (IEEE 323-2003) or international (IEC 60780) standards acceptable?
- Recent review of Topical Reports continued a case-by-case treatment of qualification for mild environments

Why is DG-1077 Needed?

- Unique characteristics of microprocessor-based equipment (functional and hardware) should be addressed
- No existing endorsement of current national or international consensus standards on environmental qualification
- No comprehensive regulatory guide defining approach to qualification for mild environments
- Potential regulatory burden arises from case-by-case treatment of qualification for mild environments