

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (not applicable)

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005
SUNSI REVIEW COMPLETE

Location: Rockville, Maryland

Date: Wednesday, April 18, 2007

Work Order No.: NRC-1527

Pages 1-307

ORIGINAL

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

April 18, 2007

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on April 18, 2007, 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.

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

+ + + + +

SUBCOMMITTEE ON DIGITAL INSTRUMENTATION

AND CONTROL SYSTEMS

+ + + + +

WEDNESDAY,

APRIL 18, 2007

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The meeting was convened in Room T-2B3 of Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Dr. George E. Apostolakis, Chairman, presiding.

MEMBERS PRESENT:

- GEORGE E. APOSTOLAKIS Chairman
- THOMAS KRESS ACRS Member
- OTTO L. MAYNARD ACRS Member
- SAID ABDEL-KHALIK ACRS Member

NEAL R. GROSS

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

1 NRC STAFF PRESENT:

2 STEVE ARNDT

3 ALLEN BRADLEY

4 CLIFF DOUTT

5 GENE EAGLE

6 ALAN HOWE

7 IAN JUNG

8 MICHAEL JUNGE

9 BILL KEMPER

10 ALAN KURITZKY

11 PAUL LOESSER

12 MIKE MAYFIELD

13 MIKE WATERMAN

14

15 ALSO PRESENT:

16 TUNC ALDEMIR

17 BOB ENZINNA

18 SERGIO GUARRO

19 KIMBERLY KEITHLINE

20 ALEX MARION

21 GERARDO MARTINEZ-GURIDI

22 RICK ROTA

23 JEFF STONE

24 RAY TORRECK

25 RICHARD WOOD

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

		3
1	<u>AGENDA ITEMS</u>	<u>PAGE</u>
2	Opening Remarks	4
3	NRC Digital I&C Steering Committee	
4	Activities	5
5	Industry Perspective on Diversity and	
6	Defense-in-Depth (D3) Issues	8
7	Current Regulatory Position on D3	
8	Requirements for Digital Safety Requirements	24
9	NRC Short Term Activities to Address	
10	D3 Issues	50
11	Longer Term Activities (Research) in the	
12	Area of D3	79
13	General Discussion of D3 Issues	128
14	Industry Perspective on Risk-Informing	
15	Digital System Reviews and Dynamic	
16	Digital System Reliability Modeling	152
17	NRC Short-Term Activities Associated with	
18	Risk-Informing Digital System Reviews	160
19	Review of Current Status of Dynamic	
20	Digital Reliability Modeling Research	195
21	Review of Current Status of Traditional	
22	Digital Reliability Modeling Research	244
23	Regulatory Guidance for Risk-Informing	
24	Digital Systems	284
25	Adjourn	

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

(8:30 a.m.)

1
2
3 CHAIRMAN APOSTOLAKIS: The meeting will
4 now come to order. This is a meeting of the Digital
5 Instrumentation and Control Systems Subcommittee. I'm
6 George Apostolakis, Chairman of the Subcommittee.

7 ACRS members in attendance are Said Abdel-
8 Khalik, Tom Kress, and Otto Maynard. Gary Hammer of
9 the ACRS staff is the Designated Federal Official for
10 this meeting.

11 The purpose of this meeting is to discuss
12 NRC staff and industry activities for digital
13 instrumentation and control systems. We will hear
14 presentations from the NRC's Offices of Nuclear
15 Regulatory Research and Nuclear Reactor Regulation.
16 We will also hear a presentation from the Nuclear
17 Energy Institute.

18 The Subcommittee will gather information,
19 analyze relevant issues and facts, and formulate
20 proposed positions and actions, as appropriate, for
21 deliberation by the full Committee.

22 The rules for participation in today's
23 meeting have been announced as part of the notice of
24 this meeting previously published in the Federal
25 Register. We have received no written comments or

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 requests for time to make oral statements from members
2 of the public regarding today's meeting.

3 A transcript of the meeting is being kept
4 and will be made available as stated in the Federal
5 Register notice. Therefore, we request that
6 participants in this meeting use the microphones
7 located throughout the meeting room when addressing
8 the Subcommittee. The participants should first
9 identify themselves and speak with sufficient clarity
10 and volume so that they may be readily heard.

11 We will now proceed with the meeting and
12 I call upon Mr. Mayfield of the Office of New Reactors
13 to begin.

14 MR. MAYFIELD: Thank you, Mr. Chairman.

15 We just wanted to spend a couple of
16 minutes to start this off and provide the Subcommittee
17 a little bit of information about how we got where we
18 are and what we are trying to accomplish.

19 There was a November 8th, 2006 meeting
20 where the staff made a presentation to the Commission
21 -- the staff as well as the industry. Coming out of
22 that Commission meeting was a Staff's Requirements
23 Memorandum directing the staff to establish an NRC
24 project plan with specific milestones and deliverables
25 with both short- and long-term milestones. And 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 address the critical path short-term actions.

2 The staff established the NRC Digital I&C
3 Steering Committee. The Executive Director for
4 Operations issued a memorandum in January of this
5 year. Jack Grobe from NRR chairs the Steering
6 Committee. Unfortunately Mr. Grobe could not be with
7 us this morning so he asked me to sit in for him. I'm
8 much better looking than he is so we went that
9 direction rather than to some of my colleagues who are
10 also on the Steering Committee.

11 CHAIR APOSTOLAKIS: And who are also good
12 looking.

13 MR. MAYFIELD: Pardon me?

14 CHAIR APOSTOLAKIS: And are also good
15 looking.

16 MR. MAYFIELD: Well, I won't go that far.
17 But the other members of the Steering Committee are
18 Mark Cunningham, representing the Office of Research,
19 Joe Gitter, representing NMSS, and Scott Morris,
20 representing INSR.

21 We have had three public meetings with our
22 industry counterparts. The first was December 21st of
23 2006. We met again in January. And then again in
24 March of this year.

25 We have had multiple internal Steering

NEAL R. GROSS

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

1 Committee meetings and have evolved into six task
2 working groups that represent cyber-security,
3 diversity and defense-in-depth, highly integrated
4 control rooms in terms of human factors, highly
5 integrated control rooms in terms of communications
6 within the control room, risk-informed issues for
7 digital I&C, and the digital I&C licensing process.

8 We have drafted some project plans and
9 problem statements for each of those task working
10 groups. Those have been shared with the industry and
11 publicly to solicit industry comment and feedback. We
12 will finalize those problem statements and the
13 associated work plans in the near future.

14 We will be briefing the Commission on the
15 status of this program in June. And we are also
16 hosting an IAEA technical meeting in June on diversity
17 and defense-in-depth. This promises to be a fairly
18 large meeting.

19 Mark Cunningham and Bill Kemper are the
20 leads on it. And so if any of you are interested, we
21 would certainly invite you to participate. We've had
22 good support from NEI, EPRI, as well as DOE in
23 organizing that meeting.

24 MEMBER KRESS: Do you know the dates?

25 MR. MAYFIELD: Well I should but I 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 MR. KEMPER: Sorry, this is Bill Kemper.
2 June the 19th through the 21st here in the D.C. Metro
3 area. I believe out in Rockville actually -- in
4 Bethesda, excuse me.

5 MR. MAYFIELD: Okay. With that, Mr.
6 Chairman, I would, I guess, turn it back to you.

7 CHAIR APOSTOLAKIS: Yes, our next
8 presentation is from NEI, Mr. Alex Marion, who is a
9 new presenter for the Committee.

10 MR. MARION: Good morning. My name is
11 Alex Marion. I'm the Executive Director of Nuclear
12 Operations and Engineering at NEI. With me is
13 Kimberly Keithline, Senior Project Manager in the
14 Engineering Group at NEI.

15 I just want to make a couple of comments
16 with regard to what Mike Mayfield said about the
17 establishment of the Steering Committee and
18 development of the project plan for licensing digital
19 I&C applications. We're really pleased with the
20 effort thus far.

21 We would have liked to have the project
22 plan in place six months ago but the industry and the
23 NRC is working very effectively. And we're hoping
24 that we can use this as a protocol for future
25 interactions on some of the more challenging

NEAL R. GROSS

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

1 regulatory issues that both the industry and the NRC
2 have to deal with.

3 With regard to the project plan that was
4 recently made public, we intend to provide comments to
5 the NRC next week.

6 MS. KEITHLINE: This is Kimberly
7 Keithline. By the 25th, April 25th.

8 MR. MARION: Okay. And we have industry
9 participation on each of the task working groups that
10 Mike Mayfield identified. And those activities are
11 going well.

12 There are two groups -- two of the task
13 working groups that aren't as developed or haven't
14 gone as far as the others. And they are in human
15 factors and digital PRA. And we'll have some comments
16 about digital PRA this afternoon. The human factors
17 group is meeting today so hopefully they will better
18 define the problem statements and milestones and near-
19 term deliverables.

20 CHAIR APOSTOLAKIS: Excuse me, Alex. The
21 Steering Committee consists of NRC people only, right?

22 MR. MARION: Yes.

23 CHAIR APOSTOLAKIS: And they have a --

24 MR. MARION: And they have public meeting
25 with the industry -- there have been three meetings

NEAL R. GROSS

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

1 thus far.

2 With regard to diversity and defense-in-
3 depth, the task working group is using a deterministic
4 approach in addressing the issues with regard to those
5 concepts. We're okay with that in terms of a process
6 and how to address the issues that need to be
7 identified so that we are confident with the
8 appropriate level of diversity and defense-in-depth in
9 the design of digital systems.

10 We need to stay focused and we are working
11 on a screening approach but it is very important that
12 this set of issues regarding diversity and defense-in-
13 depth be resolved as soon as possible because it is
14 fundamental to the design of these systems and we go
15 forward. And it is extremely important for both new
16 plants as well as the current operating fleet.

17 Branch technical position was recently
18 revised. And we recognize the staff was on a highly
19 expeditious schedule to finalize that document and
20 release it to the public.

21 There are additional comments that we have
22 on that document and we intend to work very closely
23 with the task working group to address those comment.
24 And hopefully make some additional changes to that
25 branch technical position.

NEAL R. GROSS

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

1 The problem statements that have been
2 identified by this particular working group are
3 adequate and sufficient from the industry position and
4 we are prepared to work with the staff in addressing
5 and completing the milestones that have been
6 identified.

7 There are two items that need to be
8 addressed as we go forward on resolving diversity and
9 defense-in-depth issues. One is where do you need it?
10 And how much of it do you need? And by the latter
11 point, how much diversity and defense-in-depth is
12 necessary to meet the standard of reasonable
13 assurance? And that is something that we are going to
14 focus on in our interactions with the staff going
15 forward.

16 Hopefully as the result of the
17 presentations this morning with regard to diversity
18 and defense-in-depth, we'll get a reasonably good idea
19 of where the staff is focused.

20 We intend to develop technical papers on
21 the issues that have been developed. We have already
22 agreed to develop one on manual operator actions and
23 the timing aspect. And we are also going to be
24 developing one on digital components and their
25 susceptibility to common-cause failures.

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 We are continuing to look for
2 opportunities to collaborate with the Office of
3 Research. We are focused clearly on collaborating in
4 those areas where there is a practical value-added
5 proposition to the results of the research in terms of
6 advancing the state of knowledge of the technology or
7 addressing issues that need to be addressed so that
8 the licensing of these systems can go forward for new
9 plants as well as current plants.

10 We have also agreed to do pilot
11 applications of some of the fundamental design
12 concepts. One of the plants has agreed to work
13 closely with the NRC on the reactor protector system
14 digital upgrade. And we're looking forward to the
15 interactions. We're looking forward to the briefings
16 that you will hear from the staff today.

17 We may have a comment or two at the end of
18 the morning session so if time allows, I'd like to
19 have the opportunity to comment on the subject matter
20 that the NRC staff presents. And that is all we have
21 to say about that first topic.

22 CHAIR APOSTOLAKIS: The technical papers
23 that you mentioned, these will propose specific ways
24 of checking for the need for defense-in-depth and
25 diversity or what will they do?

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 MS. KEITHLINE: This is --

2 CHAIR APOSTOLAKIS: Yes, okay, go ahead.

3 MS. KEITHLINE: This is Kimberly
4 Keithline. One of the papers that we have
5 specifically discussed is related to developing a
6 process by which you could determine what to assume.
7 What would be a reasonable assumption for operator
8 response times just as they relate to your diversity
9 and defense-in-depth evaluation.

10 We recognize that the NRC staff has a lot
11 of work and they are in the process now of trying to
12 hire people so that we felt that if there are
13 recommendations that we can make or proposals for
14 approaches to resolve some of these issues, that may
15 help the resolution along.

16 It will be, of course, up to them to
17 decide whether they want to accept any of our
18 recommendations. But that is one specific one would
19 be to recommend a process by which we could determine
20 acceptable operator response -- acceptable from the
21 standpoint of are they reasonable? Are they best
22 estimate? Can they really be used in the diversity
23 and defense-in-depth evaluation?

24 CHAIR APOSTOLAKIS: Well, it is my
25 impression that branch technical position as it is now

1 is fairly general. One could do a lot of things under
2 it to demonstrate adequacy. And also it's using an
3 approach that was described in a NUREG from 1994.

4 I'm wondering whether the industry is
5 planning to propose specific methods that have been
6 developed more recently in the last 13 years or so to
7 actually address the two questions that Mr. Marion
8 raised.

9 And I was -- you know after I saw this
10 1994, I just went to a website or a couple of
11 journals. And my goodness, I mean there are so many
12 papers that have come out. I mean there is a lot of
13 work going on in Taiwan using simulators, evaluating
14 the -- in fact, their first reference is the BTP. So
15 the NRC says this. Let's do it. And they went to
16 simulators and they evaluated the potential for
17 various common-cause failures.

18 So I'm wondering whether there is anything
19 in those methods -- not necessarily this particular
20 one but people have done a lot of thinking that could
21 be used.

22 MS. KEITHLINE: Right. And I think Mike
23 Waterman will probably tell you that as part of the
24 current research that NRC is doing, they are looking
25 at what has been done, what is being done outside --

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 well, outside of our U.S. nuclear industry and outside
2 maybe of the nuclear industry to try to build on what
3 has been done in this area.

4 CHAIR APOSTOLAKIS: But the industry is
5 not planning to do anything along these lines. So you
6 don't know yet.

7 MR. MARION: Well, no -- yes, this is Alex
8 Marion. As Kimberly indicated, the NRC is doing some
9 work in this area and I believe we'll hear details
10 from Mike today.

11 We have international participation in
12 EPRI. And EPRI is doing a lot of technical work for us
13 in this particular area. And they are receiving input
14 from some of those international members in terms of
15 what they have done in implementing this technology.

16 I don't know if Ray wants to add any
17 further detail. This is Ray Torreck.

18 MR. TORRECK: I'm Ray Torreck from EPRI.
19 Yes, we've been working in this area for a number of
20 years now for both deterministic approaches and risk-
21 informed approaches. And we will -- we are applying
22 some of that in working with NEI now. So we're
23 continuing to incorporate insights from that work as
24 appropriate.

25 CHAIR APOSTOLAKIS: Incorporating insights

NEAL R. GROSS

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

1 into where?

2 MR. TORRECK: Into like the white papers
3 that Kimberly mentioned that we will be preparing for
4 NEI and so on. So we will factor that in.

5 MS. KEITHLINE: Ray, I should probably
6 point out there are also two aspects or we could
7 divide the diversity and defense-in-depth issue into
8 two parts. One would be the as purely-deterministic-
9 as-one-can-be approach, which is the subject of this
10 morning's discussions. And then another would be
11 applying risk insights or risk informing even to take
12 it to maybe an extreme the diversity and defense-in-
13 depth evaluation process.

14 EPRI has done some work that may be very
15 applicable, especially in that second category with
16 using risk insights and risk informing. And that will
17 be more related to this afternoon's discussion.

18 MEMBER KRESS: When you say deterministic
19 system, you are referring to the application strictly
20 in design basis accidents and using the well-known
21 concepts of conservatisms and specifications.

22 MS. KEITHLINE: Right.

23 MEMBER KRESS: That's what you mean by
24 deterministic?

25 MS. KEITHLINE: Yes. With the caveat or

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 further explanation that the diversity and
2 defense-in-depth evaluation described in BTP-19 has a
3 different design basis that the regular loss of
4 coolant analysis.

5 In other words, when you assume the
6 common-cause failure and evaluate the systems that way
7 per BTP-19, you don't evaluate to the acceptance
8 criteria in 10 CFR 50.46. You can use 10 CFR 100 dose
9 criteria.

10 So it is a --

11 MEMBER KRESS: But it is still strictly
12 deterministic.

13 MS. KEITHLINE: But it is still
14 deterministic, yes, it is.

15 CHAIR APOSTOLAKIS: That is why it is
16 called deterministic without the benefit of
17 probabilities. That's what it is.

18 Somebody want to comment?

19 MR. ARNDT: I was just going to highlight
20 the fact that we are going to talk about some of these
21 issues in our presentation --

22 CHAIR APOSTOLAKIS: I understand that,
23 Steve. But what I'm trying to understand is is BTP is
24 going to be influenced by all this work that we will
25 be presenting this afternoon? Or is it going to stay

NEAL R. GROSS

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

1 the way I saw it?

2 MR. ARNDT: The purpose of the task
3 working groups are to develop potentially new staff
4 positions through our interactions with the industry
5 and Research.

6 CHAIR APOSTOLAKIS: So it is the job of
7 this Steering group to oversee all this effort? And
8 the branch technical position that we have now is
9 subject to change? Is that the correct understanding?

10 MR. ARNDT: That is correct.

11 MR. MAYFIELD: Mr. Chairman, let me --
12 from a non-I&C person's perspective, I just keep
13 getting drug in the middle of this, the way I see this
14 is that the branch technical position, the review
15 guidance that exists today could lead to licensing an
16 I&C system. However, that would not allow the
17 designers, the industry to take advantage of all the
18 features and capabilities that are available today.

19 So there has been a lot of dialogue with
20 the industry as well as among the staff on how far can
21 we go to change the approaches that the staff has had
22 for a number of years. And at the same time, not give
23 up critical pieces of safety. And the safety
24 structure that we have.

25 So we're very interested in pushing this

NEAL R. GROSS

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

1 forward. The industry obviously has both the safety
2 and an economic interest in pursuing these areas. Our
3 primary role is to assure that safety isn't
4 compromised and at the same time to facilitate moving
5 forward as far as we can reasonably go.

6 So that is what we're looking at. And
7 yes, all of these -- the SRP section, the branch
8 technical positions, the associated regulatory guides
9 have the potential of being revised.

10 CHAIR APOSTOLAKIS: So today's meeting,
11 the purpose of today's meeting is to actually discuss
12 ideas as to how to proceed to do these things?

13 MR. MAYFIELD: I think it is to inform the
14 Subcommittee about where the staff is going and to
15 seek input from you if you see a flaw or a better way
16 to go at it.

17 MR. ARNDT: And to provide you information
18 to support your letter to the Commission in this area.

19 MR. MARION: Which, of course, will be
20 highly supportive of the staff's effort.

21 CHAIR APOSTOLAKIS: As it usually is.

22 MR. MARION: As it usually is.

23 MEMBER MAYNARD: A couple of questions.
24 Back on the technical papers, George asked a question
25 a while ago and I'm not sure it was clearly answered.

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 These papers will be based on today's current standing
2 of the technology not based on 1994's understanding
3 the situation, right?

4 MS. KEITHLINE: That's correct, yes.

5 MEMBER MAYNARD: And do you have a
6 schedule or milestones? Or when would you planning to
7 issue the paper? What time frame?

8 MS. KEITHLINE: All right. We're
9 currently in the processing of developing those
10 details. NRC has given us a draft project plan with
11 milestones and deliverables. But the dates need to be
12 filled in. And then specifically for each item when
13 we will submit things.

14 So we don't have a final detailed, dated
15 schedule yet. Probably by sometime --

16 MR. MARION: Yes, this is Alex Marion.
17 I'm hoping within the next month or so, we can have an
18 agreement on the schedule. We have a meeting of our
19 working group tomorrow. We're going to review the
20 project plan and do what Kimberly just suggested in
21 terms of putting in our thoughts on the schedule. And
22 then we will convey that to the NRC in our letter next
23 week.

24 CHAIR APOSTOLAKIS: So things are still in
25 a state of flux, right?

1 MS. KEITHLINE: Being developed.

2 MR. MARION: I wouldn't characterize --
3 this is Alex Marion again -- I wouldn't characterize
4 it as a state of flux. I think we are working very,
5 very hard in the same direction, making sure we
6 understand what the expectations are relative to
7 milestones and deliverables and schedules.

8 CHAIR APOSTOLAKIS: Just to make clear
9 though where I come from because I don't want you to
10 think that I am a crazy academic who wants the latest
11 paper implemented, I realize, I fully realize that a
12 lot of these methods are just academic exercises or
13 work in progress.

14 But I do think, though, there is a lot of
15 good stuff there that we can take and implement and go
16 beyond the 1994 report, especially in the area of
17 identification of potential failure modes of the
18 system that involves digital I&C.

19 When it comes to probabilities, yes, I'll
20 be the first one to say that we shouldn't really touch
21 it at this point. But the failure mode part, it seems
22 to me, there have been some pretty good ideas and
23 applications and so on. So what I'm asking is really
24 somebody ought to look and decide, you know, if A, B,
25 F, and G are good, we can use them. The other stuff

NEAL R. GROSS

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

1 is still in development. We can wait. That's really
2 my position.

3 Thank you very much.

4 MR. MARION: Thank you.

5 CHAIR APOSTOLAKIS: Unless you have
6 something else to say?

7 MR. MARION: No, that's fine.

8 CHAIR APOSTOLAKIS: No? Thank you very
9 much.

10 MEMBER KRESS: You could still be a crazy
11 academic.

12 CHAIR APOSTOLAKIS: I could.

13 (Laughter.)

14 CHAIR APOSTOLAKIS: The next presentation
15 is from the NRC on the current regulatory position on
16 diversity and defense-in-depth by Mr. Loesser.

17 MR. LOESSER: Loesser.

18 CHAIR APOSTOLAKIS: Loesser.

19 MR. MARION: Mr. Chairman, if I could,
20 just before Paul get started, we have got a number of
21 presenters before the Subcommittee today. And I know
22 in the past you've asked some questions about just who
23 are these people and why are they standing up in front
24 of you.

25 So we wanted to share with you. I would

NEAL R. GROSS

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

1 tell you we brought the A Team but I really don't have
2 a B Team. We've been very fortunate in hiring some
3 very talented people. And several of them are going
4 to be talking to you today.

5 I'll start with Paul. He's got a fairly
6 diverse background in design. And he's been with the
7 NRC since 1990 doing technical reviews. He has a
8 diverse background in the design of computer systems
9 and control systems.

10 Gene Eagle has also a nearly 30-year
11 background in the nuclear industry as well as in
12 significant design activities. He's only been with us
13 about a year.

14 Mike Waterman has been talked about a
15 number of times. And I think he has presented before
16 the Subcommittee as well as the full Committee in the
17 past. He also brings about a 30-year background
18 coming to us from the Idaho National Engineering
19 Laboratory.

20 Cliff Douth is going to be talking to you
21 this afternoon. He is a member of the Risk Informed
22 Task Group. He's been involved in a wide extent of
23 both digital I&C as well as PRA activities.

24 Steve Arndt I won't bother to introduce to
25 you. He's presented before the Committee a number of

NEAL R. GROSS

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

1 times.

2 And Alan Kuritzky has 25 years' experience
3 in the PRA area. And he is going to be talking to you
4 this afternoon.

5 So that's sort of -- I think Richard Wood
6 is also here. He's from Oak Ridge and is going to be
7 supporting us as we go along.

8 So we've brought a fairly broad range of
9 folks with a lot of years of experience and diverse
10 experience. So with that, we'll turn it over to Paul.

11 CHAIR APOSTOLAKIS: Thank you.

12 MR. MARION: Paul?

13 MR. LOESSER: My intended presentation
14 here is to explain what the current position on
15 diversity and defense-in-depth is. That is the
16 position from which the working groups and all that
17 are starting. What we have done to date.

18 The safety concern that we were worried
19 about is that an error in common software could cause
20 all the different channels in the protection system
21 where the software is used to malfunction at the same
22 time. And the fact that a number of safety functions
23 are being handled by the same four-channel system has
24 increased this concern.

25 We feel that high quality design is still

1 the most important method to defend against common
2 mode failure or, for that matter, any kind of failure.
3 And high quality hardware and software will reduce the
4 failure probability.

5 However, despite high quality software,
6 this only reduces the probability. It does not
7 totally eliminate it. And as such, software errors
8 may still defeat the safety functions in redundant
9 safety-related channels.

10 This idea was confirmed by the 1997
11 National Academy of Science Report on I&C Systems in
12 Nuclear Power Plants. Their conclusion was that the
13 NRC position of assuming that a common mode failure
14 could occur was credible, that it conforms to
15 engineering practice and it should be retained, and
16 their recommendations echo this, that the position is
17 credible and that we should maintain our position
18 regarding the need for diversity in digital I&C
19 systems.

20 The basis for our policy of diversity and
21 defense-in-depth stems from a number of places.
22 Intense CFR 50.55a(h) protections and safety systems -
23 -

24 CHAIR APOSTOLAKIS: What do you mean by
25 basis?

NEAL R. GROSS

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

1 MR. LOESSER: This is the legal reason why
2 we think that we can require this.

3 CHAIR APOSTOLAKIS: Is there also a reason
4 somewhere that says we looked at past experience and
5 this is what we have found? And yes, there is a
6 problem with common-cause failures?

7 MR. LOESSER: There have been a number of
8 studies -- I don't think I mention any of them here --
9 where we have looked at past studies. Research has
10 done some work where they have looked at failures in
11 power plants in the past and have found quite a few
12 which could have been -- had the potential for causing
13 a common mode failure.

14 CHAIR APOSTOLAKIS: That's the thing. I
15 think we need a good discussion of the operating
16 experience because this is really what gives you
17 insights, not the legal documents.

18 MR. LOESSER: Okay, well --

19 CHAIR APOSTOLAKIS: Are they real common
20 cause failures? Were they -- did they have the
21 potential of becoming common-cause failures? I went
22 back to a presentation from Brookhaven, I believe,
23 last time we met here. And I remember the number of -
24 - 11 common cause -- potential common-cause failures.

25 MR. KEMPER: Yes, this is Bill Kemper. L

NEAL R. GROSS

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

1 Yes, George, you are right. Absolutely. We discussed
2 that at one of our previous meetings with you all.
3 Mike Waterman has prepared a table of many of those.

4 CHAIR APOSTOLAKIS: Will we have a
5 discussion this afternoon on this?

6 MR. KEMPER: Unfortunately, we hadn't
7 planned to do that. But we can talk maybe
8 extemporaneously about it.

9 CHAIR APOSTOLAKIS: Yes, isn't this --

10 MR. KEMPER: Okay, maybe we can get a
11 slide quickly, you know, and talk about it later on
12 after the break maybe.

13 CHAIR APOSTOLAKIS: I think the
14 Subcommittee would benefit a lot from actually seeing
15 real data as to what we mean by common-cause failure
16 in this new domain. And I remember was it you Steve
17 or Dr. Chi who made the presentation?

18 MR. ARNDT: It was Dr. Chi. But the data
19 has been analyzed by a number of people --

20 CHAIR APOSTOLAKIS: Okay.

21 MR. ARNDT: -- including us. And what we
22 can do -- we've intentionally included a short section
23 at the end of the D3 on general discussion.

24 CHAIR APOSTOLAKIS: Yes?

25 MR. ARNDT: And we'll get some information

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and we'll --

2 CHAIR APOSTOLAKIS: That would be great --

3 MR. ARNDT: -- shoe horn it in.

4 CHAIR APOSTOLAKIS: -- because I think it
5 is going to provide tremendous insight to the members.
6 Remember this is a data-driven Committee.

7 MR. ARNDT: Yes, I understand. Just a
8 quick logistical issue before we go on, what we have
9 here is Paul is going to talk about the current
10 position and how we got there. Gene is going to talk
11 about our activities going forward. And then Mike is
12 going to talk about the research. Then we've got a
13 short general discussion where we can talk about these
14 things.

15 CHAIR APOSTOLAKIS: Okay.

16 MR. ARNDT: One other issue, the primary
17 purpose here is the D3 stuff. So if we have to slip
18 the afternoon a little bit, that's fine.

19 CHAIR APOSTOLAKIS: And I agree with that.
20 I think the diversity issue and defense-in-depth is
21 extremely important.

22 MR. ARNDT: Okay.

23 CHAIR APOSTOLAKIS: That's why I really
24 want the discussion of the experience as well.

25 MR. ARNDT: Okay.

1 CHAIR APOSTOLAKIS: Sorry to interrupt.

2 MR. LOESSER: Unfortunately, I am --

3 CHAIR APOSTOLAKIS: Actually I'm not
4 sorry.

5 MR. LOESSER: -- I am not prepared at this
6 moment to discuss the experience.

7 CHAIR APOSTOLAKIS: I understand.

8 MR. LOESSER: But I think we can be at a
9 later time.

10 CHAIR APOSTOLAKIS: But I think it is
11 important also to express the view of the Subcommittee
12 I believe. I see my colleagues are nodding.

13 MR. LOESSER: The policy also derives from
14 a SECY paper, 93-087, where a four-point position on
15 the common mode failure for I&C was given. And this
16 was modified somewhat by the Commission's Staff's
17 Requirements Memorandum dated July 21st, '93.

18 And it basically says that the applicant
19 needs to assess the diversity and defense-in-depth,
20 demonstrate that the vulnerabilities to common-cause
21 failure have been addressed, that while performing
22 this assessment, they should analyze each postulated
23 common mode failure in conjunction with each event
24 evaluated in the accident analysis using best estimate
25 methods. And the vendor can then demonstrate adequate

NEAL R. GROSS

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

1 diversity exists.

2 CHAIR APOSTOLAKIS: I guess the key here
3 is to postulate the appropriate common-cause failures,
4 right?

5 MR. LOESSER: Yes.

6 CHAIR APOSTOLAKIS: Which is what Mr.
7 Marion meant I think by saying where.

8 MR. LOESSER: In general the way it has
9 been done to date is just to assume failure of the
10 software. And that whatever protective function is
11 supposed to be wouldn't occur.

12 There are other ways where you could
13 assume certain types of failure but those are
14 significantly more difficult to do. And the
15 licensees, I don't think, have chosen that route so
16 far. When they do, we will, of course, evaluate what
17 they have and tell them if we believe that their
18 analysis was adequate and correct or if it was not.

19 CHAIR APOSTOLAKIS: But I suspect though
20 that in postulating common-cause failures people are
21 heavily influenced by the corresponding work on
22 hardware where essentially you look at similar
23 components in the same system and you say yes, if I
24 have two trains and they are nominally identical, and
25 we have their pumps, I may have a common-cause failure

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 of the pumps or of the valves and so on. For example,
2 we don't look at -- or we rarely look at similar
3 components in different systems and so on.

4 But these are hardware failures. I wonder
5 whether there are unique features here with software
6 where, you know, we have a broader set of potential
7 failures.

8 MR. LOESSER: I think there certainly is.

9 CHAIR APOSTOLAKIS: That's why operating
10 experience really helps.

11 MR. LOESSER: I think there certainly is
12 a difference. First of all, when we are talking about
13 a particular I&C system, the hardware has often been
14 used many times before and has a fairly definitive
15 history behind it.

16 For example, if you use a Pentium chip,
17 there's what -- a 50-, 100-million of them used
18 throughout the world, possibly more. And there are
19 known failures but -- there are known problems with
20 the Pentium but they are known. There might be some
21 unknown ones but that's based on history.

22 However, if you write new software for a
23 plant for a particular functions and this is the first
24 time the software has operated, you don't have a
25 history on it. So you have to approach it a little

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 bit differently.

2 There are some differences between
3 hardware and software. And that is part of what the
4 diversity and defense-in-depth group is trying to look
5 at. What do we need to consider? How do we need to
6 consider it? What are the issues involved? And
7 frankly, I don't have a total answer at this point.
8 I have personal opinions but I can't prove a lot of
9 what I believe.

10 CHAIR APOSTOLAKIS: But your personal
11 opinions would be useful, too.

12 MR. LOESSER: Well, in my opinion,
13 something that is being used for the first time has a
14 higher probability of having a problem with it than
15 something that has been used many times. That is one
16 issue.

17 Second of all, I believe that sufficiently
18 complex software will have a problem in it somewhere.
19 I don't know what that problem is yet but if you are
20 running to a half a million lines of code, it is very
21 difficult to find all the issues. We can find most of
22 them.

23 I think virtually every digital system we
24 have approved in the past, despite the high quality,
25 has later on been found to have some sort of issue.

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 In some cases, it is a trivial one. In some cases it
2 is a more important one. But some sort of problems
3 have slipped by the entire quality control, the entire
4 V&V teams, all of this. And I think we need to
5 continue with that assumption that sufficiently
6 complex software will have an issue.

7 It is the same with hardware.
8 Sufficiently complex hardware will have an issue. And
9 the experiences, for example, of the Pentium show
10 this. However, as you have a whole bunch of operating
11 experience, you get to know what those issues are, can
12 fix them, can work around them or something like that.

13 So those are just a few of them. I have
14 many more which I will be happy to get to as we go in
15 here.

16 CHAIR APOSTOLAKIS: Let's go on. But the
17 point of this and the point of all the report and the
18 current BTPs, somebody has to postulate a potential
19 common-cause failure and then you verify that you have
20 adequate protection using 10 CFR 100 and so on. And
21 there isn't --

22 MR. LOESSER: Back to the third point here
23 --

24 CHAIR APOSTOLAKIS: -- there isn't a
25 requirement to have a methodology for searching for

1 potential common-cause failures. That is my
2 understanding from reading the document and our
3 discussion this morning.

4 MR. LOESSER: Well, actually the entire
5 quality control process we use or we require licensees
6 or vendors to use during the design, the V&V, the
7 testing, the quality control, the configuration
8 management, all of those are intended to find and fix
9 errors before the software is fielded.

10 The problem is this system is not perfect.
11 And problems work their way through it anyway. We do
12 have a method for trying to find and fix errors.
13 Otherwise we could use -- I don't know -- Windows
14 straight off the shelf.

15 CHAIR APOSTOLAKIS: What method is that?

16 MR. LOESSER: That is high-quality design,
17 thorough test, V&V, independent to some degree. And
18 I think all of those do a reasonably good job of
19 producing high quality software. But high quality is
20 not the same as perfect.

21 The third position, that if a postulated
22 common mode failure could disable a function, then a
23 diverse means needs to be provided to take care of the
24 same kind of thing. The diverse function, however,
25 could be performed by a non-safety system if 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 system is of sufficient quality to perform the
2 necessary function under the associated conditions.

3 And the fourth position is that despite
4 all of this, a set of displays and controls in the
5 main control room will be provided from manual system
6 level actuation of the critical safety functions. And
7 these displays or controls will be independent and
8 diverse from the computer systems identified in Items
9 1 and 3 that I just spoke about.

10 MEMBER ABDEL-KHALIK: How would you verify
11 this word sufficient?

12 MR. LOESSER: In which --

13 MEMBER ABDEL-KHALIK: In the first bullet
14 -- Bullet No. 3 -- one, two, three, four, fifth line?

15 MR. LOESSER: You are talking about
16 sufficient quality?

17 MEMBER ABDEL-KHALIK: Right.

18 MR. LOESSER: That is an issue. We, to
19 tell you the truth, haven't done it yet because we
20 haven't gotten to that phase where someone has
21 presented us the diverse system.

22 However, what I would expect is that while
23 it would not be safety related, it would be a
24 deliberate and careful design effort, good quality
25 testing, and this type of thing, very similar to what

NEAL R. GROSS

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

1 we required of the ATWS systems, which is documented
2 in General Letter 85-06.

3 I expect that some time in the future, we
4 will have to promulgate this in some way saying this
5 is what we really mean by high quality or sufficient
6 quality. But so far we don't have an official
7 statement on what that means. I think this is one of
8 the things that is lacking and one of the things we
9 need to do in the next few months or as soon as we can
10 get around to it.

11 MR. KEMPER: This is Bill Kemper. If I
12 could just offer something from my experience in the
13 industry, typically -- well, many times, not
14 necessarily the process but many times this is handled
15 in an augmented quality-type of analysis where
16 critical characteristics would be established or
17 identified for the requirements or the performance of
18 the system.

19 And then those requirements would be
20 institutionalized and preserved in terms of the
21 quality requirements for that piece of equipment even
22 though it is not safety related, if you will. And
23 licensees often refer to that as augmented quality.
24 That is the way it is characterized and labeled within
25 their system. And those are the critical

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 characteristics that they will preserve for the life
2 of the equipment if that helps.

3 MEMBER ABDEL-KHALIK: Thank you.

4 CHAIR APOSTOLAKIS: So sufficient quality
5 does not refer to any digital I&C that is in that
6 diverse system. Sufficient quality means that, for
7 example, if it is a cooling system, it can actually
8 cool the core?

9 MR. LOESSER: No, actually where we are
10 talking about the I&C system that we could use as the
11 diverse system, which would be credited in the event
12 of a common-cause failure.

13 CHAIR APOSTOLAKIS: So someone then has
14 done to that system what the three points -- or the
15 four points require. I mean --

16 MR. KEMPER: So, for example, if I could,
17 say we want this to have a reliable power supply, that
18 would be a critical characteristic that is identified
19 for this non-safety equipment. Typically in a non-
20 safety world, we don't address those things, right?
21 If it fails, it fails.

22 So the designer would then take it upon
23 him or herself to put in a reliable power source for
24 this non-safety piece of equipment. It could be a
25 UPS, you know, something like that.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: But that's not I&C.

2 Is it I&C?

3 MR. KEMPER: Well, no, that is
4 specifically to power the I&C system. That is just
5 one example.

6 CHAIR APOSTOLAKIS: Well, it's not
7 entirely clear to me.

8 MEMBER MAYNARD: Yes but there has been a
9 lot of experience dealing with it. It would be better
10 if there was a little more clarity as to really what
11 constitutes it. But there has been many other things
12 that we have in the industry between the regulator and
13 the user of things that aren't safety related but they
14 are important to safety or they are augmented quality
15 or there are other ways to do it.

16 But they kind of almost have to be
17 discussed and negotiated on a case-by-case basis
18 rather than have them --

19 MR. LOESSER: That's why I mentioned the
20 ATWS system where something has been written down in
21 the past and has been applied. And we could do --
22 either use the same criteria or after discussion with
23 EPRI and NEI and other industry representatives,
24 modify this somewhat.

25 What I was saying is that this has not yet

NEAL R. GROSS

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

1 been done and is something that is going to be
2 required in the future.

3 Just as some background, the way we got to
4 this area, when we were thinking about the existing
5 operating plants back in the early '90s, we assumed
6 that digital system would replace analog systems
7 pretty much one function at a time. And the digital
8 systems would perform only one safety function.

9 That is, in fact, the kind of replacements
10 we were getting in '95, '98. And that other analog
11 systems would still be available. And that the D3
12 analysis for operating plants would be comparatively
13 simple.

14 We would show that if one safety function
15 didn't mitigate the accident that another one would.
16 That is if you didn't trip on the level in the reactor
17 vessel, you could trip on the pressure for a
18 particular accident or occurrence.

19 The current digital upgrades, however, use
20 many safety functions and in some cases all of them in
21 one four-channel digital system. The diverse analog
22 systems are no longer available. The D3 analysis does
23 often show that some diversity is required.

24 And this now leads to the question of
25 exactly how diverse must the diverse system be? What

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 kind of quality do we need? And those are the reasons
2 why we have all these issues today.

3 MEMBER MAYNARD: But with the current
4 digital upgrades, aren't they still required to have
5 like the AMSAC or the ATWS --

6 MR. LOESSER: Yes, they are still required
7 to have --

8 MEMBER MAYNARD: So there is still some --
9 it has not taken away all of the current diversity.

10 MR. LOESSER: No, I said it was the safety
11 functions. The ATWS systems are generally no safety
12 functions. But, for example, we have had an applicant
13 who wanted to put all the ESF and all the RPS
14 functions together into one four-channel system where
15 one common mode failure would take out the whole lot.

16 So if you did have a software failure
17 which stopped the system as an example, froze it, none
18 of these functions would be available. The question
19 is what does the plant do now? And that is what the
20 diversity and defense-in-depth analysis is supposed to
21 show.

22 The primary difference between the SECY
23 paper that originally went up in '93 and the SRM deals
24 with the common cause software failures. The SRM says
25 that common-cause failures are beyond design basis.

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 as such, the analysis needs to be on a best
2 estimate basis.

3 The result of this is that the diverse or
4 different functions may be performed by a non-safety
5 system and that the analysis can be done on a best
6 estimate basis and that the displays and controls
7 required by the fourth point, the independent displays
8 and controls, do not need to be safety grade.

9 The current policy is that the applicants
10 need to perform a diversity and defense-in-depth
11 assessment. They need to analyze design basis events
12 as identified in the SAR.

13 If a postulated common-cause failure could
14 disable these functions, required to respond to a
15 design basis event, then a diverse means of response
16 needs to be present with a documented basis. And that
17 the diverse means could be non-safety. And once
18 again, we have the if the sufficient quality to
19 perform the necessary function is there.

20 NUREG-6303 from December '94, as you
21 pointed out, which is now 13 years old, does show an
22 approved method for performing the diversity and
23 defense-in-depth analysis.

24 CHAIR APOSTOLAKIS: But that -- I mean
25 there are methods and methods.

1 MR. LOESSER: Yes.

2 CHAIR APOSTOLAKIS: And my opinion is that
3 it is a very high-level method. I mean you can do
4 anything you want under it. Essentially it says look
5 up a block diagram and try to figure out what
6 interactions are. I mean unless I'm missing
7 something, it's a fairly general --

8 MR. LOESSER: No, you are absolutely
9 correct. Like any other NUREG, this is one method we
10 have looked at and approved. Certainly if the
11 licensees have a different way of doing a diversity
12 and defense-in-depth analysis, they can propose it.
13 And if they do a good job of it and it actually
14 accomplishes what is needed, that is to show that
15 diversity is there or diversity is not there, we would
16 review it and accept their methodology.

17 If they don't have a reasonable argument
18 as to why this is the case, then we would then reject
19 it. I think that is pretty much what we're required
20 to do.

21 CHAIR APOSTOLAKIS: And my hope is that as
22 a result of the research that the Office of Research
23 has undertaken and perhaps the efforts of EPRI and
24 NEI, we will be able sometime in the near future to be
25 more specific as to what methods could help and how

NEAL R. GROSS

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

1 and so on.

2 MR. LOESSER: I mean to be honest, when it
3 comes to a diversity and defense-in-depth analysis,
4 when you are trying to decide if two different systems
5 are diverse, I think an awful lot of the stuff in 6303
6 goes to a level that is not really needed.

7 If you were looking at two different
8 systems, and they really are different, they have
9 different microprocessors, come from different
10 companies, are programmed in different languages, you
11 can be fairly sure they are different. Granted they
12 may buy their resistors and capacitors from the same
13 vendor but this doesn't effect software and wouldn't
14 effect the software common mode failure.

15 I think in most cases, the question is not
16 are two different systems diverse. The real question
17 is do we need a diverse system. And that's something
18 different than what 6303 discusses.

19 MEMBER ABDEL-KHALIK: The National Academy
20 study, one of their conclusions stated that there
21 appears to be no generally applicable effective way to
22 evaluate diversity between two pieces of software
23 performing the same function.

24 Now so whether this second system is
25 safety or non-safety, there still has to be 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 determination that these two sets of software are
2 diverse.

3 MR. LOESSER: Yes. There is a couple --

4 MEMBER ABDEL-KHALIK: Is this statement
5 still applicable?

6 MR. LOESSER: I think there are ways of
7 determining if it is diverse. There may be some
8 issues deep down such as those that Nancy Levinson's
9 studies have talked about.

10 But if you are talking about two different
11 pieces of software, if they are derived from different
12 specifications and we know that specification failure
13 is one of the major problems with software, so if they
14 both use the same specification and there is a
15 specification error, they would both have the same
16 thing, assuming that they are correct and that
17 specification is implemented.

18 But if they have two different
19 specifications, if they have two different coding
20 teams, if there is human diversity between the people
21 performing the functions, if the hardware that it is
22 being run on, if, for example, the compiler and the
23 software, if they are programmed in different
24 languages, if there is a method made to avoid the same
25 kind of logic, I think you can be fairly certain 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 they are diverse.

2 Granted Nancy Levinson is of the opinion
3 that even if all this is done, since universities tend
4 to teach the same programming techniques, the same
5 techniques will be used throughout and there will be
6 a degree of commonality but I don't think you can ever
7 get a perfect determination. But I think you can
8 certainly get a reasonable determination that this is
9 unlikely to be subject to the same common-cause
10 failure.

11 CHAIR APOSTOLAKIS: So ultimately you have
12 to risk inform this one way or another, somehow.

13 MR. LOESSER: I wouldn't say risk inform -
14 - 10 CFR, by its very nature uses words like it is
15 unlikely or highly -- that the function is highly
16 probably or something like this. And this was used
17 long before the concept of PRA or risk-informed was
18 introduced.

19 And I think there is always a value
20 judgment that has to be made. There is always a
21 certain amount of judgment. And in my opinion, that
22 judgment needs to be documented to the point where a
23 reasonably competent engineer would understand if they
24 read this why you made the decision you did.

25 I will grant you that in engineering, as

NEAL R. GROSS

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

1 in many other fields, there are very few absolutes.
2 It is very difficult to say this is absolutely
3 different from this in every respect. Virtually all
4 semiconductors use silicon. But it is not a software
5 issue. And what we are worried about is primarily
6 software common-cause failure.

7 I would look at the various diversity
8 aspects, which will be on the next slide, and say
9 which --

10 CHAIR APOSTOLAKIS: Okay, let's move on
11 then to the next slide.

12 MR. LOESSER: In the diversity analysis,
13 it says the two systems should be compared for each of
14 the diversity attributes. And those are listed here:
15 design diversity, equipment functional/human, and by
16 human we mean the life cycle processes, not operator
17 action, signal diversity, and software diversity.

18 Then once you have considered all of this,
19 the combined assessment should be used to present an
20 argument that either the system is diverse or it is
21 not diverse. And the basis for claiming these needs
22 to be documents. I think those are all fairly
23 reasonable.

24 I will grant that two different engineers
25 looking at the same two systems might come up with

NEAL R. GROSS

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

1 somewhat different answers but as long as the
2 methodology and thoughts are documented, I think they
3 are understandable and a decision can be made and an
4 agreement can be reached.

5 The acceptance criteria in BTP-19, as it
6 currently is, says that for each anticipated
7 operational occurrence for each postulated common mode
8 failure, you do an analysis using best estimate
9 methods. And that the resulting radiation release
10 should not exceed ten percent of Part 100 guidelines
11 or violate the primary coolant pressure boundary.

12 We do the same thing for each postulated
13 accident in the design basis, use best estimate
14 methods, once again, not allowed to exceed ten percent
15 of the Part 100 guidelines, violate the integrity of
16 the primary coolant, or violate the integrity of the
17 containment.

18 That if a common element or signal source
19 is shared between the control systems and the trip
20 system, and failure of this is postulated where it can
21 create a situation where you need a reactor trip and
22 at the same time impair that reactor trip, then a
23 diverse function needs to be provided to perform the
24 safety function.

25 And the same basis not exceeding ten

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 percent of the Part 100 guidelines or violating the
2 integrity of the primary coolant boundary.

3 Also it says that no failure of the
4 monitoring or display systems, that is the non-safety
5 systems, should influence the functioning of the trip
6 system or the ESFAS. And that adequate diversity --
7 the adequacy of the diversity provided needs to be
8 justified.

9 That is actually my final slide. Are
10 there any other questions I could --

11 CHAIR APOSTOLAKIS: Yes, there is a
12 question that maybe we should discuss in more detail
13 later but maybe you can give us your opinion.
14 Shouldn't we apply the principle of diversity to the
15 review as well? The review itself should use perhaps
16 diverse ways of doing all these things rather than
17 relying on the judgment of one or two guys?

18 MR. LOESSER: Well, in fact, I believe it
19 is. While, for example, if I do the review, I read
20 all the stuff, I write up my opinion but certainly I'm
21 not the guy who signs it. This is then looked at by
22 my boss. And then very often his boss to see if I
23 made a reasonable argument, if I took things into
24 consideration.

25 To be honest, there have been times 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 I have been overridden or my opinion has been -- how
2 do I put it -- modified. There is some diversity in
3 review.

4 Now if you mean we should have two
5 entirely separate reviewers come to the -- look at all
6 this --

7 CHAIR APOSTOLAKIS: That could be one way.

8 MR. LOESSER: That could be one way.

9 CHAIR APOSTOLAKIS: Or two different ways
10 of checking the thing, that could be another way.

11 MR. LOESSER: Any of our significant
12 issues get what we call a peer review. If I do a
13 review, it is read by other reviewers. And they
14 question my logic and my thought pattern. I know I
15 have done it to others. I have had others do it to
16 me.

17 And I have to convince them that I was
18 right. Or the two opinions go up for arbitration to
19 the next level in management.

20 We don't have just one person deciding
21 these things. There is a group or at least more than
22 one person looking at it. So there is a degree of
23 diversity.

24 CHAIR APOSTOLAKIS: Okay.

25 MR. LOESSER: But as far as having two

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 reviewers look at exactly the same thing, to be
2 honest, right now I don't think we have the people to
3 do it. We might in five years. But this all takes
4 time and we have to apportion our time with what is
5 most critical and what is most important to industry
6 to some degree.

7 CHAIR APOSTOLAKIS: Any questions from the
8 members?

9 (No response.)

10 CHAIR APOSTOLAKIS: Thank you very much.

11 We are moving on to the next presentation
12 from the New Reactor Office. Mr. Eagle?

13 MR. ARNDT: While he is getting set up,
14 some of the questions with respect to looking at
15 different diverse attributes and finding more specific
16 ways of doing this are going to be covered by Mike in
17 his discussion of the ongoing research. It is the
18 second presentation on the right.

19 MR. EAGLE: Yes, hello. I'm Gene Eagle
20 with the NRO, Division of Engineering, in Instrument
21 Control, my supervisor being Ian Jung.

22 Our topic today is the NRC activities to
23 address -- our topic today will be looking at the
24 diversity and defense-in-depth issues that we have
25 been working with our task working group.

NEAL R. GROSS

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

1 To start with, we'll look at an overview.
2 We'll look at the problem statements that have been
3 worked together through both the NRC and the industry.
4 We'll take a look at some of the deliverables we are
5 expecting or we will be working on. And then our
6 conclusions.

7 CHAIR APOSTOLAKIS: Just press the arrow.

8 MR. EAGLE: Okay. Our diversity and
9 defense-in-depth working group is made up of
10 representatives from both the NRR office, the NRO
11 office, that is the New Reactor Office, and also from
12 Research. We have links with the NMSS group.

13 We have a very strong group from industry
14 that is backing us up as somewhat like consultants or
15 we've been able to meet with these. And we've met
16 with them several times and we have a good working
17 relationship, as you have already seen, from the talks
18 we had from the people just a few minutes ago.

19 Paul has already presented two of our main
20 things here that we see in the next two bullets -- the
21 basis for diversity and defense-in-depth presentation
22 in regulatory requirements and the guidance that is in
23 place for helping the reviewers. Paul has done an
24 excellent job giving us the background, what is being
25 done right now. And the main point here is that this

NEAL R. GROSS

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

1 has already been used for the certification of new
2 designs.

3 For example, the design of the AP 1000
4 from Westinghouse, the GE's ABWR, the CE ABBs, System
5 80+ are examples of where this certification has been
6 used. And used successfully.

7 Also, it is being used in some of the
8 special I&C-type systems for safety. For example, the
9 Eagle 21 with the Westinghouse area. You've had the
10 NUMAC with GE. You've had the Common Q, which is
11 going to be in the AP 1000. You have the B&W Star.
12 You have the new TELEPERM for the EPR-type reactors.
13 So we have had experience with this.

14 The key here, I think, at this point is
15 that the advances in technology now are pushing the
16 industry and the NRC to design clear and more detailed
17 guidance and being able to use these and being able to
18 provide diversity and defense-in-depth in case we do
19 have common mode failures.

20 What we have done here is to develop a
21 series of problem statements. The overall issue, of
22 course, is that the guidance does not explicitly
23 identify what constitutes acceptable diversity and
24 defense-in-depth in the nuclear facilities and safety
25 system designs. This was pointed out very clearly by

NEAL R. GROSS

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

1 Mr. Loesser in his talks.

2 So what we did was to take a look and
3 bring together, you know, first our groups and talk
4 about what are some of the problems, what are some of
5 the things we are facing? Kind of a round-robin,
6 barn-storming-type effort. And the result was a list
7 of eight problem statements that need to be looked at,
8 that we have examined in more depth.

9 The first one, of course, adequate
10 diversity is the key overall. Additionally, we
11 clarify what constitutes adequate diversity and
12 defense-in-depth for the various systems. However,
13 going further, we're looking at some of the details
14 from the other problems is the manual operator action.
15 We will need to clarify just where can we use and how
16 much can we use the operator to depend on him for a
17 second level or even a primary backup or third level
18 backup in case -- and also what time period do we need
19 to have for him to be able to respond.

20 Now probably the industry mentioned they
21 were going to try to produce a white paper on this.
22 And I think from all our standpoints, we would say
23 this is probably one of those logical -- where do you
24 get the most experienced information from reactor
25 operations is from the people actually operating the

NEAL R. GROSS

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

1 reactors.

2 So this is a major area and we look
3 forward to the information to help from the NEI and
4 the other industry group people

5 Another area is the credit for leak
6 detection. One of the most famous items in accidents
7 is where we assume that the largest pipe in the
8 reactor suddenly disappears, a guillotine break, just
9 suddenly vanishes and water starts pouring out. And
10 the emergency systems turn on and start pumping it all
11 in.

12 Basically one of the comments is is this
13 realistic? Can we back down from this? This is a
14 conservative way of looking at it. Can we back down
15 a little bit and look at it? Maybe there is leakage
16 first. And can we take an credit for that? And in
17 looking at that, this is an area that has been --

18 CHAIR APOSTOLAKIS: Hold on.

19 MR. EAGLE: Yes?

20 CHAIR APOSTOLAKIS: In number two --

21 MR. EAGLE: Yes?

22 CHAIR APOSTOLAKIS: -- I guess the intent
23 there is to see how operators can save the day. But,
24 again, if you look at operating experience, there was,
25 in particular, a common-cause failure that occurred in

NEAL R. GROSS

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

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

-

MR. EAGLE: Three Mile Island?

CHAIR APOSTOLAKIS: No, no, no, it was a combustion engineering plant where the computer technicians inserted an incorrect dataset to all four channels.

MR. KEMPER: Palo Verde in the core protection calculator.

CHAIR APOSTOLAKIS: Yes. Is that kind of common-cause failure -- this is really not a cause, right, it is a common cause, part of all this?

MR. EAGLE: Yes.

CHAIR APOSTOLAKIS: We do worry about all this? The humans and how they can do things that are -- okay -- and this will be addressed somewhere? Or is it being addressed?

MR. EAGLE: This is definitely one of the things that would have to be considered. It is one of the areas, particularly if you have what you call a live-type situation in which the operator, for example, has to insert something.

It is a little bit different if you have engineers that are developing something and maybe getting ready to go through a new cycle and they actually have to insert new constants into the system

NEAL R. GROSS

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

1 to get ready for the new cycle. There you are off
2 line. You are getting ready for it. It's not like an
3 instantaneous thing. Whereas if you have -- where an
4 operator has to put something in and then within a few
5 seconds or a few minutes it is having an effect on the
6 plant, so there are two different looking-type things.

7 CHAIR APOSTOLAKIS: But does the current
8 branch technical position allow for this? Does it
9 guide the reviewer to look for things like that? Or
10 is part of postulating the common-cause failure?

11 MR. ARNDT: It is part of postulating the
12 common mode failure. You can get common mode failure
13 be it software or hardware or integrated
14 hardware/software system, in any of a number of ways.
15 The BTP is an evaluation criteria of do you have
16 sufficient diversity given that you have a failure?
17 What you are talking about is how you get that
18 failure.

19 CHAIR APOSTOLAKIS: Right. So in
20 postulating the failures, people do take these
21 possibilities into account? Or I don't know.

22 MR. LOESSER: We actually don't take --

23 CHAIR APOSTOLAKIS: Please, come. You
24 have to identify yourself again. I'm sorry.

25 MR. LOESSER: Paul Loesser from I&C and

NEAL R. GROSS

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

1 NRR. When we postulate the common mode failure, we
2 don't really consider where it comes from. We just
3 assume there is one.

4 The kind of thing you are talking about is
5 taken care of in Appendix B, which requires high
6 quality and the way Appendix B is implemented. There
7 are a number of things that are done to make sure, for
8 example, if a software code is modified, that
9 regression testing is done, that a number of other
10 tests -- that it goes through the same level of
11 quality control, V&V testing, and this kind of thing
12 to minimize this kind of failure.

13 But once again, while we think high
14 quality can minimize it, it can't totally eliminate
15 these failures. And when you do the diversity and
16 defense-in-depth analysis, it doesn't really matter
17 where the failure came from.

18 Whether it came from the original
19 specification, whether it came from coding error, or
20 whether it came from maintenance error after the
21 system is fielded, it is there. And it is going to
22 cause a problem.

23 CHAIR APOSTOLAKIS: Well, I understand
24 that part. What worries me is when we say postulate
25 a common-cause failure. So I'm wondering how they 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 postulated because it is the issue of completeness in
2 other words. If you miss something, you missed it
3 period.

4 MR. LOESSER: It's, as I said, so far no
5 one has tried to talk about individual types of
6 failure. They postulate overall failure of the
7 system. People haven't gone in and said well, if we
8 have a failure due to coding error in this particular
9 block, this is going to happen. Or if we have a
10 failure in maintenance in putting in new software,
11 this kind of thing will happen.

12 So far the method has just been to
13 postulate the overall the system will fail. This
14 software will fail. What do we do about it? If a
15 more complex analysis was used, we would certainly
16 look at it and do our best to evaluate it.

17 MEMBER MAYNARD: I believe this Item 2
18 here, manual operator actions, what we're talking
19 about is what all operators are trained for is if a
20 limit is exceeded but the reactor protection system
21 didn't do its job, that they are trained to take
22 certain actions, manually tripping the reactor, trip
23 the turbine, or whatever.

24 And I think we're looking for methodology
25 for the time and how much credit can we take for 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 manual operator actions --

2 MR. EAGLE: Yes.

3 MEMBER MAYNARD: -- in the event that the
4 digital I&C system failed.

5 CHAIR APOSTOLAKIS: Right. Which is
6 similar to what we are doing in fires, right?

7 MEMBER KRESS: With respect to the third
8 item up there, I usually view credit for leak
9 detection as a reduction in defense-in-depth and the
10 way to reduce it. And so I don't quite understand
11 what your problem statement means there as it is
12 worded.

13 Are you looking to say eliminate large
14 break LOCAs from the design basis accidents when you
15 talk about diversity and defense-in-depth? I mean
16 just what -- would you expand on Item 3?

17 MR. EAGLE: Well, that's a possibility.
18 In other words, the conservative way that is presently
19 being looked at in the analysis for these new plants
20 is that -- or in older plants was the fact that you
21 assume the largest pipe suddenly just disappeared and
22 then what the resulting loss of coolant that results
23 from that was supposed to be considered one of the
24 worst possible accidents.

25 So then you design your defensive

NEAL R. GROSS

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

1 mechanisms, your engineering safeguards to try to
2 overcome that.

3 One of the things being questioned is --
4 and, again, this might be getting into probabilities,
5 the probability of risk assessment, is this an
6 absolute -- a way of looking at it? Is there ways
7 that perhaps by being able to detect leakage we can
8 start to say that maybe this significantly
9 conservative approach, maybe we could back away from
10 it a little bit and yet still have the safety factors.
11 So this is something that is being looked at.

12 MEMBER KRESS: Okay, you are saying that
13 doesn't -- I think the postulation is that assuming a
14 large break LOCA doesn't add much to defense-in-depth
15 and diversity.

16 MR. EAGLE: Right. Well, see, as far as
17 the -- yes, defense-in-depth here we're talking about
18 that's the physical thing. The thing that probably
19 would be more in concern with the instrument control
20 people would be can you detect that leak.

21 MEMBER KRESS: Oh.

22 MR. EAGLE: And then the instrumentation
23 that doesn't fail --

24 MEMBER KRESS: That would be the issue.

25 MEMBER MAYNARD: But this does not

NEAL R. GROSS

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

1 eliminate large break LOCA. It eliminates
2 particularly the guillotine-type break. But you still
3 have to be able to defend against a large break.

4 MR. WATERMAN: This is Mike Waterman.
5 With regard to diversity and defense-in-depth, the
6 credit for leakage detection is really a subset of
7 manual operator actions in which licensees have wanted
8 to credit the ability to detect the onset of a large
9 break LOCA and respond quickly enough in the event of
10 a common-cause failure of the emergency core cooling
11 system to actually manually initiate it within the
12 design basis of the plant.

13 And the credit for leakage detection arose
14 out of the existing Branch Technical Position-19 in
15 which we gave, as an example, a justification for
16 crediting operator action. And that example was the
17 leakage detection in a nuclear power plant. In that
18 case, although not stated in the position, it was a
19 System 80+ advanced reactor design in which they had
20 extensive leakage detection devices planned for that
21 reactor.

22 And so when I put in that example, guilty
23 as charged, I just put in for example, you could
24 credit leakage detection in a nuclear power plant.
25 And I should have been either much more specific or

NEAL R. GROSS

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

1 just not used that example.

2 So what industry has proposed is they have
3 said well, you know, you have given us leak before
4 break, if you will, leakage detection on pipe lip
5 restraints and jet impingement barriers and so why
6 can't we use that analysis to justify operator
7 response times as a diverse approach for mitigating a
8 large break LOCA. And, therefore, not have to put in
9 a diverse low pressure injection system.

10 And so that is where that problem
11 statement arose. Personally, I consider Problem
12 Statement No. 3 to be wrapped up into manual operator
13 actions. When can you consider a manual operator
14 action as a diversity strategy for certain classes of
15 accidents?

16 MEMBER ABDEL-KHALIK: The discussion
17 regarding manual operator action, in my mind, affirms
18 the need for Point 4 in your list in BTP where it says
19 a set of displays and controls located in the main
20 control room should be provided for manual system
21 level actuation of critical safety functions and for
22 monitoring of parameters that support safety
23 functions.

24 The displays and controls should be
25 independent and diverse from the computer-based safety

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 identified in the earlier points. Is that
2 true that if you are going to rely on manual operator
3 action, you must have this Point 4 as part of your
4 criteria?

5 MR. KEMPER: Yes, this is Bill Kemper.
6 Yes, I'm sorry Paul, I didn't mean to cut you off
7 there but yes, that is true. Yes, manual actions have
8 to -- it is assumed that in order to take manual
9 actions that the indicators and the controls that the
10 operators will respond by and with must not be subject
11 to the same common-cause failure.

12 MEMBER ABDEL-KHALIK: Thank you.

13 MR. EAGLE: Another factor in there is if
14 you talk to the operators themselves, they want the
15 ability to be able to if they feel that everything is
16 falling apart around them, they feel much more
17 comfortable if they have some way that they can come
18 back and do something.

19 So I think you will see the operations
20 people when they go into these advanced designs and
21 the operations people in these various plants that are
22 running 103 active nuclear plants now, when they are
23 using advisors, they will be putting some strong
24 emphasis on being able to have operator being able to
25 be -- if everything else fails, be able to be a

NEAL R. GROSS

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

1 dependable backup somewhere in there. Because we have
2 gone a long ways in human factors and operations since
3 our Three Mile Island days.

4 MEMBER ABDEL-KHALIK: If you couple that
5 statement with the statement I made earlier coming
6 from the conclusions of the National Academy study
7 that there appears to be no generally applicable
8 effective way to evaluate diversity between two pieces
9 of software performing the same function, does that
10 imply that this redundant system that would be
11 available for manual operator action can't be digital?
12 Has to be analog?

13 MR. KEMPER: Again, Bill Kemper here. No,
14 that does not conclude that the system must be analog.
15 It simply means that their backup system must be
16 diverse. So it cannot be operating on the same
17 computer system. It cannot be driven by the same
18 software.

19 An analog backup system is certainly an
20 acceptable alternative. But not necessarily a
21 directive, if you will, of ours.

22 MEMBER MAYNARD: But what we are talking
23 about are things that wouldn't even necessarily have
24 to have a computer program. You're talking about
25 being able to push a button that will trip the 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 or start a pump. So you are not necessarily looking
2 at doing something that then takes another reactor
3 protection system. It's taking manual action to push
4 a button to cause a breaker to open or a pump to
5 start.

6 MEMBER KRESS: But that did open the
7 question of what you mean by diversity. You know it
8 is different computers, different software put
9 together by different people. And so at some point,
10 you'll give us a definition of what you mean by
11 diversity?

12 MR. ARNDT: We'll talk to you about where
13 we are going on that and how we are trying to get
14 smarter about that.

15 MR. EAGLE: That's literally part of the
16 whole process that we are working on now. That is one
17 of the key areas that we are looking at.

18 MEMBER MAYNARD: One of the other, just
19 for clarity in reading the branch technical position
20 and other things, sometime we're not real disciplined
21 on our use of terms as to reactor protection system
22 versus reactor trip. And when we're talking the
23 bigger picture and the smaller picture and different
24 other components here. So that is just something else
25 you have to watch out for when you are reading some 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 this, too.

2 MR. JUNG: This is Ian Jung. I'm the
3 Chief of the I&C Branch in NRO. I started about seven
4 months ago.

5 Just one thing to add about the manual
6 operation and many of these problems statement related
7 to diversity and defense-in-depth, they are very
8 interrelated with human factors engineering and even
9 communications and software development life cycle
10 processes.

11 So this particular set of statements,
12 problem statements, are not intended to address all
13 the other areas. We are sort of focusing these
14 problem statements from a pure perspective of
15 diversity and defense-in-depth perspectives. So if
16 there are other concerns sort of related to it, that
17 will probably be addressed whereby in coordination
18 with other branches.

19 For example, manual actions, operator
20 actions, clearly we're going to work with the human
21 factors group as we resolve that issue.

22 CHAIR APOSTOLAKIS: Possibly use ATHEANA?

23 (Laughter.)

24 CHAIR APOSTOLAKIS: Please go on.

25 MR. EAGLE: Okay. In our Problem

NEAL R. GROSS

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

1 Statement No. 4, BTP-19 Position 4 challenges, this is
2 a case, again, we just read that where they set
3 displays and controls located in the main control room
4 shall be provided for manual system-level activation
5 of critical safety functions and monitoring of
6 parameters that support the safety functions. The
7 displays and controls shall be independent and diverse
8 from the safety computer system identified as above.
9 And we've already mentioned that.

10 One thing here is I've been right pleased
11 in noticing the various designs that we're seeing and
12 work coming in from the AP 1000, the SBWR, EPR, they
13 are showing the four channels and then showing not
14 only inside the four channels, they are actually
15 starting to show subdivisions within these channels to
16 even have a redundancy so what I assume a component
17 even inside a subdivision would not take the whole
18 division down.

19 So this has been an interesting thing.
20 Going back into this area, if they have credit for
21 taking components because of this, it allows maybe
22 some more diversity in being able to what components
23 can be turned on or used. And this is a question that
24 needs to be looked at a little bit more in detail.

25 Number five, effects of common-cause

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 failures, additional clarity is desired regarding the
2 effects that should be considered. Generally we think
3 of just -- as Paul spoke of not long ago, with failure
4 is all of a sudden, it just doesn't work any longer.
5 But also there may be other ways and other types of
6 failures.

7 For example, a failure to activate but
8 also a failure to -- it actually causes a spurious
9 activation, particularly in some of the engineering
10 safeguards, the actual starting of the pumps or
11 starting the pump items would not be good. So this is
12 something that has to be taken into consideration.

13 CHAIR APOSTOLAKIS: I think this is
14 related to something we discussed with the Office of
15 Research some time ago, namely classification of the
16 systems that utilize digital I&C somewhat, just
17 actuation systems there may be feedback and control
18 systems and so on. The methods are different and I
19 think several of these points, in fact, are related to
20 that. So you may want to think about rephrasing some
21 of this. And that applicability, too.

22 MR. EAGLE: Right. This is a -- point six
23 is a clarification of identification design
24 attributes. Could there be sets of attributes that
25 can be used, maybe expanded on, that help us get 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 much more simplified or clearer picture, a more direct
2 of being able to present and understand this diversity
3 and what kind of depths we would need.

4 One example might be simplicity. For
5 example, we think of these process computers being
6 quite large and complex. But also we're now seeing
7 the breakdown into such things as the field-
8 programmable gator rays, things like that that are
9 logic devices that could be brought down and maybe
10 used in small chunks or groups that are much more
11 simplified and much easier to thoroughly test. Also,
12 it's easier to predict failures within these.

13 Echelons of defense, additional
14 clarification is desired regarding the echelons of
15 defense. These echelons, for example the ones that I
16 talked about that control the reactor trip system, the
17 engineered safeguard systems, and the monitoring and
18 indication post the diverse and one depending on being
19 able to take over if the other one fails, therefore,
20 BTP-19 and some of the documents indicate these should
21 be separated.

22 One idea is that really necessary? Is
23 there some places where there might be some maybe
24 commonality but still to be able to carry the defense-
25 in-depth and the diversity. And actually may be able

NEAL R. GROSS

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

1 to achieve greater safety with certain types of this
2 combining certain things. But this is an area that
3 does need more look-see.

4 Number Eight problem statement is the
5 single failure. At this point in time, the failure of
6 all four of the computers, all of the software, or all
7 four computer systems within the four channels is
8 looked at as beyond a credible accident at this point
9 in some of the statements and some of the documents.

10 However, there have been others who say
11 really we should need to consider this as a single
12 failure. And the things Paul pointed out in accident
13 analysis, you have to just about assume a single
14 failure, common-cause failure, or common mode failure.
15 And this is another area to be looked at from the
16 group.

17 As far as deliverables, the idea is to
18 take a look very carefully at the various problem
19 statements, what we have, and to come up with some
20 consensus and then provide this in some type of
21 guidance that can come back. For example, a
22 regulatory issue summary might be achieved, be able to
23 provide this information, and to be able to use it in
24 reviews and also in development and design.

25 The goal here is to deliver an additional

NEAL R. GROSS

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

1 guidance to enhance efficiency and effectiveness in
2 handling safety issues and schedules for simulators.
3 Actually I kind of looked at it is we're all in one
4 great big football game.

5 And, of course, you know football is one
6 of the greatest pageantry system that we have in this
7 country. And the NRC represent the referees. But you
8 have all these other groups. But the whole objective
9 is to complete the game. And to complete it safety
10 and fairly.

11 We also have long-term things that will be
12 done. That will be referred to in a moment here, more
13 that will be talked about. And this is where the
14 recommendations, the things we've learned about from
15 research, from the various talks, discussions,
16 developments, conferences, will come and result
17 finally in updating, for instance, the standard review
18 plan. Maybe, for instance, updating the 10 CFR or
19 other things.

20 CHAIR APOSTOLAKIS: Now the goal in the
21 near term I find a little interesting. Schedules for
22 simulators. Did you elaborate on that? Maybe I
23 missed it.

24 MR. EAGLE: Yes. One of the most
25 important parts of developing the new reactors 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 getting ready to operate these is that you have to
2 train your personnel. So you have to have the
3 simulators for this. And to be able to order the
4 simulators, the simulator obviously has to represent
5 almost a completed system.

6 So you start asking yourself when do we
7 need to know that. And you start backing the times
8 table back. One of the areas I think has been talked
9 about is maybe somewhere in the late part of 2007 they
10 would need to have a guidance that would help be able
11 to facilitate the ordering of the simulators. That
12 the information that would be sufficiently intact so
13 that the designs could be completed and approved, that
14 would help us be able to get those simulators ordered.

15 CHAIR APOSTOLAKIS: The reason why I
16 raised the issue is because I saw a few papers in the
17 literature where they -- I fully agree with what you
18 said, by the way -- where the simulators are used to
19 actually do a safety analysis.

20 In other words, when we do all these
21 evaluations and do son and, for example, I have one
22 paper in front of me, it says the standard techniques
23 like failure modes and effects analysis, fault tree
24 analysis, and so on are static.

25 And they cannot perform dynamic analysis

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 identify the interactions among systems. So they
2 use simulators to actually do these things and try to
3 see what the consequences of common-cause failures are
4 and so on. So that could be another way of performing
5 this evaluation.

6 MR. MAYFIELD: Mr. Chairman, if I could,
7 this is Mike Mayfield from NRO. And I agree, given
8 the adequate fidelity in the simulators you could use
9 them for that purpose.

10 CHAIR APOSTOLAKIS: Yes.

11 MR. MAYFIELD: The driver here, as Gene
12 said, is training for the in-plant staff. I think we
13 didn't fully appreciate that schedule constraint when
14 we got started on this. We've had some ongoing
15 dialogue with the industry about timing for delivering
16 some of this interim guidance.

17 And it has been fairly clear that being
18 able to order the simulators to facilitate the fairly
19 lengthy training schedules becomes the long pole in
20 the tent. And so we're working hard to achieve -- to
21 try to achieve the schedule that they need to be on.

22 We got short-cycled a bit in the last
23 couple of months, which is creating some challenges,
24 some prioritization of the various activities which we
25 are interested in the industry input, where to put the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 resources first. But the schedule for the simulators
2 has proven to be the more challenging issue.

3 CHAIR APOSTOLAKIS: I think you would
4 benefit from the experience of these people but maybe
5 the use of the simulators they way I just described
6 can be part of the long term.

7 MR. MAYFIELD: I think it could very
8 definitely be part of the long term. The near term
9 thing is to give people enough assurance in these
10 criteria so that they can move forward, finish up the
11 design to the degree they need to move forward on
12 ordering the simulators.

13 CHAIR APOSTOLAKIS: I think it would be
14 useful for you guys to look at some of these papers.
15 I'm not saying you should do what they are describing.
16 But it would be useful. Where should I send it?

17 MR. MAYFIELD: Why don't you send them to
18 Steve --

19 CHAIR APOSTOLAKIS: Okay.

20 MR. MAYFIELD: -- as the initial point of
21 contact.

22 CHAIR APOSTOLAKIS: Right.

23 MR. MAYFIELD: And he will share them
24 among the working groups.

25 CHAIR APOSTOLAKIS: Just look at them and

NEAL R. GROSS

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

1 see what these guys are doing and what kind of
2 insights they are gaining.

3 MR. MAYFIELD: Yes.

4 CHAIR APOSTOLAKIS: And take it from
5 there.

6 MR. MAYFIELD: Yes.

7 MR. ARNDT: The point of this bullet,
8 Doug, just to put a point on it is some of the design
9 decisions are going to be driven by what our interim
10 guidance is on diversity and defense-in-depth. How
11 they design things.

12 Those need to be made so they can do their
13 complete design, get it reviewed, get their simulators
14 ordered, et cetera. So that the point here is that
15 the interim guidance is being driven by that design
16 decision which is being driven by their need to order
17 the simulators.

18 CHAIR APOSTOLAKIS: Good.

19 MR. EAGLE: There are two key areas here
20 concerning simulators that I'd like to point out. We
21 have already put out very clearly the importance of
22 the simulator to the nuclear plant for training the
23 operators. There is also a simulator for the vendor.
24 And I would like to make a personal recommendation to
25 the Committee that they visit these vendors'

NEAL R. GROSS

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

1 simulators because in looking at these modern systems,
2 it is nothing like you have seen before. It is more
3 like walking into "Star Wars" now.

4 And we've had the pleasure of visiting at
5 least one of these and it is an interesting experience
6 sitting down where everything is being run by
7 computers and try it. So the Committee I think would
8 find a very good learning experience by doing that.

9 CHAIR APOSTOLAKIS: Yes. Meeting R2-D2.

10 (Laughter.)

11 CHAIR APOSTOLAKIS: Okay. And what's
12 number nine?

13 MR. EAGLE: Our final is the conclusions,
14 the regulatory basis for staffing guidance on
15 diversity and defense-in-depth are in place for the
16 new reactor submittals. Additional details,
17 flexibility, clarifications are needed in some areas
18 as technology has advanced.

19 The staff, in principle, is in agreement
20 with industry in advocating the use of digital
21 computer-based I&C with the potential of providing
22 greater safety. The challenge is in the details.

23 The NRC and nuclear industry continue to
24 work closely to resolve identified problems. Once
25 again, we repeat, the goal is to deliver additional

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 guidance to enhance efficiency, effectiveness in
2 handling safety issues and schedules for the
3 simulators.

4 Is there any questions?

5 (No response.)

6 CHAIR APOSTOLAKIS: Okay. Well, thank you
7 very much.

8 MR. EAGLE: Thank you.

9 CHAIR APOSTOLAKIS: So we'll take a break
10 now.

11 MR. MAYFIELD: George, if I could --

12 CHAIR APOSTOLAKIS: Yes?

13 MR. MAYFIELD: -- just a question you had
14 asked early on about is the Steering Committee made up
15 only of NRC people and I wanted to provide the
16 Subcommittee a little bit of perspective on the
17 structure that has been put in place.

18 At the Commission meeting where this all
19 got started, the industry representatives described
20 the Steering Committee that they had in place. And
21 that seemed like such a good idea the Commission said
22 we probably should go do a similar thing.

23 So there actually is an industry Steering
24 Committee and a parallel NRC Steering Committee.
25 There are then parallel structures down at the task

NEAL R. GROSS

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

1 working groups. There is active information exchange,
2 idea exchange, in a public meeting setting between the
3 industry groups and the NRC groups.

4 But it is not a joint Steering Committee
5 or a joint task working group. These are parallel
6 groups. And they each have their own working
7 activities and things to go do. But there is very
8 active information flow between them.

9 CHAIR APOSTOLAKIS: How big is the NRC
10 Steering Committee?

11 MR. MAYFIELD: Pardon me?

12 CHAIR APOSTOLAKIS: Who are the members of
13 your Committee?

14 MR. MAYFIELD: The Steering Committee,
15 Jack Grobe chairs it. I'm on it. Mark Cunningham
16 from Research, Joe Gitter from NMSS, on the fuel cycle
17 facilities is where that one really comes in. And
18 then Scott Morris from INSR. So that --

19 CHAIR APOSTOLAKIS: Those are senior level
20 people.

21 MR. MAYFIELD: Senior level -- Division
22 Director and higher.

23 CHAIR APOSTOLAKIS: Okay. Go ahead.

24 MR. ARNDT: It was intended to be similar
25 to the PRA Steering Committee. Sorry, Steve Arndt,

NEAL R. GROSS

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

1 the other thing you might want to mention is all these
2 interactions are done in a public environment to
3 elicit additional comments from other stakeholders.
4 It is not just the industry that we are working with.

5 CHAIR APOSTOLAKIS: All right. Shall we
6 break until 10:20?

7 (Whereupon, the foregoing
8 matter went off the record at
9 10:02 a.m. and went back on the
10 record at 10:22 a.m.)

11 CHAIR APOSTOLAKIS: We are back in
12 session. Our next presentation is by Mr. Waterman on
13 Diversity and Defense-in-Depth Research.

14 MR. WATERMAN: If Dr. Wood could come on
15 up here.

16 CHAIR APOSTOLAKIS: That is different, I
17 guess, from what it says here. It says long-term
18 activities. But it is the same thing?

19 MR. WATERMAN: That is correct, Dr.
20 Apostolakis.

21 CHAIR APOSTOLAKIS: Okay.

22 MR. WATERMAN: My name is Mike Waterman.
23 I'm in the Office of Research. I was formerly in the
24 Office of Nuclear Reactor Regulation as an I&C
25 Engineer over there for about I don't know 14 or 15

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 years and came over to Research, I think, in 2003 or
2 2004, something like that. Time flies.

3 With me today is Dr. Wood from the Oak
4 Ridge National Laboratory. Dr. Wood has extensive
5 experience in the area of instrumentation and controls
6 and he is my principle investigator in the research
7 that I'm going to describe today.

8 The research I will describe in this
9 presentation really addresses the fundamental question
10 of how much diversity is enough in the nuclear
11 industry. This research was initiated last October
12 and is still in progress. And consequently any
13 conclusions I describe today are with regard to the
14 ongoing research and should be considered preliminary.

15 Now in this presentation, I will summarize
16 the diversity and defense-in-depth issue we are
17 addressing with the current diversity research
18 project. I will then provide background information
19 on diversity and defense-in-depth NRC policy, a little
20 bit of history.

21 I will then describe the research project
22 and schedule and conclude with some preliminary
23 results of that research.

24 Now adding diverse systems and defense-in-
25 depth is a worthwhile strategy for assuring public

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 health and safety. And obviously a diverse system for
2 every safety system and extensive defense-in-depth
3 could be used to mitigate common-cause failures.
4 However, from a practical standpoint, this solution
5 may be technically unfeasible.

6 Given this conclusions then, the question
7 is not whether diversity and defense-in-depth should
8 be employed but rather how much diversity and defense-
9 in-depth are enough to provide reasonable assurance of
10 adequate safety. And supporting questions include are
11 there precedents for good engineering practices? For
12 example, what is being done in other countries,
13 industries, and agencies with regard to diversity and
14 defense-in-depth?

15 Can sets of attributes provide adequate
16 diversity? For example, are there subsets of
17 attributes identified in NUREG/CR-6303 that can
18 provide sufficient diversity?

19 And finally are there standards or other
20 guidance that can be endorsed? For example, does ANSI
21 ANS 58.8, which is the time response design criteria
22 for nuclear safety-related operator actions, which is
23 referenced by IEEE Standard 6013, provide acceptable
24 guidance for determining operator response times.

25 MEMBER ABDEL-KHALIK: You know posing the

NEAL R. GROSS

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

1 question in the form of how much implies that
2 diversity can be quantified. And the issue then in my
3 mind is is that true? Can you actually assign a
4 quantifiable measure to measure diversity?

5 MR. WATERMAN: I don't think that was what
6 I was meaning. I mean you could provide some amount
7 of diversity that is just overwhelming. Different
8 microprocessors, different systems, different
9 operators who do the same function, things like that.
10 And you can just literally overwhelm a system with so
11 much diversity that you are sure is that really as
12 much as you need?

13 But I don't know about quantification.
14 We're not attempting to do any quantification.

15 CHAIR APOSTOLAKIS: This is the question
16 that was asked I don't know 15 -- 10, 15 years ago
17 when we were debating Regulatory Guide 1.174. And
18 there we were not asking the diversity question
19 because, you know, the problem with a traditional
20 regulatory system is that the question -- the
21 statement was that it doesn't guide you as to how much
22 defense-in-depth is sufficient.

23 And by quantifying risk or some metric
24 that is related to risk, you can actually say yes,
25 this is enough because I have reached an

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 unavailability level that is acceptable.

2 So what I would say -- I think strictly
3 speaking, the answer to your question, said, really
4 does not exist. But you can have metrics that give
5 you some indication.

6 But I would say that these are good
7 questions also for the Research group. One, as you
8 know, one of the major efforts there is to develop
9 risk methods that involve digital I&C. And here is a
10 set of practical questions that the Agency is
11 interested in that maybe those guys should have in the
12 back of their mind when they develop their tools. Say
13 can I answer this question? Can I give some guidance
14 to Mike or whoever else is using this?

15 Steve?

16 MR. ARNDT: Yes, and that is one of the
17 things we'll talk about a little bit this afternoon.
18 Not in a lot of detail but some.

19 What Mike is, and correct me if I'm wrong,
20 Mike also works at our Office of Research, the
21 Research Program, to answer some of the long-term
22 questions we talked about before the break, is looking
23 at qualitative strategies to answer this question.

24 CHAIR APOSTOLAKIS: Yes.

25 MR. WATERMAN: And these questions, we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 here in the NRC, we didn't invent these questions.
2 These are really questions that have risen out of the
3 industry when we've told the industry employ diversity
4 and defense-in-depth and they come back and say well,
5 how much do you need?

6 CHAIR APOSTOLAKIS: Because as far as they
7 are concerned --

8 MR. WATERMAN: And we're trying to answer
9 that.

10 CHAIR APOSTOLAKIS: -- you can keep adding
11 diversity to systems.

12 MR. WATERMAN: That's right.

13 CHAIR APOSTOLAKIS: To make them safer and
14 safer and safer.

15 MR. WATERMAN: Of course, as you get more
16 and more diverse, you become more and more complex and
17 so the reliability starts suffering.

18 CHAIR APOSTOLAKIS: That's why there is a
19 period of public comment.

20 MR. WATERMAN: Now some background here is
21 our policy was established really in the early to mid-
22 1990s as a means to address common-cause failures in
23 digital safety systems. However, our knowledge of
24 digital technology has increased significantly since
25 that time, mostly by experience. And the technology

NEAL R. GROSS

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

1 itself has evolved considerably since the Agency's
2 policy was established.

3 Now as recognized by the nuclear industry
4 and others, common-cause failures in digital systems
5 are difficult to predict. And consequently, just as
6 difficult to prevent. Generally the perceived
7 solution has been to design and build systems that
8 will not fail.

9 Indeed, for production- class systems,
10 that is an overlying objective of the quality
11 assurance processes and other contractual obligations
12 of the system supplier.

13 Historically, however, designing systems
14 that will not fail has been difficult to achieve not
15 just in the nuclear industry. You name it, you know,
16 any industry, pick any industry, and they have all had
17 that same problem. And that objective becomes more
18 difficult as the size and complexity of the systems
19 being developed have increased.

20 Before I settle into a discussion on
21 ongoing NRC research, I think it would be helpful to
22 provide just a brief definition of what diversity is
23 and what defense-in-depth are because often in
24 conversations you hear people use those two terms
25 interchangeably. Sometimes they say defense-in-depth,

NEAL R. GROSS

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

1 sometimes they say diversity. And you're not really
2 sure what they are talking about.

3 So let's just do a brief illustration
4 here. Now this slide illustrates the difference
5 between diversity and defense-in-depth.

6 Now the slide is for illustration purposes
7 only in that reactor trip systems and engineered
8 safety feature systems are often complementary and not
9 hierarchical in structure. In other words, ESF
10 doesn't always depend upon a reactor trip system to
11 operate in order for it to be called up to operate.

12 In this illustration, however, four
13 echelons of defense-in-depth are arranged
14 concentrically such that when the control system
15 fails, the reactor trip system reduces reactivity when
16 both the control system, a control system such as main
17 feedwater, turbine generated, governor controlled,
18 chemical volume control systems won't effect, when
19 both the control system and the reactor trip system
20 fail, the engineered safety features continue to
21 support the physical barriers to radioactivity release
22 by maintaining cooling to the core and allowing time
23 for other measures to be taken by reactor operators to
24 bring the plant to a safe state.

25 Now monitoring and indications, that last

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 echelon down there, allow the operators to monitor
2 plant conditions and to take control of the plant in
3 the event the other three echelons of defense-in-depth
4 cannot. And often operators are directed to take
5 control of the plant even when the engineered safety
6 features are running. For example, terminate high-
7 pressure safety injection under certain conditions.

8 Now diversity is used to provide added
9 assurance that the reactor trip systems in this case
10 and the ESF systems will function as required. So
11 summarizing, defense-in-depth is a strategy that uses
12 different functional barriers, if you will, to
13 compensate for failures in other barriers -- reactor
14 trip systems, compensating for failures in the control
15 system barrier for example.

16 Diversity is a strategy that uses
17 different means within the functional barrier to
18 compensate for failures within that same functional
19 barrier. And that is given by the little trapezoid
20 here versus the ellipse, right, those are both reactor
21 trip systems but they are diverse functions such that
22 if a hazardous condition is not handled by one of the
23 diverse means, it may be handled by the other one
24 right here.

25 So that is what diversity is and that is

NEAL R. GROSS

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

1 what defense-in-depth are. So that is sort of in
2 response to your question earlier, I believe, Dr.
3 Apostolakis, you know how do we define these things.

4 CHAIR APOSTOLAKIS: This is the swiss
5 cheese model, right?

6 MR. WATERMAN: This is the swiss cheese
7 model, yes.

8 CHAIR APOSTOLAKIS: Because Jim Reason has
9 proposed it in human performance.

10 MR. WATERMAN: Generally there are two
11 approaches you use in diversity and defense-in-depth
12 strategy. And these approaches are not exclusive
13 approaches. They are used generally as complementary
14 approaches.

15 The first approach is avoidance, produce
16 high-quality error-free systems. Build a system that
17 will not fail. Minimize common elements in the system
18 so you can avoid a common-cause failure. Or just
19 limit the fault propagation to a specific system so
20 that it doesn't propagate over and cause a common-
21 cause failure.

22 In addition to avoidance is the mitigation
23 strategy where you acknowledge you may have a common-
24 cause failure. How do you mitigate it as quickly as
25 possible or as effectively as possible so you can

NEAL R. GROSS

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

1 continue to accomplish your function. And by
2 mitigation, you add defense-in-depth to compensate for
3 failure in other functional barriers or systems. And
4 you can provide diverse systems that will not fail at
5 the same time within a functional barrier. So those
6 are the two general approaches.

7 The current process for confirming
8 adequate diversity and defense-in-depth has been
9 incorporated in safety system design is fairly
10 complex. Current regulatory guidance identifies six
11 categories of diversity attributes that can be used in
12 design of systems.

13 What we want to know is how can you
14 combine those diversity attributes such that you can
15 come up with sets of diversity strategies. In a
16 research approach for identifying what would
17 constitute the components of the diversity strategy is
18 we want to go out to academia, scientific
19 organizations, other countries' industries and
20 agencies, and find out what the rest of the world is
21 doing with regard to diversity and defense-in-depth.

22 We also want to use the information that
23 was provided in NUREG/CF-6303 on diversity strategies,
24 combine those and try to develop -- this is the core
25 of the program -- develop sets of D3 strategies 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 use the attributes and associated diversity criteria
2 out of NUREG/CR-6303.

3 Once we develop those sets of strategies,
4 we need to know whether or not we need to develop
5 guidance and acceptance criteria for each of those
6 strategies. And, of course, that will feed through
7 the D3 -- the diversity and defense-in-depth task
8 working group that you heard about earlier today, and
9 along with public interaction.

10 Once we have that guidance, we really need
11 to validate is the guidance applicable? Okay, you've
12 got guidance. Can you actually apply that guidance to
13 license a system?

14 With that, we will be working with current
15 and new plant designs, licensees, applicants, what
16 have you, to validate our guidance against real
17 systems to find out -- and that was what Alex Marion
18 described early as this cooperative research effort,
19 if you will, to find out is our guidance applicable in
20 a licensing environment? As opposed to just having
21 guidance there that nobody can apply.

22 And finally to integrate our licensing
23 guidance and acceptance criteria into our regulatory
24 practices. So that is kind of the basic outline of
25 what we are intending to do. Of course there will be

NEAL R. GROSS

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

1 public interaction in some parts of that and there
2 will be licensee interaction in other parts.

3 CHAIR APOSTOLAKIS: Excuse me, Mike, we
4 have our consultant, Dr. Guarro on line.

5 MR. WATERMAN: Good.

6 CHAIR APOSTOLAKIS: So I'd like everybody
7 to know that there is somebody listening in and
8 participating.

9 Sergio, are you there?

10 (No response.)

11 CHAIR APOSTOLAKIS: I take it back. We
12 don't have anyone. Okay, he'll come back, I'm sure.

13 MR. WATERMAN: As described in the above
14 slides, the research project objectives are to
15 supplement and augment existing guidance, acceptance
16 criteria, and licensing processes by evaluating
17 processes used in other countries, agencies, and
18 industries, coupled with recommendations from
19 academia, crazy and otherwise, and scientific
20 organizations.

21 CHAIR APOSTOLAKIS: Yes, Dr. Kress just
22 pointed out to me that the way you have it there, they
23 appear to be mutually exclusive.

24 (Laughter.)

25 CHAIR APOSTOLAKIS: That's okay, keep

NEAL R. GROSS

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

1 going.

2 MR. WATERMAN: That's right past me.

3 The results of this research will be
4 integrated into the development of D3 strategies that
5 are based upon the guidance developed in NUREG/CR-
6 6303, as I described earlier. And this phase of the
7 research project is scheduled to be completed in the
8 May time frame of this year.

9 A follow-on research effort will solicit
10 industry support to validate the licensing process
11 developed by the research to improve clarity and
12 consistency of the licensing process. And this effort
13 is tentatively scheduled to be completed by the end of
14 this year. That is the validation of results, August
15 2007 time frame, maybe September. It depends on how
16 we schedule things with the licensees and who steps
17 forward.

18 CHAIR APOSTOLAKIS: So this is what the
19 staff is doing in response to the SRM that the staff
20 should establish an NRC project plan with specific
21 milestones and deliverables? Is that what you are
22 doing here?

23 MR. ARNDT: No, sir.

24 CHAIR APOSTOLAKIS: Yes?

25 MR. ARNDT: The project -- no.

1 CHAIR APOSTOLAKIS: No?

2 MR. ARNDT: This is the milestones for a
3 specific research program that is addressing a
4 specific issue within the overall I&C project plan.
5 The project plan is what Alex was talking about
6 earlier. And Mike was talking about earlier. The SRM
7 directed us to put together a project plan to answer
8 the short- and long-term issues that have been
9 identified.

10 CHAIR APOSTOLAKIS: Right.

11 MR. ARNDT: So for each of the six areas,
12 D3 is one, risk is one, cyber is one, there is going
13 to be a piece of the project plan. And in each of
14 those project pieces, there are going to be problem
15 statements like the ones you heard earlier. And under
16 each of those problem statements, there is going to be
17 actions associated with it. So this is one piece of
18 that problem.

19 MR. WATERMAN: And this research -- well,
20 this research will be integrated into that task
21 project. But it doesn't encompass the whole project.

22 MR. KEMPER: George, let me try. I think
23 your question can be answered in two parts here.

24 CHAIR APOSTOLAKIS: Who is speaking? I'm
25 sorry.

NEAL R. GROSS

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

1 MR. KEMPER: Yes, Bill Kemper here, sorry.

2 Number one, as you know, we presented the
3 digital safety system research plan and program to you
4 all. It is a five-year plan. This research project
5 is a component of that plan. It has been in there for
6 a long time.

7 CHAIR APOSTOLAKIS: The one we have seen?

8 MR. KEMPER: Yes, the one you have seen
9 and commented on, as a matter fact, to the Commission.

10 CHAIR APOSTOLAKIS: All right.

11 MR. KEMPER: Now it just so happens that
12 when we kicked this off, we also formed these TWGs at
13 the same time. So everything kind of came together
14 quite nicely from a schedule perspective, if you will.

15 And we've also got other projects, too,
16 like in the communications for highly-integrated
17 control rooms, digital system risk, which we will talk
18 about this afternoon as well. So the research,
19 because we are in a point where it is producing
20 results in a timely fashion, is being integrated as
21 part of the information that is being reviewed by
22 these task working groups. If that clears it up.

23 CHAIR APOSTOLAKIS: So the specific answer
24 to the SRM, the SRM addressed to you because we also
25 have one as well, is listing those six items or

NEAL R. GROSS

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

1 questions?

2 MR. ARNDT: Six specific areas.

3 CHAIR APOSTOLAKIS: Areas -- and then say
4 what you will plan to do under each one?

5 MR. ARNDT: Correct.

6 CHAIR APOSTOLAKIS: That's really what
7 this requires.

8 MR. ARNDT: That is correct.

9 CHAIR APOSTOLAKIS: And it requires also
10 a schedule and so on which you are giving us here as
11 well for this particular piece.

12 MR. ARNDT: This is for the Research.

13 MR. WATERMAN: This is just this Research
14 project.

15 CHAIR APOSTOLAKIS: Yes. But Research
16 feeds into --

17 MR. ARNDT: Yes.

18 MR. WATERMAN: Yes.

19 CHAIR APOSTOLAKIS: Yes, it is not a
20 different agency.

21 MR. ARNDT: No, it's not a different
22 agency.

23 CHAIR APOSTOLAKIS: No, I'm trying to get
24 the big picture.

25 MR. ARNDT: Yes.

NEAL R. GROSS

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

1 MR. WATERMAN: But, for example, this
2 particular research project will not answer the
3 question of what are acceptable manual operator action
4 types.

5 CHAIR APOSTOLAKIS: I understand that.
6 And the Research plan we have reviewed did not include
7 operators, as I recall, operator actions.

8 MR. ARNDT: No, that is actually in the HF
9 part of the work. So it wasn't included in the
10 research plan.

11 CHAIR APOSTOLAKIS: It was not. But now
12 there will be a piece of it?

13 MR. ARNDT: There will be a piece of it in
14 the project plan which is the Agency plan to deal with
15 these specific issues.

16 CHAIR APOSTOLAKIS: But who is going to do
17 it is open?

18 MR. ARNDT: No, it is going to be dealt
19 with by the TWG on human factors. And it is also
20 going to feed into this particular project plan.

21 CHAIR APOSTOLAKIS: By human factors, you
22 mean they can come back to the Office of Research --

23 MR. ARNDT: Well, Research at NRR.

24 CHAIR APOSTOLAKIS: At NRR, okay.

25 MR. ARNDT: They've got it. We're just

NEAL R. GROSS

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

1 looking at those specific issues.

2 CHAIR APOSTOLAKIS: Is that research plan
3 that we have seen being modified in any way as a
4 result of this new activity with the group?

5 MR. ARNDT: It is not specifically being
6 modified. We're going to update it. And this will
7 obviously have an impact on it. But it is not being
8 modified specifically to address these.

9 MR. WATERMAN: And actually this research
10 here was called out in the existing research plan as
11 something to do. So this was a planned research
12 project.

13 MR. KEMPER: Yes, excuse me, yes, I'm
14 sorry, Mike, I didn't mean to talk over you. Bill
15 Kemper, again.

16 Yes, this has always been one of our
17 desires is to clarify what diversity attributes should
18 exist in a system because the guidance right now, as
19 we've said to the Commission, it is sometimes
20 difficult for licensees to understand and decipher and
21 figure out how much diversity they should build into
22 their systems. So that is what we are attempting to
23 accomplish here is to clarify that.

24 CHAIR APOSTOLAKIS: But it seems to me
25 coming to my earlier -- now bear in mind I'm still

NEAL R. GROSS

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

1 trying to understand what is going on -- my earlier
2 comment that the work that your group has been doing
3 on the data should be a critical input here.

4 MR. KEMPER: Data, you mean failure data?

5 CHAIR APOSTOLAKIS: Yes, common-cause
6 failures and all that. What has happened in the past?
7 And what did we learn from it? How are the answers to
8 -- or how is the formulation of diversity strategies
9 effected by what we have learned? I think that would
10 be a very valuable thing.

11 My impression from last time we had a
12 presentation and the data was that it was primarily
13 done for us to understand what had happened and see
14 how that could effect the risk part of the plan. But
15 it seems to me that there is a broader perspective
16 there that can be gained.

17 And you have already done a lot of it.
18 But I mean, again, I come back to the Brookhaven
19 presentation. And also John Bickling, the paper that
20 I just sent you, looked at the combustion engineering
21 experience.

22 So I would say that that should be an
23 important resource here. This is what happened. And
24 if we had this strategy, we would have handled it this
25 way. Or whatever else -- lessons.

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. MAYFIELD: This is Mike Mayfield, if
2 I could suggest, I kind of like your idea, which is
3 unusual in and of itself. But if I could offer the
4 proposal, let us take this back and chew on it.
5 Obviously, it hasn't -- what you are suggesting isn't
6 something that we have thought through carefully in
7 terms of expanding the use of the data to this
8 application.

9 I kind of like the suggestion. Why don't
10 you let us take it back and work it both at the
11 Steering Committee -- you know, on the staff Steering
12 Committee as well as with the task working groups on
13 the industry side as well as staff. And let's see
14 where we can go.

15 I'm sure this won't be the last time we're
16 talking to the Subcommittee or the full Committee.
17 And let us come back to you with a strategy.

18 CHAIR APOSTOLAKIS: Are you scheduled to
19 address the full Committee next time? In May?

20 MR. ARNDT: We've got an hour and a half
21 to talk about D3 issues. We had not decided yet how
22 much you are going to report and how much we are going
23 to present.

24 CHAIR APOSTOLAKIS: I understand that.

25 MR. ARNDT: So that is something we 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 talk about later.

2 CHAIR APOSTOLAKIS: Right. But, Mike, do
3 you think you may have some preliminary thoughts along
4 these lines in two weeks?

5 MR. MAYFIELD: Well, I think this is
6 something that -- when are we supposed to be back?

7 CHAIR APOSTOLAKIS: In two weeks or so.

8 MR. MAYFIELD: I would think this is
9 something -- preliminary thoughts but nothing
10 definitive. I think that would be unrealistic.

11 CHAIR APOSTOLAKIS: That would be great,
12 yes.

13 MR. MAYFIELD: But let us -- and this is
14 something where we can reach out to Kimberly Keithline
15 from NEI --

16 CHAIR APOSTOLAKIS: Good.

17 MR. MAYFIELD: -- motivate some
18 discussion. And at least give you some initial
19 thoughts on it.

20 CHAIR APOSTOLAKIS: Very good. Yes, that
21 should be sufficient. Yes, we'll come back to you.

22 MR. WATERMAN: Now in that vein from a
23 historical perspective, a lot of research has already
24 been done. And some of the conclusions are is that a
25 lot of the common-cause failures arose because 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 inappropriate specifications. And we are seeing a lot
2 of common-cause failures arise as a function of
3 maintaining a system once it is installed.

4 Somebody does a modification. The
5 modification didn't go through the same process and
6 caused the common-cause failure.

7 Within the vein of specification, you
8 could -- we could come up and insist that all
9 specifications be sent through a formal methods
10 process. As the systems get more complex, that
11 becomes a much less tenable approach.

12 With regard to maintaining a system,
13 putting in a software patch, if you will, or something
14 like that, what else can you do? You tell people do
15 a good job and somebody misses something, it causes a
16 failure. There is not a lot of diversity strategy
17 that you can apply toward telling somebody to do a
18 good job.

19 The software processes that are used for
20 safety-critical systems are all Appendix B-type
21 processes, independent verification and validation,
22 configuration management, software quality assurance,
23 all of those are rolled into it. But it is the
24 practice. It is the actual application of that.

25 And a diversity strategy that says well,

NEAL R. GROSS

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

1 you've got to do a better job of independent
2 verification and validation is not a very good
3 strategy because the people who are doing it are
4 already doing the best job they can.

5 It is when that process breaks down. And
6 what my experience has been, the process breaks down
7 during the mod -- you know, somebody needs to do a
8 patch. The Palo Verde core protection calculator
9 example, that was a system modification. And the
10 error was introduced into the system after it was in
11 there.

12 And incidently, that wasn't really a
13 common-cause failure. I just want to clarify that.
14 It was a potential common-cause failure. It required
15 a hardware failure in each channel before the common-
16 cause failure would manifest itself. So just to clear
17 the air on that. I don't want the industry to be
18 defensive because it was a potential. It was a
19 precursor to a common-cause failure.

20 So with that in mind, if I can move on now
21 to talking about what our sources of information are
22 that we have gone with. We've looked at from the
23 academia and the scientific disciplines, we've looked
24 at, of course, the National Academy of Sciences, the
25 National Science Foundation.

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 We've looked at various papers that were
2 produced by universities. Some of those papers were
3 sponsored by agencies such as the Federal Aviation
4 Administration and things like that.

5 With regard to engineering disciplines,
6 the science organizations, if you will, we've looked
7 at IEEE, the standards organization, to see what they
8 are doing, the IEC, we've looked at their standards
9 organization.

10 We've looked at Controls Engineering, the
11 American Society of Chemical Engineers, and the
12 Society of Automotive Engineers.

13 With regard to foreign reactors, we looked
14 at the French, British, Korean, and Finnish designers
15 and researchers and regulators. As a matter of fact,
16 Dr. Wood and I are planning a trip, as directed by the
17 Commission, but we had already anticipated the trip
18 over to Europe next month to talk to the French
19 regulators, the Finnish regulators, and the UK
20 regulators about what they are doing for diversity and
21 defense-in-depth to get a regulatory perspective.

22 I mean we could talk to the plant
23 designers, too, but what we're really after is what is
24 the regulatory perspective. Why does France, for
25 example, impose one type of diversity? What was 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 basis for that? Try to gather some of that
2 information together.

3 In the chemical processing industry, we've
4 looked at the Center for Chemical Process Safety. In
5 mission-critical defense systems, we've looking in the
6 area of battlefield management.

7 There was a suggestion that we take a look
8 at nuclear submarine power plant-type stuff. But a
9 lot of that stuff is classified. And we are trying to
10 get something out that you can actually put out to the
11 public. And so we really haven't looked at the
12 classified stuff as much as we've looked at
13 battlefield management systems.

14 With regard to avionics, we've looked at
15 the Federal Aviation Administration and the Radial
16 Technical Commission for Aeronautics and NASA. And
17 within transportation, we've looked at the Motor
18 Industry Software Reliability Association information
19 and Federal Railway Administration.

20 So why are we looking at all of this?
21 Well, we're trying to develop some specific strategies
22 that can be used to evaluate system diversity
23 recommendations from academia scientific community.
24 And we want to use those recommendations and
25 approaches to develop specific diversity attribute

NEAL R. GROSS

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

1 criteria strategies.

2 Now what do I mean by diversity attribute
3 criteria? Well, for those of you who have seen
4 NUREG/F-6303, which was written by Lawrence Livermore,
5 a National Labs -- under contract to the NRC back in
6 like 1994 -- Gary Prekshaw was the head engineer on
7 that -- they developed a set of diversity attributes -
8 - six of them -- design, equipment, function, human,
9 diversity, which is really life cycle process
10 diversity signal, and software because software is
11 unique.

12 And within each of those attributes, those
13 six attributes, they developed certain criteria that
14 could be applied, diversity criteria that could be
15 applied within that attribute. For example, in signal
16 diversity, you could have diverse driven equipment or
17 diverse parameter sensor types or diverse parameters.

18 And we already employ some of that
19 diversity in the existing analog systems, right? I
20 mean we trip the reactor on high temperature and we
21 trip the reactor on high flux. Both of them are
22 designed to protect the fuel. Or we trip the reactor
23 on low pressure or low flow or whenever we usually
24 have a DNBR-type trip function.

25 Those are diverse functional trips using

NEAL R. GROSS

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

1 often different signals -- high temperature signal
2 versus a flux signal. So some of that is already
3 employed.

4 Within the digital area, we have other
5 types of diversity. We could have diverse software
6 languages, Pascal and C, for example, or Assembly
7 language and Pascal. Different operating systems,
8 maybe we run a Motorola operating system on Motorola
9 chip versus a risk-based system on an Intel chip. We
10 could use different algorithms.

11 Within the life cycle process, we've seen
12 a lot of this diverse approach like independent
13 verification or validation, if you will, is a
14 diversity strategy in the life cycle process. When I
15 say life cycle process, I mean the software
16 development life cycle process.

17 Typically we may use different management
18 teams to assure that there is some diversity in the
19 approaches followed. Or we might use different
20 designers, engineers, and programmers. And, of
21 course, that is the inversion approach that, you know,
22 has been shown to have some flaws.

23 Dave Parness says there is nothing wrong
24 with inversion as long as you impose diversity on the
25 two different parties who are doing the program. In

NEAL R. GROSS

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

1 other words, they are not totally independent. You
2 have a referee in there that tells somebody you have
3 to use rectangular coordinates. And you have to use
4 polar coordinates, for example, if you are doing slope
5 of a line or something like that.

6 So these are the -- the colored areas in
7 there are what we call the diversity attribute
8 criteria. And what we are attempting to do with this
9 research project is to develop diversity strategies,
10 to identify diversity strategies that use various
11 diversity attribute criteria. We are trying to
12 determine, you know, are there collections of these
13 criteria that if they are put together as a diversity
14 strategy, that provides enough diversity.

15 Now this is just an example diversity
16 strategy. Don't follow the arrows. Don't think there
17 was a lot of thought that went into the arrows. There
18 was a little bit but not total.

19 The idea is to develop say, I don't know,
20 five or six diversity approaches, diversity
21 strategies, the licensee could look at their system
22 and determine well, Strategy A is good for my system.
23 I'll follow that. And he would know exactly what
24 diversity approaches he could follow that would be
25 found acceptable here at the NRC. It would be our

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 job, of course, to ensure that they were applied
2 correctly and appropriately.

3 Right now the licensee has no guidance
4 like that. When they come up with a diversity
5 approach, they don't know whether it is going to be
6 approved by the NRC or rejected. And they really
7 don't know what the criteria is for either one.

8 And so what this is intended to do is to
9 provide much more licensing certainty to the industry
10 and much more licensing guidance to the NRC staff so
11 that everybody knows what the rules are on diversity
12 and defense-in-depth, especially diversity.

13 So that is basically the approach that
14 this research is trying to do is to find out what the
15 rest of the world is doing, identify specific
16 diversity strategies that seem to be working such as
17 like what is being done on the Boeing 777, you know
18 what are they doing for diversity and defense-in-
19 depth?

20 And then to take those and try to bring
21 them into the nuclear industry in a coherent set of
22 diversity strategies that people can follow.

23 So what have we learned to date? Well,
24 with regard to other industries, this slide describes
25 the results of our diversity research with regard 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 strategies being used by other agencies and industry
2 such as NASA, the FAA, the aircraft industry, et
3 cetera. The industry strategies are not necessarily
4 used throughout an industry.

5 What we have done is we've looked at
6 specific applications, identified diversity. But that
7 does not necessarily mean the whole industry follows
8 that strategy. But they are examples of what was
9 found in selected applications within an industry.

10 The next step in the research project is
11 to develop these diversity attribute strategies to
12 determine specific diversity attribute criteria
13 strategies within each.

14 For example, in the space shuttle where
15 they are using functional diversity, what type of
16 functional diversity are they using? Where's my
17 wheel? Okay, when we say functional diversity, are
18 they using different functions or are they using
19 different mechanisms? Different response times?
20 Diverse response times? Or what? So, you know, we're
21 trying to -- that's the next step in doing that.

22 But you will notice interestingly
23 something I noticed here is the signal diversity. Do
24 you notice that? It seems like nobody is using
25 diverse signals like RTDs versus thermocouples.

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 Nobody is following that approach. They all seem to
2 acknowledge that signals are pretty immune to common
3 mode failure, I guess, although you could argue that
4 the Rosemont certainly would disprove that, the
5 Rosemont pressure transmitter.

6 But it seems like nobody is really using
7 signal diversity as one of their diversity --

8 CHAIR APOSTOLAKIS: In the chemical
9 industry, you don't quite have assorted green but --

10 MR. WATERMAN: Yes, this right here is an
11 indication of this thing about it is not an industry-
12 wide approach. This was just one application. But I
13 wanted to caveat the rest of them with that same
14 comment.

15 DR. WOOD: If I may interject, this is
16 Richard Wood, the chemical industry, part of the
17 reason those are shaded is because you have
18 recommended practices that acknowledge some virtue to
19 different kinds of diversity. And in the case of the
20 chemical industry signal diversity, using different
21 measurement technologies can have some value and
22 provide some additional means of protection against
23 the potential for common-cause failure.

24 In some of the other cases, for example
25 the NASA cases or the FAA, they are limited in what

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 they can do because of size, weight, and power
2 consumption considerations. So they don't tend to
3 look at -- and the other thing is they tend to want
4 the same signals going into the same software giving
5 the same results for points of comparison. That is a
6 philosophy that you will see in some of those
7 applications that is distinct from what the nuclear
8 industry does.

9 MR. WATERMAN: And we can provide
10 additional detail on, for example, space shuttle or
11 anything like that. I've got that in a -- I can
12 reference that fairly quickly.

13 With regard to the foreign reactors, we've
14 looked at Sizewell, Temeline, well, you can read the
15 list there all the way down to Lungmen, and to
16 determine what they are doing. And this is
17 preliminary information. There may be some
18 corrections that come out, for example, Dukovany or
19 something like that.

20 Sizewell B does use diverse signals. But
21 none of the rest of them use that. But you'll notice
22 that functional diversity seems to be a common thread
23 throughout all of the plants.

24 And software diversity, interestingly, is
25 not something that is embraced by all the plants. For

NEAL R. GROSS

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

1 example, Sizewell, Dukovany, and Beznau and Paks for
2 that matter, don't really push the software diversity
3 attribute that hard.

4 So that's basically a summary of where we
5 are at right now is we've narrowed it down to what are
6 the attributes that are being used. And the next step
7 is to go into each of those attributes for each of
8 these diversity examples and determine what criteria
9 in each attribute are being used so we can synthesize
10 some diversity strategies.

11 MEMBER MAYNARD: What is the expected
12 output of this? Will it be like a NUREG? Will it be
13 a --

14 MR. WATERMAN: A NUREG is proposed right
15 now. To do that. Long-term, I guess that is what
16 that is really, long-term I'd like to see all of this
17 rolled into the SRP, standard review plans for the
18 various nuclear facilities.

19 While we are focusing on nuclear reactors
20 right here, Advisory Committee on Reactor Safety, I
21 foresee that this could also be applicable to nuclear
22 facilities in general such as mixed oxide fuel
23 facilities or advance centrifuge facility or the
24 American Centrifuge Project and things like that to
25 also address safety over in those areas. Even though

NEAL R. GROSS

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

1 the risk from those facilities is not as high, they
2 still have safety systems. And safety is safety.

3 MEMBER MAYNARD: Well, it just looks like
4 there is a lot of good information and interesting
5 information that would come out of this that I would
6 hate -- it would be nice if it was in some
7 consolidated document.

8 MR. WATERMAN: Well, the NUREG is the
9 project deliverable on this. But we need to move
10 beyond the NUREG space into regulatory acceptance
11 criteria space, too. I agree with that totally. And
12 I'm sorry -- I'm kind of from two perspectives here.
13 One is interesting information I'd like to see
14 captured.

15 But yes, that may not -- you know the more
16 timely thing is what is needed to be factored into the
17 guidance. And the information that is actually going
18 to be used in the regulatory process.

19 DR. WOOD: If I could make a couple of
20 observations, this is Richard Wood, again. On the
21 previous viewgraph dealing with other industries and
22 agencies, there are some -- one point that I think we
23 should be aware of is none of these industries has an
24 objective set of criteria for how much diversity is
25 enough. We haven't found it. If it is there, it is

NEAL R. GROSS

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

1 well hidden.

2 But in many cases, the amount -- or the
3 need for diversity or, I think as FAA calls it
4 dissimilarity, depends on the consequence of the
5 hazard. And there is some risk impact considered in
6 that as well.

7 And engineering judgment is very important
8 in the determination of have you got enough diversity.
9 And a great deal of analyses, hazard analyses up
10 front. Some of the other applications like the
11 Department of Defense rely very heavily on the up
12 front analyses and very rigorous processes for the
13 development of the system of systems. And not so much
14 on intentional diversity introduced into the system of
15 systems.

16 One interesting point is on the Boeing
17 777. As they went into the development process, there
18 was an intention to use design diversity. And then a
19 decision during the process not to pursue that because
20 of concerns of the complexity it would add in the
21 development of the system. And then the maintenance
22 of the system.

23 And we found in looking at some of the
24 NASA examples that it is the upgrades that happen that
25 have created the common-cause failures that have

NEAL R. GROSS

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

1 caused some problems. The International Space Station
2 is one example where they a multi-tiered control
3 system for the International Space Station. They
4 loaded some upgrades into their top tier. And
5 subsequently had a loss of all the computers on the
6 top tier.

7 And they had, by design, implemented a
8 reduced functionality fail-safe that resided in the
9 second tier, which was then uploaded to the top tier
10 that kind of saved them on that one. So complexity --
11 balancing diversity versus the complexity it adds is
12 the challenge in all of these industries.

13 And what we are hoping to do is -- what we
14 are working to do is to take these examples, translate
15 them into the nuclear context because the applications
16 are different and the needs are different, and use
17 those as the bases.

18 But we're also taking a different, a
19 diverse approach to developing some diversity
20 strategies as well is looking at more systematic ways
21 of assessing what are the kinds of common-cause
22 failures you have to mitigate.

23 And what are the diversity strategies that
24 are effective against those? So hopefully we can
25 supplement what is developed from what we have learned

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 from the other industries with the underlying
2 technical basis that says this set of attributes gives
3 equivalent coverage to this set of attributes.

4 And so we're working multiple paths to try
5 to come to an effective answer that the industry and
6 the NRC can make use of.

7 MEMBER MAYNARD: I'm glad to see that you
8 are factoring in the consequences of too much
9 diversity or making it too complicated. Just like on
10 the Boeing 777 there, in the industry, we've got to be
11 careful we don't just think about the operators
12 because we also have to maintain these systems.

13 And you do reach a point of complexity and
14 the number of different things people have to be
15 trained on and knowledgeable about and parts for and
16 everything that we can make it where it is so
17 complicated it becomes less safe than if we had less
18 diversity or less defense-in-depth sometimes. So we
19 have to find that right balance.

20 MR. WATERMAN: Yes, that's the trick.

21 DR. WOOD: And one other observation I
22 wanted to make. It was discussed earlier whether or
23 not there were measures that could be used.

24 And some universities in the United
25 Kingdom have been working on mathematical methods for

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 assessing diversity among software. And we're hoping
2 to -- we've accumulated a lot of reports and articles
3 from those sources. And we are also hoping to have
4 discussions when we visit the United Kingdom to talk
5 about how that is being used there. And what is their
6 actual status.

7 CHAIR APOSTOLAKIS: That's it?

8 MR. WATERMAN: That's it.

9 CHAIR APOSTOLAKIS: Okay. Thank you.

10 So now we can move on to the general
11 discussion. Do you gentlemen want to come up front
12 here?

13 MR. ARNDT: What we thought we'd do is
14 Mike has a very brief discussion on operational
15 history.

16 CHAIR APOSTOLAKIS: Oh, good.

17 MR. ARNDT: And we'll use that as a segue
18 to the general discussion.

19 CHAIR APOSTOLAKIS: Very good.

20 MR. WATERMAN: Now before I bring this
21 slide up, I want to preface this next slide -- it is
22 a historical perspective, if you will, of potential
23 common-cause failures that have been reported in the
24 nuclear industry since 1987 or something like that --
25 1987, 1988 through 2006.

NEAL R. GROSS

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

1 They are not necessarily common-cause
2 failures but they were events that were reported to
3 our Operating Experience Report database. And the
4 reports that go into that database are reports of
5 things that could potentially effect accomplishment of
6 a safety function.

7 And so many, many of the failures we see
8 here -- the reason I did this research -- I wasn't
9 paid to do it, I did it on my own time -- is I was
10 curious about the question about everybody claims that
11 digital systems are very highly reliable.

12 And I wanted to know well they performed,
13 you know, over the history here in the nuclear
14 industry. And are we getting better at implementing
15 digital systems in the nuclear industry. I mean you
16 would expect to curve the tail down as we get smarter
17 and smarter and learn more and more lessons.

18 And so I did a histogram, if you will.
19 There we go. Thank you, Steve. And these are some of
20 the things I found. And like I said, I want to
21 preface this. They are not all common-cause failures.
22 But they are events that happened in a digital system
23 that potentially could have been common-cause
24 failures.

25 And they go back to 1987. You'll notice

1 no numbers up there. I guess I can give you a number.
2 Represented here -- and it is only on a single
3 screening -- are 340 events over a 20-year period of
4 time.

5 MEMBER KRESS: What this doesn't show is
6 the denominator -- how many digital systems are out
7 there.

8 MR. WATERMAN: That's correct. And the
9 reason why is that to tell you the truth, I didn't put
10 in that kind of review to determine how many digital
11 systems were actually in place in a given year because
12 it was like on my own time.

13 MEMBER KRESS: Well, this could actually
14 be telling then.

15 MR. WATERMAN: Yes, that would be telling
16 from a fraction of total number of systems implemented,
17 yes. But what I was really wondering is well,
18 absolute failure-wise, are they going down? Or
19 staying constant?

20 MEMBER KRESS: That would tell you
21 something. That's for sure, yes.

22 MR. WATERMAN: Plus general trends.

23 MR. KEMPER: Do you have handouts of this?

24 MR. WATERMAN: Yes, I do. I have handouts
25 of this.

NEAL R. GROSS

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

1 MR. KEMPER: Good.

2 MR. WATERMAN: Okay, well, I thought we
3 weren't going to but --

4 MR. KEMPER: No, no, just that.

5 MR. WATERMAN: Yes, okay.

6 MEMBER ABDEL-KHALIK: So when you say
7 relative number of events, what does the word relative
8 mean?

9 MR. WATERMAN: Well, this was on a poster.
10 And I didn't want to put in how many events per year.
11 So I just put relative number of events. A high tower
12 is a lot of events and a low tower is a few events.

13 CHAIR APOSTOLAKIS: So this is the actual
14 number?

15 MR. WATERMAN: Yes, the actual numbers
16 went into actually building this. And I just took off
17 the left axis, if you will, and called it relative
18 number of events.

19 And then across the bottom down in here,
20 I put in certain events that occurred during different
21 years. I could have put more arrows in but it gets
22 kind of noisy after a while. Yikes, you guys are sort
23 of in the way.

24 But the color slide is coming around here.
25 We had low sequencer events in '95 at Turkey Point.

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 was an Allen Bradley PLC load sequencer. That
2 truly was a common-cause failure.

3 Feedwater control system events, not a
4 safety system, but it was a digital feedwater control
5 system. And mind you this went into the operating
6 event report and I was just trying to determine how
7 are digital systems in the nuclear industry going.

8 And you can be assured that a licensee
9 does not put in junk for a digital feedwater control
10 system. It costs a lot of money to shut a plant down
11 because their feedwater goes down. So they do a good
12 job of building these systems.

13 We some oscillator power range monitoring
14 issues from '99 to '03 as they were shaking out
15 various oscillation power range monitor systems that
16 were being put into the plant. One and -- oh, which
17 one was it -- '99, that was actually a microprocessor
18 common-cause failure.

19 It was kind of interesting. They used --
20 the company that built that OPRM selected the Intel
21 286 microprocessor. And the reason why they selected
22 it was because that company had been building mission-
23 critical weapons delivery systems for the Department
24 of Defense for years with that chip. And they knew
25 that chip intimately.

NEAL R. GROSS

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

1 And that's why they went with that instead
2 of something like a 386 or at that time SX or
3 something like that. It turned out that had never
4 used that microprocessor in that system architecture.

5 In that system architecture, there was a
6 master computer that was calculating oscillation power
7 range functions. And it was synching a slave computer
8 that was supposed to use the same data, calculate,
9 come up with the same answer. And as long as the
10 answer came out to be the same, that channel was
11 assumed to be operable.

12 And what happened is on the Intel 286
13 chip, they have a priority baton passing glitch on
14 that chip. It is well advertised on the site. I know
15 I learned to start looking at the site when I'm
16 reviewing these systems.

17 And when the master would synch the slave
18 processor, depending upon what that slave processor
19 was doing, it might have been doing some self-testing
20 function on memory, when it got synched, the priority
21 baton would be taken away from the maintenance program
22 and given to the safety function program.

23 The safety function program would do the
24 calculation as it was supposed to. But because of a
25 problem with the Intel 286 chip, sometimes that

NEAL R. GROSS

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

1 priority baton did not get passed back down to the
2 routine that had been interrupted. And a watchdog
3 timer would notice that the routine didn't complete on
4 time. And it would reset the slave processor.

5 And when the slave processor reset, the
6 operator assumed this channel was nonfunctional. So
7 that is a case there of, you know, it wasn't software,
8 it was really the darn chip. Self-testing routine,
9 right, that's -- self-testing, it has been my
10 experience in most of these, self-testing is really --
11 it has some benefits but it can cause some real
12 problems.

13 The load sequencer issue was caused by
14 self-testing functions. It wasn't the safety function
15 itself. It was all the self-testing to make sure the
16 safety function would operate correctly.

17 The main feedwater systems, we had a
18 recirc pump variable frequency drive, that was
19 actually -- that happened just last year at Browns
20 Ferry Unit 3 -- where is Alan at -- Unit 3, right,
21 Alan?

22 MR. HOWE: Yes, Unit 3.

23 MR. WATERMAN: Yes, in which that was a
24 datastorm issue that locked up the variable frequency
25 drives on the recirc pumps. So there are all kinds of

NEAL R. GROSS

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

1 different things that have been going on in the
2 industry. And most of these are precursors -- as a
3 matter of fact, I'd say a preponderance of all these
4 events are probably safety parameter display systems-
5 related events.

6 We've got a lot of SBDSs out there. Every
7 plant has got one. And any time the SBDS goes down,
8 they have to report it because the SBDS is used by the
9 operators to accomplish the safety function that is
10 reportable. So we have a lot of SBDS problems here.

11 We've got some plant security systems --
12 you know, that is access control for, you know, the
13 protected areas and things like that. We've had some
14 security problems with computers.

15 Emergency response data systems that are,
16 you know, sound the sirens. Some of those systems
17 have crashed.

18 And interestingly in the Operating Events
19 Report database, it describes the symptom, it
20 describes the system that was effected. And then it
21 provides the cause. In a lot of those causes, there
22 are no cause reported. System reset, no cause
23 reported. Restart it and keep on moving.

24 So anyway, across the top, D3 policy and
25 guidance, sort of a timeline of how we've put our

NEAL R. GROSS

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

1 policy together -- 91-292 out there, that was sort of
2 the first show at diversity and defense-in-depth.
3 Updated the SRP in '97. And then, you know, for about
4 ten years there we didn't do anything to the SRP. So
5 we're just starting to update it again here in 2006,
6 2007 time frame.

7 So anyway that kind of gives you an
8 overall perspective of digital equipment in the
9 nuclear industry. But I want to caution, not all of
10 those events are common-cause failures. They are just
11 events that happened in digital systems that show that
12 digital systems aren't as bulletproof as some people
13 might like you to believe.

14 Oh, well, we're going to replace our
15 obsolete analog stuff because digital is so much more
16 reliable, right. And when I heard that, it just
17 spurred me to go in and I didn't just do a keyword
18 search where I say I looked at computer and anything
19 that was computer popped up and I just did a count, I
20 had to read those things.

21 So if there are 340 events here, you can
22 imagine how many events I read because, you know, when
23 somebody took an SBDS down for routine maintenance,
24 that's not on that chart. That is not a failure of a
25 digital system. That's just doing business, you know.

NEAL R. GROSS

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

1 MR. ARNDT: Mr. Chairman, another issue
2 that you raised earlier was this concept of the fact
3 that common mode failure in hardware and software is
4 different because the systems are inherently
5 different, the recirc pump datastorm is a good example
6 of that.

7 That was a failure of a system not because
8 of the component itself or the software in that
9 component but because of data being provided in a very
10 rapid fashion across a communication bus which is a
11 different kind of failure mode and can lead to a
12 different kind of common-cause failures.

13 CHAIR APOSTOLAKIS: Well, that was a
14 common-cause failure, rights?

15 MR. WATERMAN: That one was, yes. That
16 was common-cause failure there.

17 MR. HOWE: Both of the variable frequency
18 drives failed. Excuse me, this is Alan Howe. I'm the
19 Chief of the Instrumentation and Controls Branch in
20 NRR.

21 And just for your information, we have a
22 draft of an information notice on that event that is
23 in process right now. It should be fairly close to
24 being issued. So that will provide a little bit of
25 additional background as to what happened in that

NEAL R. GROSS

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

1 event.

2 MR. WATERMAN: That's just a little
3 historical perspective in answer to your question, Dr.
4 Apostolakis.

5 CHAIR APOSTOLAKIS: Okay.

6 MEMBER ABDEL-KHALIK: Is there an apples-
7 to-apples comparison with analog systems?

8 MR. WATERMAN: I haven't done that. It's
9 probably a good idea to say well, maybe digital is
10 more reliable. And it may be.

11 MR. ARNDT: There have been some studies
12 in the literature associated with apparent reliability
13 after a change-out. There was a paper done -- help me
14 -- I think it was Korea -- after one of their analog
15 to digital change-outs and what their immediate
16 reliability was in terms of very gross availability
17 numbers.

18 But there has been very little specific
19 detailed analysis of diversity or reliability or
20 availability between the systems to my knowledge.

21 MR. WATERMAN: And I guess the other thing
22 I'd like to say is despite all of these failures, our
23 nuclear power plants have been safe in every case.
24 They have systems that would trip the plant, or they
25 would take control of the plant, or whatever, none 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 these are, you know, precursors to TMI.

2 The operators have always been on top of
3 it. In the case of the load sequencers at Turkey
4 Point, they identified the problem with that
5 particular malfunction like in less than a day, they
6 knew exactly what caused it.

7 So I'm not saying look at all the ways we
8 could have killed the public or anything like that.
9 That's not what I'm saying. The plants remain safe
10 but there is a potential precursor out there if
11 everybody doesn't do their job right. So far, people
12 seem to be doing their job right. But if everybody
13 doesn't do their job right, well, we have issues
14 coming down the road.

15 CHAIR APOSTOLAKIS: Good. So shall we go
16 on now with the discussion?

17 MR. ARNDT: At this point we basically
18 just wanted to give the Subcommittee an opportunity to
19 have a dialogue associated with what they have learned
20 and additional open questions to hope they gain our
21 insights on what the current position is and what you
22 might want to put forth to the Commission on your
23 opinions. So this is your opportunity to get what
24 information you need from us.

25 MEMBER MAYNARD: What I haven't heard --

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 I've heard a lot about what our plans are and what we
2 are planning to do and the various groups and
3 committees and things but I haven't heard are we to a
4 point yet of identifying what we are really looking at
5 proposing in the way of new change?

6 I understand the branch technical position
7 here but on more diversity or less diversity? More
8 defense-in-depth? Less defense-in-depth? Or where
9 are we going with it? I haven't heard too much about
10 that.

11 MR. WATERMAN: Well, until our research
12 gets completed, I really -- I don't want to force fit
13 a diversity strategy on the industry that just isn't
14 a very good strategy.

15 MR. KEMPER: Yes. I think we really need
16 to interact with the industry more and be sure that we
17 understand what their issues are primarily so we can
18 digest those and consider them all in conjunction with
19 the research results that we are obtaining right now.
20 So we're probably a couple -- two, three, four months
21 away from being at that point yet.

22 MR. HOWE: This is Alan Howe again. I'll
23 just add a little bit to this is that the existing
24 Commission policy and the branch technical position
25 right now provide an overall framework. It is a

NEAL R. GROSS

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

1 workable framework but as you have seen from the
2 discussion and presentation today, there are questions
3 that are coming up in terms of how do you apply this?
4 How do you answer that question?

5 I think there was a question early on
6 about what constitutes sufficient quality. So we're
7 now trying to fill in, if you will, and address some
8 of those questions. So one of the outputs would be to
9 identify what are the key questions out of the problem
10 statements? And go forward with addressing them with
11 clarifying what the position would be.

12 With regard to that, as you've seen right
13 now the policy, as we are going forward with
14 implementing it, is that diversity is an important
15 aspect in terms of overall safety at the plants. But
16 it is now just really answering these questions how do
17 you identify what is the adequate level of diversity
18 and defense-in-depth and how do you address the
19 solutions to that problem.

20 CHAIR APOSTOLAKIS: So if I look at the
21 SRM again, it says the short-term milestones should
22 address critical path actions. The critical path
23 actions are related to the eight statements -- problem
24 statements? These are --

25 MR. MAYFIELD: This is Mike Mayfield.

1 There are near-term and longer-term actions and
2 deliverables for each of those areas.

3 CHAIR APOSTOLAKIS: For each of these.

4 MR. MAYFIELD: Not so much for the -- in
5 diversity, it is not that they are broken out by each
6 of the eight. But for each of the six task working
7 group activities, there are near-term and long-term
8 activities.

9 CHAIR APOSTOLAKIS: Is it six or eight?

10 MR. MAYFIELD: There are six -- for
11 diversity and defense-in-depth, there are eight pieces
12 to the problem statement. There are six task working
13 groups.

14 CHAIR APOSTOLAKIS: Oh, I see.

15 MR. MAYFIELD: Of which diversity and
16 defense-in-depth is one of the six. Does that help?
17 No?

18 MR. HOWE: Part of what we are doing is we
19 are interacting with the industry to identify -- you
20 talked about the critical path items -- which ones are
21 the -- you know, from the industry's perspective, what
22 are the critical path issues that need to go out
23 there? That way it gives us -- informs us in terms of
24 how to apply the right resources in addressing those
25 issues earlier whereas some of the other ones could 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 longer-term-type of issues.

2 That's part of what we have asked for
3 feedback on the problem statements.

4 CHAIR APOSTOLAKIS: Well, let's clarify.
5 The six groups --

6 MR. MAYFIELD: Yes.

7 CHAIR APOSTOLAKIS: -- they were presented
8 earlier?

9 MR. MAYFIELD: We talked about them and
10 listed them for you.

11 MR. HOWE: If I could, I'll just give you
12 a little bit of perspective on that. When we briefed
13 the Commission back in November, they issued the
14 Staff's Requirements Memorandum. Subsequent to that,
15 a charter was issued by the EDO to form a Steering
16 Committee and also develop a project plan.

17 As we have developed in that process, what
18 we did is we looked at the key areas. And we
19 identified six key areas that we then further -- under
20 the oversight of the Steering Committee, we further
21 broke down into what we call our task working groups
22 to deal with the individual issues.

23 And I'll try to give you the list here off
24 the top of my head. Cyber-security is one of them.
25 Diversity and defense-in-depth is a second key area.

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 Integrated control rooms communications, integrated
2 control rooms human factors, risk informed, and last
3 area is licensing issues.

4 CHAIR APOSTOLAKIS: Well, you did a good
5 job.

6 MR. HOWE: So we tried to chop apart the
7 big problem and establish what we call these task
8 working groups to focus on the individual areas.
9 There is also going to be interactions with the
10 external stakeholders on that as well as interactions
11 both at the working group level and at the Steering
12 group level to ensure that we do go forward with a
13 coherent approach here.

14 Because what we don't want to do is to
15 have the different parts getting out of synch and we
16 have recommendations coming from one group that are at
17 odds with recommendations from another group.

18 MR. KEMPER: Yes, if I could add just one
19 more segue onto what Alan said and primarily we didn't
20 just think of these things from thin air, we drew this
21 from industry. We have been interacting with industry
22 for quite some time on this.

23 And I think our first meeting was back in
24 March of last year where we started talking about some
25 of these issues. And then we had another

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 comprehensive meeting I think it was in October.

2 MR. HOWE: October 19th.

3 MR. KEMPER: And that is really where most
4 of the issues were bubbled up, if you will, to us from
5 the industry. And so from that, that is where we put
6 together the picture of what you see now as far as the
7 critical issues that have to be addressed to address
8 the short-term critical path items.

9 CHAIR APOSTOLAKIS: So when the Commission
10 says critical paths, these six are the critical paths?

11 MR. HOWE: These are the key issues that
12 we have identified. And now what we are working on is
13 subsets from those broad issues, what are the critical
14 issues --

15 CHAIR APOSTOLAKIS: Within each of the
16 areas.

17 MR. HOWE: -- that we need to focus on
18 immediately. And which ones will be dealt with in the
19 longer term.

20 CHAIR APOSTOLAKIS: Okay. That makes it
21 clear.

22 So today then we heard only -- well, we
23 focused on Key Area B, diversity and defense-in-depth.
24 That's correct?

25 MR. ARNDT: So we'll talk about risk-

NEAL R. GROSS

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

1 informed this afternoon.

2 CHAIR APOSTOLAKIS: This afternoon, okay.

3 MR. ARNDT: Now, if I could --

4 CHAIR APOSTOLAKIS: We are asked to
5 comment on this? Then we have an SRM that says the
6 Committee should provide its view to the Commission on
7 staff's effort related to digital instrumentation
8 control. The Committee should consider potential
9 means for providing reasonable backup if appropriate.
10 Are we writing two letters, Gary? One on the staff's
11 efforts? And one on --

12 MR. JUNGE: No, we're just writing --

13 CHAIR APOSTOLAKIS: One letter.

14 MR. JUNGE: Yes, we're writing one on the
15 SRM.

16 CHAIR APOSTOLAKIS: This was Mike Junge.

17 MR. ARNDT: Yes, George. The reason we
18 structured this presentation the way we did is you
19 need to write a letter on generally what we are doing
20 but also specifically the back-up issue which --

21 CHAIR APOSTOLAKIS: That's correct.

22 MR. ARNDT: -- goes to this issue and
23 other issues associated with D3.

24 CHAIR APOSTOLAKIS: But we cannot really
25 say anything on the four key areas that we are 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 discussing today.

2 MR. ARNDT: That's correct.

3 CHAIR APOSTOLAKIS: Unless we go back to
4 the research plan which I don't think would be the
5 appropriate thing to do.

6 MR. MAYFIELD: Well, if you wanted to do
7 that what we would need to do is get you the task
8 plan, the project plans for each of these six areas.

9 CHAIR APOSTOLAKIS: These areas.

10 MR. MAYFIELD: And I think it would -- to
11 get you that information in a timely fashion so that
12 you could review it and we could engage with you in
13 this setting or the full Committee, I think that would
14 be probably useful but challenging in time.

15 CHAIR APOSTOLAKIS: What do my colleagues
16 think? I mean the Commission's charge is very clear.
17 The staff's effort related to digital I&C. And then
18 specifically on backups. So we know about that.

19 So with the afternoon's presentation, we
20 can address also the key area on risk-informed digital
21 I&C. But we will not have any plans for how to handle
22 cyber-security, highly integrated control rooms, and
23 the licensing process.

24 Should we then agree that maybe at the
25 full Committee meeting we'll have a briefing on your

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 plans in these areas?

2 MR. MAYFIELD: Why don't we take as an
3 action and work it back with the ACRS staff and come
4 back to you with a proposal as to what we could do in
5 two weeks to give you the broad picture about all six
6 working groups. Obviously it can't be at this level
7 of detail.

8 CHAIR APOSTOLAKIS: Right. But what do
9 you --

10 MEMBER MAYNARD: I'm not sure that we --
11 well, first of all, I think that would probably be
12 good, the big picture view. I'm not sure that we have
13 to evaluate or review each specific area.

14 I think probably of bigger value would be
15 are these the right areas. You know is there
16 something else that is not there or whatever. But are
17 there -- do they have a plan in the right areas or is
18 there some big part of the picture that is missing
19 here.

20 CHAIR APOSTOLAKIS: To answer this, we'd
21 would definitely need what Mike said. We'd need this
22 overall view. So we can address this question and
23 then maybe focus more on the D3.

24 MEMBER KRESS: Well, I think we need the
25 overall picture. But two weeks is not a lot of time.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: It is not a lot of
2 time but they can get it done in that time.

3 MR. MAYFIELD: Given the amount of time we
4 are likely to get on a full Committee agenda to give
5 you a snapshot of the six areas --

6 MEMBER KRESS: This one of those cases
7 where I think we need to have the written invitation
8 far ahead time to read because we're not going to be
9 able to get enough --

10 MR. MAYFIELD: We can certainly provide
11 you the draft information that has been shared
12 publicly, recognizing it is draft.

13 MEMBER KRESS: That's all right. We do
14 that all the time.

15 MR. MAYFIELD: And we have been
16 specifically asking for comment and frankly to have
17 comment back from the Committee would be very useful
18 at this time. Six months from now, it is going to be
19 a whole lot less useful simply because we're going to
20 be moving.

21 MEMBER KRESS: So I think we ought to
22 comment on the whole plan --

23 CHAIR APOSTOLAKIS: I think so, too.

24 MEMBER KRESS: -- because I think we're
25 asked to.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: That's what the
2 Commission wants.

3 MEMBER KRESS: Yes. And the only way to
4 do it is to get the written information at least a
5 week before the meeting.

6 CHAIR APOSTOLAKIS: Yes. And this should
7 go to the full Committee.

8 MR. ARNDT: We will get that to you late
9 this week.

10 MEMBER KRESS: Okay. That would be good.

11 CHAIR APOSTOLAKIS: I think you can have
12 a shorter presentation than what was presented today.
13 A lot of it, I think, the members are more or less
14 familiar with.

15 MEMBER KRESS: Yes.

16 CHAIR APOSTOLAKIS: So a discussion of
17 each of the six areas and then saying for diversity
18 and defense-in-depth, here is a little more detail.
19 For risk informing, here is a little more detail it.
20 That should do it. We have an hour-and-a-half?

21 PARTICIPANT: Yes.

22 MEMBER KRESS: Now we had a full meeting
23 on the risk informed some time ago. I don't know if
24 that's --

25 CHAIR APOSTOLAKIS: More than a year ago

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I believe.

2 MEMBER KRESS: Yes, I don't know if that
3 has changed a lot.

4 MR. MAYFIELD: One of the other points
5 that I guess I had wanted to make with you gentlemen
6 is that there is a disconnect or a potential
7 disconnect in schedule interest for new reactors
8 versus the operating fleet. And where the fuel cycle
9 facility interests fit in in that schedule is
10 something I guess I'm still interested in learning
11 about.

12 The approach we are taking, when you see
13 these plans, you will see some discussion about
14 interim guidance and then longer-term where we would
15 fix up the SRP, fix up the reg guides and so have you.
16 The intent is that we will provide interim guidance to
17 support the first schedule need, which is almost
18 always going to be the new reactor interests.

19 I think when we first got into this, that
20 wasn't quite as clear as it has become. Where the
21 pacing issues appear to be the COL applications as
22 well as some of the design certification reviews for
23 new reactors. So we are looking at interim guidance
24 to make sure we are actively moving to support the
25 rate-limiting licensing activity.

1 Mike talked about the longer-term research
2 that will -- as systems continue to evolve, as
3 interests continue to evolve, then I think the
4 research fits in further adjustments downstream. But
5 our interest -- and I think the industry's interest is
6 to provide guidance in a timely manner, recognizing
7 that may evolve a little bit for future systems,
8 future applications. But that's -- I'm sorry?

9 CHAIR APOSTOLAKIS: This memo from Mr.
10 Grobe says that there are six attachments. Are these
11 relatively short attachments? I mean maybe we can get
12 those. I mean it is up to you.

13 MR. MAYFIELD: What letter are you looking
14 at?

15 CHAIR APOSTOLAKIS: It says in order to --
16 from Grobe -- Digital I&C Project Plan.

17 MR. MAYFIELD: Yes. We can provide those.
18 It's not hundreds of pages.

19 CHAIR APOSTOLAKIS: Good.

20 MR. MAYFIELD: It's 20, 25 pages.

21 CHAIR APOSTOLAKIS: All together?

22 MR. MAYFIELD: Yes.

23 CHAIR APOSTOLAKIS: Yes, that's fine.

24 MR. MAYFIELD: So it is probably --

25 CHAIR APOSTOLAKIS: That probably would be

NEAL R. GROSS

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

1 a good think to have.

2 MR. MAYFIELD: It is just a matter of
3 setting somebody in front of a computer, hitting the
4 print key and getting them in front of a copier to get
5 copies over to Gary.

6 CHAIR APOSTOLAKIS: Very good.

7 MR. HOWE: Just one other thing I would
8 offer up is that in the Commission's SRM back in
9 December, they also had staff set up a digital
10 instrumentation control website. And that website was
11 established I think in January as a kind of Phase I
12 process.

13 But that is also information that is
14 readily available right now in terms of background.
15 Some of these subjects that we have talked about in
16 detail today and some of the topics of the working
17 groups are also described in the different pages in
18 the website.

19 CHAIR APOSTOLAKIS: And that is at the
20 nrc.gov?

21 MR. HOWE: It is an NRC public website.

22 MR. ARNDT: But we will give you the
23 specific address in the transmittal.

24 CHAIR APOSTOLAKIS: Good. Good.

25 DR. GUARRO: George, this is Sergio. Can

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you hear me now?

2 CHAIR APOSTOLAKIS: Yes.

3 DR. GUARRO: Oh, okay. I have a question
4 with respect to the research in the diversity and
5 defense-in-depth. Is there anything specifically in
6 your research plan that looks at whether one can go
7 beyond the block approach, so to speak?

8 In other words, if I understand correctly
9 now a common-case failure is assumed to occur in one
10 of these blocks. And everything proceeds from there.
11 Wouldn't, you know, a path would be perhaps a little
12 bit less conservative if possible to look beyond that
13 level? And try to see if there are ways of being able
14 to classify types of common-cause failures within a
15 block?

16 And also from the point of view of the
17 remedies, prove that the remedy indeed addresses with
18 sufficient diversity a particular type of common-cause
19 failure?

20 CHAIR APOSTOLAKIS: The blocks you are
21 referring to are the ones in the old NUREG, right?

22 DR. GUARRO: Right, right, well, yes, I'm
23 referring to the current approach. So, you know, is
24 there some attempt to look beyond that level of --
25 well, I think is pretty top level in terms of 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 assumption made.

2 MR. KEMPER: Sergio, this is Bill Kemper,
3 let me start it out, Mike, and you just jump in here.
4 We really hadn't talked about it from the perspective
5 yet. Your point is well made. The block strategy of
6 trying to diagnose the portions of a digital
7 processing system that is subject to a common-cause
8 failure is difficult to decipher.

9 And so generally speaking what the
10 industry inventors have done, they have just assumed
11 the whole platform fails, right, because to provide an
12 analysis with finer granularity would mean you would
13 actually be looking at circuit boards, you would be
14 looking at microprocessors, semiconductors, that sort
15 of thing. And it has generally been my experience in
16 talking with many folks over the years on this, it is
17 just not cost effective to do that type of analysis.
18 That is why they don't generally get into it in that
19 detail.

20 DR. GUARRO: Well, I wasn't referring to
21 much to the, you know, circuit board level. I mean
22 the block approach is taken -- isn't it taken also at
23 the functional level so for other types, isn't it also
24 assumed? And the same way for software? Or, you
25 know, any of these major functional components?

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. LOESSER: On the analysis we've seen
2 so far, no one has even gone to the block level yet
3 because of the increased level of complexity that this
4 would offer. If, however, a licensee did go down to
5 the block level or even went further, we would have no
6 objection. It might be a little more difficult to
7 review but we'd certainly take a look at it.

8 DR. GUARRO: No, I guess what I'm asking,
9 I understand that currently that is what is done
10 because nobody is able to do better or thinks that it
11 is not possible to do better but as part of your
12 research, if one wants to try to see how one can be a
13 little bit less, you know, broad-brush conservative,
14 so to speak, shouldn't the research try to determine
15 if there has been a circumstance that permits to go to
16 a lower level in some areas?

17 I'm not saying -- obviously I intuitively
18 agree that in certain areas, probably we haven't made
19 any progress. But maybe in some of the areas in which
20 the present approach is applied, one could go a little
21 deeper and save themselves some conservatism.

22 CHAIR APOSTOLAKIS: Well, that would be a
23 longer term issue, right?

24 DR. GUARRO: Right, right. I'm talking
25 about longer-term research. But I mean since in the

NEAL R. GROSS

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

1 discussion I haven't heard anything that goes in that
2 direction, that is why I was asking the question.

3 MR. KEMPER: No, this is Bill Kemper
4 again, clearly we're trying to focus on a set of
5 suitable diversity attributes because right now 6303
6 just mentions them in general. And it doesn't really
7 give you any guidance on how to deploy or implement
8 that guidance. So that is what we are trying to do
9 now is refine that guidance from how do you build in
10 diversity into your design.

11 What we're seeing pretty much now is what
12 is being submitted to us is here is our design. Now
13 let's see how that matches up with 6303 criteria. And
14 then find ways of coping with the lack of diversity,
15 in many cases, that exists with a given design.

16 But it is certainly something that we can
17 look at in the long term, I believe, as we work
18 through this research. We just haven't talked about
19 it in detail. It doesn't mean that we are not
20 thinking about it or going to do that. That is
21 probably the next phase.

22 DR. GUARRO: You know it would seem that
23 in order to answer the question of how much diversity
24 is enough, one has to understand a little bit more
25 about, you know, the nature of the problem that

NEAL R. GROSS

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

1 effects the common cause issue. And so that, you
2 know, you can decide what type of diversity works for
3 what, so to speak. So anyhow, that's just a thought.

4 CHAIR APOSTOLAKIS: Thank you.

5 Okay, so it seems like we are beginning to
6 formulate the presentation to the full Committee.

7 MR. ARNDT: Let me reiterate. I think
8 what I heard was the general overview of what we are
9 doing and why we are doing it. And what the structure
10 is. I'm sorry -- a general overview of what we're
11 doing, why we are doing it, what the plan is about,
12 how we are getting there. A short review of what we
13 talked about this morning. Did you also want a short
14 review of this afternoon's presentation?

15 CHAIR APOSTOLAKIS: I think that would be
16 useful, yes.

17 MR. ARNDT: Okay.

18 CHAIR APOSTOLAKIS: Although the Committee
19 is probably more familiar with the afternoon. But so
20 you use your judgment.

21 MEMBER KRESS: Since the last time we had
22 this meeting, there have been a lot of new members
23 added.

24 CHAIR APOSTOLAKIS: And we have a lot of
25 new members, you are right.

NEAL R. GROSS

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

1 MEMBER KRESS: So it might be worthwhile.

2 MR. ARNDT: Okay. We will have to manage
3 this because of the timing issues. But we will get
4 with you. And we will start with that as a start and
5 work through that.

6 MR. MAYFIELD: Well, let me add -- this is
7 Mike Mayfield -- let me add that I think it would
8 useful for the full Committee to hear it because I
9 think the risk area is one where there is probably the
10 greatest disconnect with the industry based on what I
11 heard. So I think that would be useful for the
12 Committee to hear. Where we are and why we think we
13 are going where we are going.

14 CHAIR APOSTOLAKIS: And I'm not sure now
15 will the industry have time at the Committee meeting?

16 PARTICIPANT: Yes.

17 CHAIR APOSTOLAKIS: About 15 minutes or
18 so?

19 PARTICIPANT: Yes, we will be providing
20 that time.

21 CHAIR APOSTOLAKIS: Yes. So we should
22 take that into account.

23 MR. ARNDT: We will work it out, yes.

24 CHAIR APOSTOLAKIS: Okay.

25 MR. WATERMAN: This is Mike Waterman.

NEAL R. GROSS

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

1 Just one comment.

2 CHAIR APOSTOLAKIS: Yes.

3 MR. WATERMAN: The purpose of the research
4 stems from if an applicant came to the NRC today and
5 said we have a diverse system. We have used different
6 microprocessors and different channels. We have used
7 two different management teams and development teams
8 to develop the software.

9 We have rearranged the software so there
10 is a different order of software processing in each
11 channel, and we think that is enough diversity -- it
12 sounds good -- but we don't have any guidance at the
13 NRC right now that says that is good enough or not
14 good enough or any basis for saying why it is not good
15 enough.

16 So the licensees and the applicants out in
17 the industry haven't got a clue of what to do for
18 diversity and defense-in-depth because frankly I don't
19 think we've got a clue on how to handle it. And that
20 is what the focus of this research was is to try to
21 nail that down so that when a licensee comes in here,
22 they know what the answer is before they come in. And
23 we know what the answer is when we take a look at
24 something.

25 CHAIR APOSTOLAKIS: Now one other point,

1 we've heard the words short-term, long-term. Mr.
2 Mayfield said earlier that under the eight problem
3 statements that refer to defense-in-depth, there are
4 long-term and short-term issues.

5 Can we make that a little more explicit at
6 the full Committee meeting? What is short term? What
7 is long term?

8 MR. MAYFIELD: Yes, the challenge is that,
9 as several folks have suggested, we are looking to
10 prioritize, looking for interest from the industry on
11 priorities for the various activities. Specific
12 dates, when you get this information, you are going to
13 see a lot of open slots in the table.

14 CHAIR APOSTOLAKIS: Right.

15 MR. MAYFIELD: And the reason is we are
16 waiting on that priority information to finalize the
17 specific schedules. But relatively we can give you a
18 sense of what --

19 CHAIR APOSTOLAKIS: That's what I mean.

20 MR. MAYFIELD: -- short- and long-term
21 mean.

22 CHAIR APOSTOLAKIS: Yes, like Mike
23 Waterman just said, you know, we really need these
24 because we don't know and the industry doesn't know.
25 That's a short-term need.

NEAL R. GROSS

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

1 MR. MAYFIELD: I look at it as short term

2 CHAIR APOSTOLAKIS: Yes, it is short term.

3 MR. MAYFIELD: Yes.

4 CHAIR APOSTOLAKIS: But you don't have to
5 tell us, you know, by May such and such, no. That
6 would be useful.

7 MR. MAYFIELD: We will give you some
8 insight on that.

9 CHAIR APOSTOLAKIS: Anything else?

10 (No response.)

11 CHAIR APOSTOLAKIS: This is a happy
12 meeting. We'll break for lunch and be back at one
13 o'clock.

14 (Whereupon, the foregoing
15 matter went off the record at
16 11:47 a.m. to be reconvened in
17 the afternoon.)

18

19

20

21

22

23

24

25

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

2 1:00 p.m.

3 CHAIR APOSTOLAKIS: Okay. We can start
4 again.

5 And the first presentation is from NEI.

6 MR. MARION: Good afternoon. My name is
7 Alex Marion with NEI. And with me is Kimberly
8 Keithline.

9 I just would like to make a couple of
10 comments regarding the staff activity relative to
11 modeling, if you will, digital systems. Our basic
12 needs are rather straightforward. One is we want to
13 ensure we have quality PRAs, probabilistic risk
14 assessments, and we minimize requests for additional
15 information that the NRC may call for.

16 And we want to be able to use risk
17 insights to allow us to focus on the risk-significant
18 aspects, if you will, of digital system performance.
19 And, of course, in order to do that, operating
20 experience is extremely important in developing a
21 database so you can make some reasonable estimation of
22 failures, et cetera, and get a better understanding of
23 the performance of these systems.

24 So we agree that that is a very important
25 area. And we are going to look into that. And also

NEAL R. GROSS

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

1 work with the NRC staff to make sure we are not
2 duplicating efforts unnecessarily.

3 But I do want to make it very clear that
4 we think the -- we don't support the detailed modeling
5 aspect that the staff is going to talk about this
6 afternoon or any research related to advancing the
7 state of the art. We don't think that that is needed
8 relative to digital system applications in nuclear
9 power plants.

10 And the reason for that is very
11 fundamental. Every industry in this country has
12 applied digital technology except the nuclear
13 industry. And a lot of the utilities are hesitant in
14 doing that because of the uncertainty in the
15 regulatory process.

16 But what we have in place with the
17 Steering Committee and these task working groups will
18 provide some structure to what the issues are so that
19 we can stabilize the regulatory process going forward.
20 But we need to keep a focus on research that will
21 accommodate or support that activity in the near term.
22 And that's basically where we are coming from.

23 We also believe that the existing PRA
24 methods are adequate and sufficient to model digital
25 technology. And we haven't seen any work indicating

NEAL R. GROSS

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

1 that there are gaps, if you will, in the use of PRA
2 technology today.

3 I'm trying to recall if the NRC had done
4 any work to identify gaps or vulnerabilities in PRA
5 models that are being used today. I don't recall.

6 MS. KEITHLINE: There was -- and help me
7 out here, guys, if you need to -- I think there was a
8 NUREG-6901 that had a list of reasons why you might
9 need to do more detailed or dynamic-type modeling.
10 And our industry folks who are knowledgeable in this
11 area think that those tend to be things that people
12 wouldn't use in safety systems.

13 And, Jeff, you may want to -- Jeff Stone
14 from Constellation probably has a better, more
15 detailed answer. I'm pretty new to the PRA part of
16 this.

17 MR. STONE: We have looked at -- oh, I'm
18 sorry, Jeff Stone from Constellation -- we have looked
19 at the 6901 and the newer research that we reviewed in
20 December that hasn't come out yet, I don't believe
21 that has a number that I know of yet -- at this point
22 we haven't seen any quantitative evaluations that show
23 dynamic modeling will have a significant impact on
24 overall core damage frequency or a significant impact
25 on the probability of failure of a system.

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 what will be driving it is probably
2 the software probabilities we use or potentially a
3 hardware common cause failure probability between
4 computers. We do encourage the research to go forward
5 if that is the intention.

6 But before we implement something as
7 complicated and as costly as dynamic modeling, we feel
8 that there should be some sort of cost benefit to show
9 that there is a significant change to our models to
10 require this sort of expense.

11 And I think I've gone over my time but
12 that's my opinion.

13 CHAIR APOSTOLAKIS: Thank you.

14 MR. MARION: Yes, with regard to dynamic
15 modeling, we are concerned with the added complexity
16 it is going to provide. And then quite frankly the
17 practicality of it all. We feel reasonably confident
18 in the techniques currently available.

19 We think that in the near term, as an
20 alternative to dynamic modeling, we need to do some
21 work to better define software failure probabilities,
22 focus a little bit of effort on failure modes and
23 effects, and as we said earlier, start collecting and
24 evaluating operating experience with the existing
25 systems.

1 And we think that from a design
2 perspective, we can deal with the recognized set, if
3 you will, of common cause failures such that we can
4 provide reasonable assurance that these systems will
5 function properly and maintain safety at the plants.
6 And that completes my comments. I don't know if you
7 want to elaborate on that.

8 MS. KEITHLINE: We've -- this is Kimberly
9 Keithline -- the part that we are most concerned about
10 is what you will see as the third problem statement
11 within this task work group on risk related to
12 developing or implementing state-of-the-art techniques
13 and the dynamic modeling as an example.

14 There are two other problem statements
15 that we are more on board with, the first dealing with
16 more life refining techniques to be used for design
17 certification and COL applications, how we would use
18 them near term to support using digital I&C in the new
19 plants.

20 And then the second would be more like a
21 simplified approach to be applied to existing plants
22 and maybe new plants -- existing plant upgrades -- we
23 think that may be a useful thing that would help
24 support and even improve diversity and defense-in-
25 depth evaluation process.

1 And the NRC staff, I think they are
2 planning to describe what they are doing in all three
3 of those areas. So we are more aligned on the first
4 two and it is really the third area that we have the
5 most concern with.

6 CHAIR APOSTOLAKIS: Are you opposed to
7 this particular approach? Or attempts to develop
8 models for risk evaluation in general? The risk
9 evaluation with a digital I&C obviously. In other
10 words to bring the digital I&C into the PRA.

11 Now you may say that you don't see any
12 value to this dynamic modeling. Or this is a subject
13 we shouldn't worry about at all.

14 MR. MARION: It is the value aspect of the
15 dynamic modeling. We just think it provides
16 unnecessary complexity and really don't think it is
17 needed because of everyone we have talked to within
18 the industry from the standpoint of PRA practitioners
19 are indicating to us that the PRA methodology today
20 should be adequate and sufficient to effectively model
21 digital systems and determine the risk significance of
22 any problems you can have with those system designs.

23 CHAIR APOSTOLAKIS: Well, I see it as the
24 problem having two parts. The first part is
25 identifying potential failure modes. Maybe additional

NEAL R. GROSS

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

1 minimal cut-sets or whatever. That will be a
2 combination of the traditional events that we have in
3 the PRA plus a contribution from digital systems. And
4 that is extremely important also as we said earlier to
5 discuss diversity, and defense-in-depth, and all that
6 stuff.

7 And then you have the issue of
8 quantification, which is much tougher in my view and
9 much more difficult to achieve. It seems to me that
10 for the first part, my view is that it is a necessary
11 thing to do and we should try to identify and to
12 develop those methods to understand because the
13 failure modes of software are not understood as well
14 as the failure modes of analog systems or hardware
15 obviously so the issue is there, you know, are we
16 missing anything and so on.

17 When it comes to probabilities, I think it
18 is a much longer-term issue. And, you know, there are
19 certainly many ideas how to approach the issue. Is
20 the dynamics of the situation an essential part of it?
21 Or can we do it somewhere else? As you probably know,
22 there have been fault trees in the past that have been
23 applied to digital systems.

24 So the issue -- especially because a lot
25 of the failure are due to specification errors which

NEAL R. GROSS

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

1 are the equivalent of design errors and we really
2 don't know how to handle those.

3 But the first part, I guess, is really
4 more urgent, the identification of the failure modes
5 it seems to me.

6 MR. MARION: Yes, we also feel that from
7 the standpoint of software performance, that the
8 software development process can address a lot of the
9 issues to provide some level of reasonable assurance.
10 The question becomes one how much is enough.

11 You know you are not looking at an
12 environment where you have one individual cranking out
13 lines of code anymore. That is the way it was 15, 20
14 years ago. Software development has changed
15 significantly in that time.

16 So we think there are adequate techniques
17 out there now that can be credited in assuring some
18 sense of reliability in the performance of the
19 software.

20 CHAIR APOSTOLAKIS: But the words
21 reasonable assurance, of course, are part of the
22 traditional way of doing business.

23 MR. MARION: Right.

24 CHAIR APOSTOLAKIS: We want to quantify --
25 and I remember I believe it was the AP 1000 and maybe

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 others where they just assumed that, you know, all the
2 software went down, see what happens, it was more of
3 a sensitivity kind of analysis rather than quantifying
4 what is going on.

5 Okay, any questions?

6 (No response.)

7 MR. MARION: Thank you.

8 CHAIR APOSTOLAKIS: Thank you very much.

9 And now we move on to Mr. Douth, NRC
10 short-term activities associated with risk-informing
11 digital system reviews.

12 MR. ARNDT: Let me give a brief
13 introduction. This afternoon's presentation is going
14 to be a series of presentations talking about where we
15 are in the terms of digital system research as well as
16 the shorter-term activities.

17 Cliff is going to give a presentation
18 basically on the current status associated with what
19 the TWG, task working group for risk is, what the
20 problem statements are, and how they align with our
21 current work.

22 After we go through that, I'm going to
23 give a short update of where we are in the dynamic
24 reliability modeling.

25 And then we're going to have a longer

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 presentation on the traditional reliability modeling,
2 which is the parallel program that you have heard
3 about but not as much detail as the dynamic
4 reliability modeling.

5 Then I'm going to give you a real short
6 presentation on where we are in regulatory guidance.
7 It will become obvious as we go that since we have
8 been more directed toward short-term guidance, the
9 longer-term formal regulatory guidance in this area
10 has been put back. But I'll give you just basically
11 a five-minute version of that 30-second statement at
12 the end of the day.

13 CHAIR APOSTOLAKIS: Okay.

14 MR. DOUTT: We'll try this again. Good
15 afternoon. My name is Cliff Doutt. I'm with the PRA
16 Licensing Branch in the Division of Research.

17 CHAIR APOSTOLAKIS: PRA Licensing Branch,
18 are you licensing PRAs?

19 MR. DOUTT: No, licensing as in licensing
20 actions.

21 CHAIR APOSTOLAKIS: Oh, I see.

22 MR. DOUTT: And don't I wish. In the
23 Office of Nuclear Reactor Regulation. Basically I
24 think Steve kind of did the beginning here but what
25 we're basically trying to do here is do a presentation

NEAL R. GROSS

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

1 on what the working group has come up with in the way
2 of project plans, tasks, problem statements, and
3 whatever on how we try to incorporate risk insights
4 into methods to review digital I&C systems.

5 I'll tend to use digital I&C systems a
6 little more than other people have done. It is simply
7 because I think it is a little wider subject that just
8 defense-in-depth and diversity. That is keeping with
9 our project goals in long-term work.

10 We have had a couple of meetings of the
11 working group so far. The first one was in February,
12 on the 23rd. And we had a second one April 11th and
13 12th. That's with industry, public meeting, to try to
14 hash out, again, the problem statements and project
15 plan. We've issued -- well, we'll get into that but
16 we've issued a draft of the project plant.

17 Based on this, there are future meetings
18 planned. One for hopefully the end of May. And so
19 everything we are doing here is pretty preliminary.
20 Keep that in mind on this regard to ongoing work.

21 This gets us to more introduction. We'll
22 do a background which is just a quick review of where
23 we think we are right now. We'll go through the
24 problem statements, what we think the goals of the TWG
25 should be and maybe what we think they are going to

NEAL R. GROSS

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

1 be, project plan, what we think the deliverables will
2 look like, a very general approach, I would think,
3 will address the problem.

4 And, again, we'll do a little bit of
5 discussion on application of PRA so far in digital
6 systems and where we think this has occurred. And
7 what has happened. And out of that, I'll give you a
8 real brief insight as to what we've seen so far.

9 And, again, I'll make a list of challenges
10 that we would think we will need to look at, resolve,
11 or address in order to implement PRA in a -- digital
12 system in a PRA. We'll discuss briefly on schedule
13 and then there will be a conclusion.

14 And this is a refresher from this morning
15 really. You've seen the presentations on
16 deterministic defense-and-depth and how to deal with
17 that. That's the current way of doing it. Specific
18 digital I&C system development, design, testing,
19 maintenance, and staff review processes are basically
20 deterministic. That is how it is being done.

21 The process is to ensure adequate quality,
22 reliability, and diversity and defense-in-depth when
23 implementing a digital I&C system. Why we're doing
24 what we are doing now, one of the reasons is is
25 within the staff requirements dated December 6th,

NEAL R. GROSS

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

1 there was an item in there to address risk-informing
2 as a topic for deployment of digital I&C.

3 So one of the things in deterministic
4 space as far as that staff requirements goes,
5 licensing actions to date involve usually a
6 significant amount of staff and licensing effort. So
7 one of the things is to see how we can address that.
8 And based on that SRM, the TWG was formed. And where
9 we are at.

10 Current short-term tasks and what we
11 believe currently is existing guidance does not
12 provide us sufficient clarity on how to use current
13 methods to properly model digital systems in PRAs for
14 design certification applications or license
15 applications under Part 52.

16 There is a second part to this, too, which
17 is using current methods for PRAs. In that respect,
18 the NRC has not determined how or if risk insights
19 could be used to assist in the resolution of key
20 specific digital system issues in operating reactor
21 licensing action requests and specific defense-in-
22 depth and diversity.

23 Just a little clarification, obviously the
24 first one is Part 52. The second one which is
25 operating plants, one of the reasons to divide those

NEAL R. GROSS

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

1 is just requirements of PRA in general. In Part 52
2 there is a PRA in operating plants. A little
3 different perspective. So one of the reasons to split
4 those.

5 This is the long-term tasks. I'm not
6 discussing it except just to bring it up and that it
7 exists and we are considering the work to try to
8 develop a state-of-the-art method for a detailed
9 modeling of those systems. And one of the things is
10 to advance the state of the art in order to provide a
11 comprehensive risk-informed decision-making framework.
12 We don't believe we have that right now.

13 And this would include licensing reviews
14 of digital systems for current and future reactors.
15 So that is a fairly significant long-term task. And
16 a wider scope than the short term as you'll see as we
17 move forward.

18 MR. ARNDT: This is really what you heard
19 the industries say. They are not in agreement with us
20 in the fact that the staff currently does not believe
21 that the state of the art is such that you can do
22 detailed quantified digital system reliability models
23 to a standard like 174. So the words here have been
24 carefully chosen to not make any specific statement as
25 to what the state of the art is. We refer to it as

NEAL R. GROSS

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

1 not been established from a regulatory standpoint to
2 take into account that there is a disagreement on this
3 level of the state of the art.

4 The first two tasks, number one in Part 52
5 space, on what is necessary for that particular
6 licensing action and number two is short-term use of
7 risk insights for things like D3 and other issues was
8 the points that Kimberly was making earlier.

9 MR. DOUTT: Next slide. So from the risk
10 task working group goals, we've set the up --
11 basically improve the NRC review process is obviously
12 a goal.

13 We also thought if we could implement risk
14 assessment in a D3 or import it in for digital systems
15 that we could look at -- get a better insight into
16 vulnerabilities including diversity and defense-in-
17 depth. And it is a little different review structure
18 than design basis and a strictly deterministic way of
19 looking at it.

20 That may help improve some insights as to
21 where -- that may improve on the question from this
22 morning as to where and when and how much. I guess
23 this is a place where we think there might be some
24 benefit.

25 To do that -- and I split the task down --

NEAL R. GROSS

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

1 is to provide some interim guidance on the use of
2 current PRA methods in modeling digital systems. And
3 we would do this in design certification and COL area.

4 The other part of this is provide some
5 type of interim approach on use of risk insights in
6 the licensing review. And, again, we split this.
7 Let's see if there is anything else. Again, basically
8 that was --

9 CHAIR APOSTOLAKIS: So why do you have the
10 two sets separated?

11 MR. DOUTT: One of the reasons to separate
12 them -- this was the request but part of it is, too,
13 is how we think going forward the COL design
14 certification has a PRA and a rule structure and
15 different acceptance guidelines. Operating plants can
16 come in risk-informed, non-risk-informed. And
17 acceptance guidance we are not as clear on and it is
18 different.

19 And that's how we -- we feel -- and the
20 two tasks are just different. To look at how those
21 models may be structured. Now -- and I see comments
22 but one of the --

23 MR. STONE: Cliff, can I --

24 MR. DOUTT: Sure, go ahead.

25 MR. STONE: -- can I just comment one

NEAL R. GROSS

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

1 point.

2 CHAIR APOSTOLAKIS: Give your name please.

3 MR. STONE: I'm sorry, Jeff Stone,
4 Constellation. What we had considered the second for
5 was BTP-19 right now is relatively deterministic. It
6 does have the best estimates. We were looking for are
7 there any ways we can use any risk screening risk
8 insights into those in the BTP-19. If there is any
9 way that the NRC would find acceptable or we could
10 find acceptable between -- in the task working group
11 and with the NRC?

12 MR. DOUTT: And we weren't quite that
13 specific.

14 CHAIR APOSTOLAKIS: But all four are short
15 term, right?

16 MR. DOUTT: Yes. That is the intent.

17 Now project plan, currently we are looking
18 to receive a couple of industry technical papers. One
19 is on PRA methods which applies to -- when we go into
20 the problem statements you will see that, PRA methods
21 of either a simplified or whatever -- there is also a
22 document on lessons learned. We would like to
23 incorporate those with staff PRA risk insights which
24 we hope will look at key principles and methods and
25 what we have done so far. We just need to go back 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 take a look and see what has happened. Most of that
2 has got to be in design cert. space.

3 Operating reactors have not employed PRA
4 in a digital system in the licensing. And the other
5 thing is to look at research as what we've done to
6 date. And this is a wide focus. Not just what we've
7 done, completed, go out to industry, academia, the
8 usual things, and see if we can pull some insights in
9 and try to incorporate them in a short-term solution.

10 The other thing, which is relatively
11 important -- I think it is very, very important
12 actually -- is to integrate these results with the
13 other two TWG recommendations. After you listened
14 this morning, it is a very deterministic process with
15 deterministic acceptance criteria.

16 If we are going to do this, it has to be
17 consistent either with the SRM, regulations. We have
18 to look at that way or we have to look at it as our
19 policy issue. Right now we are leaning for short-term
20 is to be consistent with current regulation and
21 consistent with the other TWG recommendations.

22 In other words, we would be, like 174, it
23 is complementary. We would provide complementary
24 insight. But we wouldn't -- we'll get further into
25 this as far risk-informing defense-in-depth goes. I'd

NEAL R. GROSS

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

1 like to avoid that.

2 Now for project deliverables, for Problem
3 Statement 1, which was back -- issue interim guidance
4 and address use of current methods, modeling of
5 digital systems, and again, for COLs and/or design
6 certification.

7 In the longer term, we would intend to
8 update regulatory guidance as needed. And that is
9 SRP, Reg Guides, and NUREG best practices, things like
10 that. But we thought we need to pull those off into
11 long term. It is not going to be a short-term
12 resolution.

13 One thing I should mention, too, on this,
14 and we did have a discussion last week on it, as the
15 papers from industry, as to how those would be
16 reviewed. To do a short-term project, we were looking
17 at using that information and incorporating it in what
18 we are doing. If it ends up being a formal review
19 like a topical report or something like that, that can
20 impact scheduling. So we are discussing how we want
21 to handle that.

22 MEMBER MAYNARD: Cliff?

23 MR. DOUTT: Sure.

24 MEMBER MAYNARD: Just briefly for me on
25 interim guidance versus a long-term change in the

NEAL R. GROSS

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

1 standard review plans, my understanding that somebody
2 comes in with a COL application that they are tied to
3 the SRP or whatever that was in place six months
4 prior, how does the interim guidance play into this if
5 we don't -- if we put as a longer-term item as
6 updating the standard review plans and the reg guides,
7 what are they bound to when they come in with a new
8 COL application?

9 MR. ARNDT: Let me.

10 MR. DOUTT: Okay.

11 MR. ARNDT: They are bound to the
12 regulations and guidance six months ahead of time,
13 just like what -- what's the reg guide, I can't
14 remember off the top of my head, that provides that
15 guidance?

16 MR. DOUTT: 1.206.

17 MR. ARNDT: 1.206, thank you. This
18 interim guidance is going to be specifically -- and
19 this is true for most of the TWG actions regardless of
20 area is going to provide clarification, additional
21 information, and that kind of things.

22 There are specific rules on what we can do
23 without doing a formal regulatory guide update or a
24 formal SRP update. The idea here is to provide that
25 additional information as to what we really mean, what

NEAL R. GROSS

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

1 the acceptance criteria really means, what the level
2 of detail -- the word we are using is added clarity
3 associated with this.

4 In Problem Statement 1, if you recall, the
5 statement was we want to -- there is a concern that
6 there is not enough clarity in the guidance associated
7 with digital systems in terms of the design cert. in
8 COL PRAs. So that is a specific regulatory decision.
9 Accept the results of those PRAs.

10 And what we are trying to do is provide
11 additional clarity in the guidance that is out there,
12 which is very general, as you know, as to what is good
13 enough to make that particular regulatory finding that
14 we are comfortable with that.

15 MR. ROTA: This is Rick Rota from
16 Research.

17 That is correct, Steve, but they are not
18 bound to the SRPs and reg guides that are in place.
19 But they need to explain how they meet them or why
20 they don't meet them. So they would, you know, if we
21 have guidance and they say we will meet this guidance,
22 then obviously we found that as acceptable approach.

23 MR. DOUTT: And the goal in the sort term
24 is to be consistent with current guidance and
25 regulations. We are not foreseeing that that would be

1 a change. In the long term, though, on a
2 comprehensive look at this, that may, in fact, be
3 required.

4 MR. ARNDT: And the reason we carry a
5 long-term outcome of the short-term goals is we want
6 the guidance to be as clear and concise and usable as
7 possible. But the process of putting it into a reg
8 guide or an SRP update is a two- or three-year
9 process.

10 MEMBER MAYNARD: And I don't want to
11 belabor it but it seems to me like we are kind of
12 heading down a path where we are going to end up with
13 is this really clarification? Or is this new
14 requirements and everything? I can see a lot of that
15 coming down the pike with this approach.

16 MR. ARNDT: We understand that. And that
17 is also a concern of our industry colleagues. But we
18 also have a concern that we don't get ourselves into
19 a box where we do something for expedience that we
20 later have to do redo. So we don't want to go down
21 that path either.

22 MR. DOUTT: For Problem Statement 2, this
23 has the catch phrase in it -- it is to develop, if
24 possible, an acceptable approach using risk insights
25 and licensing reviews of digital systems, including

1 consideration of proposed industry methods. If we
2 agree on that, then if an acceptable approach can be
3 established, we will issue the interim guidance and
4 acceptance criteria for use of risk insights in
5 licensing reviews of digital systems.

6 And, again, we have a longer term task
7 there. I don't know if I need to -- one thing we have
8 acceptance criteria here which is somewhat
9 inconsistent with Reg Guide 174, which would be
10 acceptance guidelines. In other places in it we have
11 said acceptance guidelines. We had to do the problem
12 statement as stated. So I think there is some
13 clarification there.

14 The reason we say if possible is in the
15 short term, in risk informing, I think we were pretty
16 leery that we could actually pull that off. Risk
17 insights might be valuable. I think they would be --
18 personal opinion.

19 That this would provide some additional
20 clarification or help as far as doing a risk insight
21 from a -- if you did the defense-in-depth diversity
22 analysis and came up with how much do I need or
23 whatever, this might provide some insight as to how
24 well you did.

25 Or, in fact, provide indication where you

NEAL R. GROSS

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

1 need to do more or maybe less actually. You never
2 know.

3 But that is the idea here. And we are
4 just -- on the short term here, we're a little bit
5 leery of the success.

6 MR. ARNDT: I'm sorry. And this really
7 goes to the point that you were making earlier,
8 George. There are probably some insights -- and we
9 use the term insights so it is not risk informed
10 because that is a very specific process, in terms of
11 failure modes, in terms of what is important and what
12 is not important, in terms of what we can learn from
13 the analysis either qualitatively or quantitatively.

14 And this is certainly something that the
15 industry wants us to do. And they have got their
16 ideas, which is why including consideration of
17 proposed industry methods is in the problem statement,
18 that's something we are going to work to in the short
19 term.

20 As you heard, there are other
21 disagreements associated with what the best modeling
22 approach is. So this is specifically written in such
23 a way that it is comprehensive but doesn't pin anyone
24 down. We want to be able to use the insights that can
25 be gathered but we're just not sure how we are going

NEAL R. GROSS

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

1 to do it and how much we can do in a relatively short
2 time period.

3 CHAIR APOSTOLAKIS: And we will have some
4 Subcommittee meetings on these things?

5 MR. ARNDT: We will have supplemental
6 discussions on this.

7 CHAIR APOSTOLAKIS: The other thing, of
8 course, that is different here from the traditional
9 hardware analysis is that if you find any problems
10 most likely people will fix them.

11 MR. DOUTT: Yes.

12 CHAIR APOSTOLAKIS: Whereas if you say,
13 you know, a pump may fail in the future, you can't
14 really fix that. I mean there is a failure rate.
15 Because the problems here tend to be specification
16 errors or some other design-type error, typically you
17 go back and fix it.

18 Now if the fix though is very expensive
19 and you believe that the circumstances or the context
20 that will lead to this kind of behavior is extremely
21 unlikely, you may tolerate that. But it is a very
22 different approach here.

23 MR. ARNDT: It is. And there is, as you
24 know, a lot of different work in the software
25 reliability community, if you will excuse 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 terminology, associated with both identification of
2 latent failures and the likelihood that you haven't
3 identified latent failures. And the likelihood that
4 they will occur. And there are a lot of things like
5 that.

6 What Alex was mentioning earlier, there
7 are other approaches associated with how you design
8 your software and how you design your digital system
9 to mitigate the consequence of design faults and
10 things like that. And that is something we have to
11 work out with industry. We have some things we agree
12 with and some things we are not yet agreed to on.

13 CHAIR APOSTOLAKIS: Are you talking about
14 a year from now to have answers to these things?

15 MR. ARNDT: We haven't put a date on it.
16 Part of the issue is how important this effort is
17 compared to D3, compared to cyber and things like
18 that.

19 We would like this to be a relatively
20 short-term activity. But the same resources, to some
21 extent, that is going to be used in D3 or cyber or
22 something else also impacts these resources both
23 internally and in the industry.

24 CHAIR APOSTOLAKIS: But the first bullet
25 certainly would effect any decisions on diversity,

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 wouldn't it though?

2 MR. DOUTT: Right. I mean --

3 MR. ARNDT: It could, yes.

4 MR. DOUTT: -- one of the things here is
5 that we have to work in concert. And if we come up
6 with some insights or methodologies, there is an issue
7 here of -- if there is -- that is a 1.0 type deal over
8 there.

9 You run through your defense-in-depth and
10 you come up and you don't have it added. We would
11 come up with -- you could come up with the perspective
12 that you added it, how did you do? Maybe that wasn't
13 the most benefit or the least.

14 But again, from an acceptance guideline
15 point of view, we are stuck with -- you know we don't
16 know whether we can say well how does that relate to
17 implementing the change or not. Or how does that work
18 in current guidance for D3. That are the concerns
19 that we have to try to fit that -- it has got to be a
20 complementary-type -- well, as short term, I think it
21 is complementary.

22 We have to look at it from like a 174
23 approach and apply principle to an idea. But --

24 CHAIR APOSTOLAKIS: 1.174?

25 MR. DOUTT: Well, from a standpoint of --

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: That's some issues.

2 MR. DOUTT: Well, we can't do it that way.
3 What I'm saying is from a -- it has to be
4 complementary to defense-in-depth, okay?
5 Complementary to defense-in-depth.

6 DR. GUARRO: George, this is Sergio. Can
7 you hear me?

8 CHAIR APOSTOLAKIS: Yes.

9 DR. GUARRO: One way in which, I think, a
10 risk-informed approach can be useful in the area of
11 software licensing is in evaluating the level of
12 testing that software and the type of testing a
13 software may have to undergo for different types of
14 scenarios and functions for which it is used because
15 as we have learned, often the failure of software is
16 conditional upon the mode in which it is called to
17 perform.

18 And so knowing in what type of likelihood
19 scenario a certain function is performed is important
20 to determine how to handle the software function from
21 a risk perspective itself.

22 CHAIR APOSTOLAKIS: Yes, that could be.

23 MR. DOUTT: Back it up from the system
24 back to the development, yes.

25 MR. ARNDT: And that, as Sergio has

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 pointed out, that has been used in other industries as
2 a criteria associated with how do you really -- how
3 much testing is necessary, what kind of testing is
4 necessary, what your acceptance criteria for release
5 of the software for practical applications and things
6 like that.

7 So there are a lot of aspects of this that
8 we might be able to use to improve the other
9 deterministic analysis.

10 CHAIR APOSTOLAKIS: Good.

11 MR. ARNDT: That's really where we are
12 trying to go from the staff's standpoint. The
13 industry has got a couple of very specific decision
14 criteria they want us to use this in but the problem
15 statement is more general than that.

16 MR. DOUTT: And just a very general idea
17 on approach. For the short term, we are trying to --
18 obviously guidance is the SRM to SECY 93-087 and the
19 four points and the discussion here this morning, stay
20 consistent with policy statements on PRA, encouraging
21 the incorporation of it.

22 Commission safety goals, the thoughts are
23 right now is to try to stay with current methodologies
24 in the short term.

25 And the review process is -- I'm not clear

1 on the review process and I don't think we are for
2 sure. It could be a 174-type look and risk informed.
3 We think that is probably tough on an insight point of
4 view in trying to implement in digital.

5 We also have non-risk-informed
6 applications and how we want to deal with that if they
7 came in and had risk insights, but not risk-informed.

8 Let's see, I've got some other issues
9 here. One of the things is in acceptance guidelines,
10 which isn't here, how we would do that. Whether it is
11 a delta CDF and it is, of course, LERF, is it, as in
12 the SRM, which is Part 100, and so we have to look at
13 how we want to do acceptance criteria here, too.

14 CHAIR APOSTOLAKIS: Again, I think the
15 function classification that we have discussed in the
16 past would be extremely useful here because fault
17 trees event risk probably could be useful in
18 situations where you just have to actuate something.

19 MR. DOUTT: Right.

20 CHAIR APOSTOLAKIS: If you have continuous
21 feedback, that's a time-dependent problem, is it not?
22 I mean you can't really force it to a fault tree kind
23 of thing.

24 MR. DOUTT: Yes, we just --

25 CHAIR APOSTOLAKIS: So I think this

1 classification is really needed because it is the
2 background to everything else.

3 MR. ARNDT: We will talk about that very
4 briefly in the next presentation.

5 CHAIR APOSTOLAKIS: Good, good. Non-risk-
6 informed applications -- non-risk-informed --

7 MR. ARNDT: Well, there is a --

8 CHAIR APOSTOLAKIS: Everything is non-
9 risk-informed.

10 (Laughter.)

11 MR. DOUTT: Well, I put that there simply
12 because if an effort was risk informing this but in
13 licensing actions you have a choice. And whether we
14 would incorporate this and how we would do that, that
15 puts it in a little different perspective in how we
16 would -- and whether we would or not review it.

17 And it really is -- if it comes in on risk
18 perspective or risk insight, and we come up with that
19 guidance, it isn't really in that category.

20 This is just quick on what we looked at
21 from applications so far of PRA to digital systems.
22 And this is reactor space. And operating reactors, to
23 my knowledge anyway, to date risk insights have not
24 been incorporated into a digital I&C submittal for
25 upgrade or whatever by either staff or industry.

NEAL R. GROSS

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

1 Some questions have been asked about
2 whether it would be useful or not but we haven't
3 actually seen it.

4 In new reactors, a brief look is that some
5 have included digital systems, essentially software
6 common cause failure, and/or performed uncertainly,
7 importance, or sensitivity studies to look at digital
8 systems and essential to evaluate the software.

9 So what we have seen so far is mostly
10 uncertainty, sensitivity-type work, not a strict
11 modeling of the system. You will find software,
12 you'll find a common cause failure, but the software
13 failure rates are not well document and well defined.
14 Nor is the modeling tending -- you know, sometimes it
15 is there. And in other cases, it is not. The
16 software is ignored. And it is just the hardware.

17 There are other options, too. It is the
18 hardware/software combined. If you knew the system
19 had been working for a long time and you had the
20 monitor, you have some operating history, you can
21 combine that and assume that approach. Whether it is
22 acceptable or not is unknown but that is the way it
23 has been done.

24 The other part of his is strictly going
25 out and looking at what other people are doing. We

NEAL R. GROSS

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

1 haven't -- we need to do that and try and incorporate
2 this into the short term. Some research tasks are
3 working on this. We can pull some of that from there.
4 We need to look at some other industries. As you
5 mentioned, there are other papers available and we
6 have pulled some of those to see if we can get a
7 little different perspective on this.

8 MR. ARNDT: As Cliff mentioned earlier in
9 the presentation, and you may not have caught it
10 because he went through it fairly quickly. On both
11 the shorter term actions, what we are planning on
12 doing is basically three parallel paths. We are going
13 to look at what the industry provides us as input to
14 the interim guidance. And they have told us they are
15 going to provide those and they have given us some
16 flavor of what those are going to look like.

17 We are going to look at what we have done
18 in terms of past experience and review of the AP 1000
19 and other limited but significant experience we have
20 had looking at these kinds of issues.

21 And the third path is where we stand on
22 the research at the point where we are starting to put
23 together the interim guidance.

24 So as you know, we have been working in
25 research and have come up with some ideas and some

NEAL R. GROSS

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

1 guidance and some preliminary results both in terms of
2 traditional modeling and dynamic modeling. So we're
3 going to try to meld all three of those -- what is
4 going on in the industry, what we've done, and what
5 we've looked at in the research, which includes other
6 areas.

7 MR. DOUTT: Okay. And this generally
8 first bullet, general insight, and the strength, I
9 guess, of it. In uncertainty, sensitivity, and
10 importance studies have been used and essentially
11 reduce the impact on uncertainties associated with
12 digital systems and really software failure
13 probability.

14 And in doing this, how you might impact
15 the PRA conclusions or insight when implementing the
16 digital I&C systems. In fact, if some of these
17 failure modes would change your conclusions. That's
18 mostly obviously in new reactor design certification
19 work. That's a general, if not obvious, look at it.

20 There is a corollary to that though. It
21 may, in fact, show that it didn't have an impact. Or
22 this is not relatively insensitive in some cases.

23 What we have seen so far is basically a
24 standard fault tree/event tree method. The level of
25 detail in some cases is to the board level on failures

NEAL R. GROSS

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

1 identified to the board level.

2 Hardware failures were derived from
3 proprietary general databases. There are numbers for
4 that.

5 The common cause failure of hardware was
6 there in boards and boards across systems. Software
7 common cause failure, I mean it may have been
8 considered in modules and across multiple modules, but
9 what that really meant was and what the software
10 failure probability was was pretty consistent through
11 there and not well defined as to what that basis might
12 be. So that is why the sensitivity studies were done
13 is to give an idea of what the impact might be on
14 software.

15 And that is where we are currently as far
16 as general ideas go.

17 And we made up a list of what we think are
18 challenges. What was pointed out last week, I think
19 a kind of reasonable comment was is that this is very
20 similar to an analog problem set, I think, except that
21 when you add software to this, it becomes much more
22 complex. And I don't know if the list is any order of
23 priority but I put software reliability at the top.

24 If we are doing short term, we've got to
25 deal with that somehow. And, again, how are we going

NEAL R. GROSS

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

1 to treat the common cause failure for that?

2 One issue is hardware/software
3 interactions and dependency, if there is anything in
4 that area that we need to consider. Again, we've got
5 the modeling issues as to how well we need to do this.

6 I put failure modes in there and we added
7 it as included unknown or unforeseen failure modes and
8 that -- but the general method right now is to take a
9 look at the failures, what you think they are, in
10 deterministic and design basis and run those.

11 We may not know exactly what all those
12 failure modes are. And some of the failures that have
13 been pointed out, in fact, weren't what was expected.
14 Failure data, we don't really have that. That is
15 research work going on.

16 And any human reliability issues, a couple
17 things. One is we won't really treat this but how
18 you are looking in the software side it from updates
19 and changes and things like that, whether we need to
20 be concerned. And like obviously the interfaces,
21 whether they will have the information available when
22 this failure occurs. And what the manual actions are
23 and how we are going to treat those.

24 And then the big question is we think we
25 do conventional. And interfacing a digital system

NEAL R. GROSS

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

1 with PRA might be simpler.

2 The other concern is diagnostics and fault
3 tolerance and coverage and how we might want to handle
4 that. There is a desire to credit that in a PRA. And
5 we will need to come up with a method or see how we
6 want to handle that in short-term space.

7 That's the first list. There is another
8 list here.

9 CHAIR APOSTOLAKIS: But I mean it seems to
10 be now a given that we are taking the systems-centered
11 point of view, right? Everything is system-oriented
12 here which is good.

13 MR. ARNDT: Yes, how you actually define
14 the models for the particular analysis methodology you
15 want to use for the particular system you want to use
16 may have the more --

17 CHAIR APOSTOLAKIS: Very good.

18 MR. ARNDT: -- software centric or
19 hardware centric. But from a conceptual standpoint,
20 it's --

21 MR. DOUTT: One of the things we did look
22 at briefly is architecture and how that may impact
23 some conclusions. And there could be some differences
24 -- well, there are differences depending on how you
25 did it.

1 In this one, I just did a low probability
2 but credible event to point out in the deterministic,
3 the SRM essentially made that conclusion by making it
4 beyond design basis. But it also concludes that if
5 you don't have something, while you said it could be
6 non-safety and/or it can meet Part 100, but you still
7 have to have something. You have to have some means.

8 In a PRA, there is a little different
9 perspective on that. So we might want to -- how we
10 want to be consistent with that approach.

11 Time dependency is in there just simply as
12 you mentioned before, how we might want to handle in
13 a fault tree/event tree space if we've got issues with
14 time.

15 One thing that hasn't been talked about
16 much is external events. And I just put fire in
17 parenthesis. Digital systems and susceptibility to
18 externals, whether that is different than analog and
19 whether we need to consider it.

20 Again, the review process, that is a broad
21 -- whether it is a Reg Guide 174, some other way, a
22 simplified method, we need to look at -- we have some
23 variety of ways to look at this. Along with that,
24 then what acceptance guidelines would be acceptable.
25 Also PRA quality here -- you know, it's going to come

NEAL R. GROSS

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

1 in here somewhere.

2 It may not in the short term. We might --
3 he have to consider that in the long-term. It is
4 definitely is there.

5 CHAIR APOSTOLAKIS: PRA quality from what
6 perspective?

7 MR. DOUTT: Well, from this point of view
8 and on a license amendment, is the PRA adequate for
9 the request? If I'm going to implement a digital
10 system and I'm doing risk insights here, in fact is
11 this adequate to make those conclusions? And we have
12 to come up with some guideline for that.

13 There may be policy issues here, too, in
14 the sort term. That is where we try to avoid that.
15 But in the long term, there might be trying to blend
16 this with a deterministic process, and risk-informing,
17 if you will, defense-in-depth. We're trying to avoid
18 that.

19 CHAIR APOSTOLAKIS: Is that how we do it
20 now?

21 MR. DOUTT: No, it is not how we do it
22 now.

23 CHAIR APOSTOLAKIS: Isn't 1.174
24 implementing this?

25 MR. DOUTT: When you -- in 1.174, there

NEAL R. GROSS

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

1 are a couple of issues in there with defense-in-depth.
2 One is it is deterministic and listed as, you know,
3 there is another part in there that says you can also
4 use the PRA to provide insights on your defense-in-
5 depth. However, you don't want it to be circular,
6 okay.

7 And that the uncertainty, you know, one of
8 -- now, I don't want to say I have to put in a diverse
9 system. It is a one based on deterministic. I come
10 back and say well, but defense-in-depth is -- I don't
11 want to -- that was what was limiting my uncertainty
12 in software was that defense-in-depth. I don't know
13 if I want to have a screening criteria that would
14 remove it.

15 So I want it to be a complement to that
16 defense-in-depth diversity analysis right now. Going
17 forward, in the long term, that is something else.

18 CHAIR APOSTOLAKIS: I don't see what 1.174
19 does, I think because you have the defense-in-depth
20 philosophy. Then you have the risk change.

21 MR. DOUTT: Right.

22 CHAIR APOSTOLAKIS: Make sure you don't
23 overdo it.

24 MR. DOUTT: Right. Make sure you keep the
25 two in synch. And that is what we are trying to

NEAL R. GROSS

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

1 maintain.

2 MR. ARNDT: The concern Cliff has is that
3 if you are actually changing the defense-in-depth,
4 then you have a potential issue with 1.174 because 174
5 says you can do a regulatory change so long as the
6 risk criteria is met and you maintain defense-in-depth
7 --

8 CHAIR APOSTOLAKIS: Philosophy.

9 MR. ARNDT: -- philosophy, correct.

10 CHAIR APOSTOLAKIS: So you can effect
11 difference in there. In fact, if you didn't, there
12 would be very, very few applications.

13 MR. DOUTT: But what happens is -- and
14 where are we in this particular case, how much is
15 enough, and where is it in acceptance? So we have to
16 look at that.

17 CHAIR APOSTOLAKIS: Well, it is the same
18 thing in 1.174.

19 MR. DOUTT: Well, that's the other thing.

20 CHAIR APOSTOLAKIS: I don't think this is
21 new. This is the same.

22 MR. DOUTT: Okay. All right.

23 And then that puts us into consistent with
24 current regulations guidance.

25 CHAIR APOSTOLAKIS: Well, improved

NEAL R. GROSS

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

1 guidance. We want to effect the guidance.

2 MR. DOUTT: And the timeline is at this
3 point relative simple. We need to determine that.
4 Part of that is we provided the project plan to
5 essentially public industry. We need those comments
6 back as far as prioritization of what they think and
7 what resolution and aggressive target dates are
8 needed.

9 There are also going to be comments
10 obviously on the problem statements and we will have
11 to work on that.

12 So we have not determined that yet. But
13 short term, as Steve said, is a relative term. And,
14 again, long term is update regulatory guidance, SRPs,
15 reg guides, and/or whatever else it looks like. But
16 that should be a long-term task.

17 CHAIR APOSTOLAKIS: It is critical that
18 industry include priorities for resolution and the
19 dates?

20 MR. DOUTT: It depends on --

21 CHAIR APOSTOLAKIS: The dates will come
22 from the industry?

23 MR. ARNDT: No, they will give us the
24 priorities.

25 MR. DOUTT: The requested dates.

NEAL R. GROSS

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

1 MR. ARNDT: The requested dates and
2 priorities. This goes back to the issue we had this
3 morning. There are some things -- if you go out to
4 the transcript of the November 8th Commission meeting
5 where the industry came in and said we need to
6 finalize our designs so that we can do certain things
7 like order simulators and things like that, what we
8 specifically asked in our cover letter to the public
9 was if there is some date that is driving your
10 requirement, like we want to order simulators by such
11 and so a date or we need this so we can resolve a
12 particular technical issue so we can do our design, if
13 there is some date that is driving that, then that
14 will drive our prioritization to some extent.

15 So when we say that, the requested target
16 dates for completion is basically input to us saying
17 we want to have guidance in this or some other area by
18 such and so a date so that they can take a particular
19 action. And that will not necessarily be the date in
20 the final problem plan but we will certainly consider
21 that as part of our internal prioritization.

22 Clear?

23 CHAIR APOSTOLAKIS: Yes, I would take that
24 comma out from --

25 (Laughter.)

1 CHAIR APOSTOLAKIS: It's confusing.

2 MR. ARNDT: We can do that. That can be
3 done.

4 CHAIR APOSTOLAKIS: Okay.

5 MR. DOUTT: Some sort of conclusions as we
6 just talked about.

7 CHAIR APOSTOLAKIS: Good.

8 Any questions?

9 (No response.)

10 CHAIR APOSTOLAKIS: Very good. Thank you,
11 gentlemen.

12 MR. ARNDT: Thank you.

13 CHAIR APOSTOLAKIS: Although I guess Steve
14 will stay up there.

15 Review of current status of dynamic
16 digital reliability modeling research, so you are
17 going to tell us why dynamic reliability modeling is
18 important?

19 MR. ARNDT: That's part of what we are
20 going to do.

21 For those of you who are not familiar,
22 this is Professor Tunc Aldemir from Ohio State
23 University who is one of our researchers in this area.

24 CHAIR APOSTOLAKIS: So this is now a
25 color? Is that what it is? Yes? Okay.

NEAL R. GROSS

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

1 MR. ARNDT: So what I'm going to talk
2 about today is a quick background. And I want to do
3 that because -- and it is going to be three or four
4 slides -- I want to put this in perspective. The
5 discussion by the industry this afternoon focused in
6 on this particular project.

7 And although it is certainly one of the
8 areas that we are looking at and we think shows a lot
9 of promise and we have gained a lot of useful insights
10 on it, it is not the only thing we're doing in terms
11 of long-term research. So I want to put it in
12 perspective.

13 And then we're going to talk a little bit
14 about what we have done since the last time we came
15 and talked to the Committee, particularly issues
16 associated with the revision and update of the draft
17 document that you looked at last summer. And then a
18 couple of quick slides on the methodology and where we
19 are on that.

20 One of the big issues that was found in
21 the comments that we got -- and I'll talk about that
22 more in a minute -- was there is a lot of issues
23 associated with practicality. And we want to talk a
24 little bit about --

25 CHAIR APOSTOLAKIS: As you know --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. ARNDT: -- how we are trying to
2 resolve those.

3 CHAIR APOSTOLAKIS: -- especially Tunc
4 knows very well, this issue of dynamic PRA, not just
5 in the context of digital I&C has been around now for
6 10 years, 15 years?

7 MR. ALDEMIR: More than that.

8 CHAIR APOSTOLAKIS: More than 15 years.
9 There were several groups that were involved from
10 Maryland, from other places, American cities has
11 worked from this, there have been workshops and so on,
12 and the problem -- not the problem -- I mean the issue
13 has always been really what NEI raised this morning or
14 this afternoon. Where is the smoking gun? Where is
15 the convincing argument that says you must go this
16 way? And that the existing methods that are based on
17 event trees and fault trees are inadequate in some
18 sense?

19 And I must say I haven't heard that
20 argument yet in the context of the broader PRA. There
21 have been also effort from Italy and so on --

22 MR. ALDEMIR: Belgium.

23 CHAIR APOSTOLAKIS: What?

24 MR. ALDEMIR: Belgium.

25 CHAIR APOSTOLAKIS: Belgium -- and

NEAL R. GROSS

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

1 although people were enthusiastic in the workshops and
2 all this needs to be done, it is very exciting work,
3 by the way, modeling and so on. But that has been the
4 problem so far. That nobody doing work of consequence
5 in the sense of decision-making and so on has seen a
6 reason to go into this, which is considerably more
7 complex than the existing methods.

8 So I guess NEI repeated this argument
9 earlier today regarding this particular application
10 and it seems to me --

11 MR. ARNDT: And I will try and address
12 that in a very, very, very short --

13 CHAIR APOSTOLAKIS: Pascal-ful state.

14 MR. ARNDT: Hopefully.

15 (Laughter.)

16 MR. ARNDT: Because the -- well, both in
17 terms of how we are focusing our research, which, I
18 think, is somewhat misunderstood, and what the
19 objectives of it is.

20 CHAIR APOSTOLAKIS: I just wanted to make
21 it clear to people who are not from the PRA community
22 --

23 MR. ARNDT: Sure.

24 CHAIR APOSTOLAKIS: -- that this is not
25 new. And the argument that we heard against it is 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 new either.

2 MR. ARNDT: Right.

3 CHAIR APOSTOLAKIS: Okay? Not being new
4 doesn't mean it is not valid.

5 MR. ARNDT: Right.

6 A couple quick things, the Office of
7 Research has a program for evaluating and developing
8 models needed to support risk-informed regulation.
9 This is something that we have been doing for about
10 three years now. It's not something that we started
11 doing just because of the task working group. We have
12 been doing this for a while trying to develop these.

13 The phraseology is specifically chosen.
14 If we find something that we like, we don't have to
15 develop something new. But we do want to understand
16 what is out there, evaluate its capabilities and
17 limitations, and look at how you can develop new
18 things or relax the limitations that we find.

19 As you know, the NAS study recommended
20 looking at this from a systems-centric standpoint and
21 looking at hardware and software modeling, either as
22 explicit hardware/software and then the interactions
23 or the way we are doing it, the dynamic way, as a
24 system-state-system type analysis. And we'll talk
25 about that in a second.

NEAL R. GROSS

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

1 So what we are doing is looking at these
2 things. And for near-term applications -- and when I
3 say near terms here, I mean the next ten years, not
4 next year -- one of the other boundary conditions is
5 that whatever structure we come up with, no matter how
6 complicated, needs to eventually fit back into the
7 broader plant PRA because that is what the acceptance
8 criteria is written again.

9 So what we are doing is research to
10 understand what can be done with traditional methods.
11 Basically that's part of the research is looking at
12 how far can we move what we currently know in terms of
13 modeling digital systems and capturing the unique
14 aspects of digital systems.

15 And then from the other side, in parallel,
16 we are looking at what advanced methods can bring to
17 the table. How much do you need to do? Where is it
18 going to give you advantages and more power associated
19 with that? And then how do you link it back to the
20 event trees?

21 So --

22 CHAIR APOSTOLAKIS: Sergio, are you still
23 on the line?

24 DR. GUARRO: Yes, I am.

25 CHAIR APOSTOLAKIS: Maybe for this part,

1 you should not participate.

2 DR. GUARRO: I'm not participating.

3 (Laughter.)

4 CHAIR APOSTOLAKIS: Let's make sure.

5 DR. GUARRO: If you want, I can cut off
6 completely.

7 CHAIR APOSTOLAKIS: Sorry? What did you
8 say?

9 DR. GUARRO: I said if you want, I can
10 disconnect.

11 CHAIR APOSTOLAKIS: No, no, you can stay
12 on line if you will but please don't participate in
13 this part.

14 DR. GUARRO: I haven't made a sound have
15 I?

16 (Laughter.)

17 CHAIR APOSTOLAKIS: Okay. Thank you.

18 DR. GUARRO: Okay.

19 MR. ARNDT: Okay. So the objective of the
20 program is basically to identify or develop methods
21 for regulatory guidance, et cetera, needed to support
22 the problem statements that we just talked about.

23 The real quick overview of what we are
24 doing, we've got a set of different tasks that have
25 been assigned to different groups within the office.

NEAL R. GROSS

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

1 I'll go through this quickly. The overall program
2 coordination is with my group.

3 CHAIR APOSTOLAKIS: You group is --

4 MR. ARNDT: DEFERR.

5 CHAIR APOSTOLAKIS: DEFERR?

6 MR. ARNDT: DEFERR, Division of Fuels
7 Engineering and Radiological Research.

8 CHAIR APOSTOLAKIS: That's where they are
9 digitalizing the logs?

10 MR. ARNDT: The engineering part is where
11 I&C is.

12 CHAIR APOSTOLAKIS: So it is DEFERR?

13 MR. ARNDT: Yes. And then the development
14 of the regulatory guidance is also in our shop. And
15 the interface with the Steering Committee.

16 The investigation or refinement of
17 traditional modeling methods with traditional failure
18 modes and effects analysis is with DRASP, the other
19 division. The investigation and development of
20 methods in dynamic models is with us.

21 And then development of the two benchmark
22 cases that we will talk about -- one of the things we
23 are trying to do is gain additional insights into the
24 methods by actually trying them out on a couple of
25 actual systems. And we will talk about those more.

NEAL R. GROSS

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

1 But the first system is a system that is
2 more likely to have dynamic interactions but has a
3 potentially lower safety significance. The second
4 system is one that is less likely to have dynamic
5 interactions but has potentially more safety
6 significance. So we are trying to choose a couple of
7 example systems that will cover as much of the
8 territory as possible.

9 MR. KEMPER: Steve, this is Bill Kemper.
10 If I could just interject. Now that last bullet, we
11 intend to benchmark -- use a benchmark to test both
12 methodologies?

13 MR. ARNDT: Correct.

14 MR. KEMPER: The traditional methods using
15 event tree/fault tree as well as the dynamic methods?

16 MR. ARNDT: Yes.

17 MR. KEMPER: Okay. So basically we're
18 trying to validate both processes in parallel here.
19 And see which one best suits the application?

20 MR. ARNDT: And that really gets back to
21 the point that you mentioned earlier associated with
22 understanding what systems need to be modeled at what
23 level based on a set of characterizations.

24 CHAIR APOSTOLAKIS: I really think we need
25 that, Steve. We need to see something along these

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 lines.

2 MR. ARNDT: Okay. And we've started down
3 that path looking at a three-axis model which is very,
4 very preliminary at this point, looking at system
5 complexity, system interaction, and system importance.
6 Those are the orthogonal axis right now.

7 It is very preliminary at this point. If
8 you'd like to discuss it offline or we can come and
9 talk to you specifically about it.

10 CHAIR APOSTOLAKIS: I think we should
11 discuss it. I know that it was even a problem within
12 the group that put together the National Academy
13 report.

14 MR. ARNDT: Yes.

15 CHAIR APOSTOLAKIS: There were strong
16 disagreements within the group.

17 MR. ARNDT: Yes, it is a difficult issue.

18 CHAIR APOSTOLAKIS: Because, you know,
19 somebody comes in with a failure that occurred in RER,
20 a very complex feedback and control system, and says
21 oh, you have to worry about it when you talk about
22 describing the reactor. I mean it is not the same
23 thing.

24 MR. ARNDT: Right. Yes.

25 CHAIR APOSTOLAKIS: It's just not.

1 MR. ARNDT: Right. And there are
2 different issues --

3 CHAIR APOSTOLAKIS: We need that.

4 MR. ARNDT: -- associated with it.

5 CHAIR APOSTOLAKIS: Yes, exactly.

6 MR. ARNDT: And right now that is the
7 approach we are looking at. We haven't vetted it with
8 a lot of people yet. But we can come back and talk to
9 you more about it.

10 So let me drop out of the general model
11 now and talk about the specific dynamic model. We are
12 going to have a longer presentation after I get done
13 on the traditional modeling methods. And where we are
14 going from that.

15 But the point here is these are parallel
16 efforts. We are trying to learn as much as we can
17 about both. And the principle idea is on the dynamic
18 modeling methods, learn how powerful and how useful
19 these can be under particular circumstances. And on
20 the traditional side, look at how far can you push the
21 traditional models before you run into issues. So it
22 is looking at it from both sides.

23 CHAIR APOSTOLAKIS: Is there any reason
24 why you have color copies here with green characters
25 and blue background?

1 MR. ARNDT: The ones we provided this
2 morning were all black and white.

3 MEMBER KRESS: To see if you are color
4 blind.

5 CHAIR APOSTOLAKIS: That was your idea,
6 too? Using the boilerplate?

7 (Laughter.)

8 CHAIR APOSTOLAKIS: Okay.

9 MR. ARNDT: Okay. So the basic structure
10 is to investigate the capabilities and limitations.
11 This is the 6901 that was talked about earlier. There
12 is obviously some concern about that particular
13 document although we thought it was a pretty good
14 review of the models capabilities and limitations.

15 Look at what potential modeling methods
16 would be the most practical for implementation in that
17 we specifically looked at models that have had some
18 level of implementation previous to this, which is why
19 we came down on a Markov and a DFM modeling
20 methodology, review past experience, review existing
21 regulatory framework associated with the unique
22 aspects of the digital system that need to be modeled,
23 identify requirements -- and when I say requirements,
24 I don't mean that in a regulatory sense, I mean that
25 in a modeling capability sense, identify 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 methodologies, and then demonstrate the methodologies
2 with the benchmarks.

3 Again, we're using two benchmarks. We
4 will talk about the results of the first benchmark.
5 That was a feedwater control system. The second
6 benchmark is going to be a reactor trip system.

7 Current status, we've talked about this
8 three times already. We put out 6901 which basically
9 reviewed the methods. We identified two benchmark
10 systems. We've looked at an example initiating event
11 for integration of the dynamic models into the
12 traditional fault tree/event tree.

13 That is one of the biggest challenges
14 associated with non-event tree/fault tree-type models.
15 How do you integrate them into this structure. Tunc
16 will talk about that a little bit in a few slides.
17 But we have identified a methodology that we think
18 works well.

19 We have compiled this into a draft NUREG
20 that is specifically designed to be a proof of
21 concept. The title is there and it is in final review
22 right now.

23 CHAIR APOSTOLAKIS: What is DFWCS?

24 MR. ALDEMIR: Digital Feedwater Control
25 System.

1 CHAIR APOSTOLAKIS: Sorry.

2 MR. ARNDT: And then what we are doing is
3 publishing a third document which will have the actual
4 quantification, basically the numbers. One of the
5 concerns that we got in the review of that document
6 was well, where is the beef? What is the final
7 numbers? And what does it tell you?

8 The point here is just to demonstrate that
9 this kind of modeling methodology can be made
10 practical. But certainly we would like to demonstrate
11 that the quantification can be done. So we are going
12 to have another document that will have the specific
13 points.

14 CHAIR APOSTOLAKIS: Well, I guess there
15 are two steps here. The first is do we get anything
16 very useful that we cannot get with the traditional
17 methods --

18 MR. ARNDT: Right.

19 CHAIR APOSTOLAKIS: -- which is the heart
20 of the argument against this. And then second, can we
21 make this practical.

22 MR. ARNDT: Right. And that is something
23 you really have to do almost in parallel because you
24 learn -- I mean theoretically there are a lot of
25 things you could possibly learn from using these kinds

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 of things. Identify new failure modes, identify new
2 interactions that are dynamically based, identify new
3 issues that might be there.

4 But the issue really is are you really
5 going to see any of those in the practical
6 implementation? Is there enough data? How do you
7 parse the data? How do you aggregate the data? Is it
8 going to be too computationally-intense to ever get
9 any real insights?

10 So there is some synergism there. But
11 yes, those are the questions that we need to answer.
12 And we'll talk a little bit about that. Not in any
13 great detail.

14 Because this has been a somewhat
15 controversial issue, as you well know, we have had
16 probably more peer review of this document than we
17 have of a research document in a long time. We have
18 had extensive internal reviews, including the comments
19 you provided us last year. We've had internal reviews
20 from the Research PRA group, the Research I&C group,
21 the NRR PRA group, the NRR I&C group.

22 We have had external peer reviews from
23 academia, from the labs, and from the industry. We
24 had approximately 180 different succinct comments
25 grouped in a number of different areas including

NEAL R. GROSS

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

1 regulatory issues, issues on the benchmark system both
2 in terms of its applicability and the exact details,
3 issues about data collection and generation. How do
4 you feed the monster? Issues about the dynamic
5 methodologies and their practicality. And issues
6 associated with integration with the fault tree/event
7 tree.

8 CHAIR APOSTOLAKIS: Are we going to see
9 this before publication? Or this is it?

10 MR. ARNDT: It is in final publication
11 now.

12 We prepared a comment resolution document
13 that will be published in parallel with this which
14 will basically have all 180 comments --

15 CHAIR APOSTOLAKIS: Yes, I'd like to see
16 that.

17 MR. ARNDT: -- without attribution.

18 CHAIR APOSTOLAKIS: Without it?

19 MR. ARNDT: Well, what we've decided to
20 protect the guilty is the reviewers will be listed but
21 they will not be -- each individual comment will not
22 be tied to an individual reviewer.

23 CHAIR APOSTOLAKIS: Can you give us some
24 names?

25 MR. ARNDT: Internally, Nathan, and people

1 like that. Externally, do you remember the academics?

2 MR. ALDEMIR: Enrico Zio.

3 CHAIR APOSTOLAKIS: Did you pay them?

4 MR. ALDEMIR: No.

5 MR. ARNDT: Curtis Smith.

6 MR. ALDEMIR: Curtis Smith.

7 CHAIR APOSTOLAKIS: Industry, who was from
8 the industry?

9 MR. ARNDT: Mr. Stone who was just
10 speaking.

11 PARTICIPANT: Bob Enzinna.

12 MR. ARNDT: Thank you. Bob Enzinna. Our
13 friend from EDF, Tweat who has done a lot of the EPRI
14 work in this area.

15 CHAIR APOSTOLAKIS: Oh, the gentleman who
16 was here at the last meeting?

17 MR. ARNDT: Yes.

18 MR. ALDEMIR: Also from Norway --

19 MR. ARNDT: Oh, Altusa.

20 MR. ALDEMIR: Altusa Tunam.

21 MR. ARNDT: She's the lead software
22 engineer at Halden. So pretty broad spectrum of both
23 practitioners and theoreticians and others.

24 CHAIR APOSTOLAKIS: Was there anybody who
25 was positive?

NEAL R. GROSS

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

1 MR. ARNDT: Oh, yes. There were a lot of
2 positive comments. There were a lot of negative
3 comments, too.

4 CHAIR APOSTOLAKIS: I knew that.

5 MR. ARNDT: So it was --

6 MR. ALDEMIR: But even from the industry
7 we had a few positive comments. Well, in different
8 sections of it.

9 CHAIR APOSTOLAKIS: Good, good.

10 MR. ARNDT: So we will talk about a couple
11 of the things that we did here in a second.

12 Just to give you a broad brush associated
13 with it, it was not a super simple system. It was a
14 real practical system. It was the digital feedwater
15 control system. It had a high power mode and a lower
16 power mode, a backup computer, and a main computer.
17 And had different controllers.

18 We looked at the input devices. We looked
19 at the output actuation devices. So it was not a
20 trivial academic-type system.

21 MR. ALDEMIR: If I may say one word here.

22 CHAIR APOSTOLAKIS: What is this business
23 trivial academic?

24 (Laughter.)

25 MR. ALDEMIR: One of the -- last time we

NEAL R. GROSS

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

1 were presenting a similar presentation here, there was
2 a whole bunch of equations on the screen. And --

3 CHAIR APOSTOLAKIS: And now it is clear.

4 (Laughter.)

5 MR. ALDEMIR: And, of course, a concern is
6 how are we going to do it? What kind of expertise is
7 needed to do that? That is one of the reasons why we
8 developed the Simulink Model which, I think, is easier
9 to generate from a process diagram because it looks
10 pretty much like the process diagram as we incur it
11 rather than dealing with a bunch of equations.

12 So the point I'm trying to make is that
13 this is in response to the comments we received in
14 terms of practicality.

15 CHAIR APOSTOLAKIS: You developed a
16 simulation?

17 MR. ARNDT: Yes.

18 MR. ALDEMIR: Yes. A Simulink Model which
19 you can interface with much more easily generically.
20 Eventually we would like to come up with a shell that
21 you plug in your own module. So rather than having
22 the equations which are going to be user-unfriendly,
23 we thought it would be a better idea to develop a
24 Simulink Model which is much more well known.

25 And so if we designed the interface for 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 Simulink interface, then it is easier on the part of
2 the user if they wish to use it in the future to link
3 up with it. That was our intention.

4 CHAIR APOSTOLAKIS: Clever idea. Clever
5 idea.

6 MR. ARNDT: And the other point here is
7 some of the comments we received basically was you
8 really have to do a lot of work to do this. And in
9 the NUREG, the original version of the NUREG, it had
10 all the system equations and things like that.

11 And the point is you only need system
12 equations or system simulation to the extent that the
13 system is interfacing with the system. If it is a
14 simple trip function, then this part is much simpler.
15 It is a set of and/or type else systems.

16 CHAIR APOSTOLAKIS: Well, wouldn't the
17 plant simulators --

18 MR. ARNDT: The plant --

19 CHAIR APOSTOLAKIS: -- simulate already a
20 lot of these things?

21 MR. ARNDT: Yes, it could if you linked it
22 with the PRA model. What you need to track the
23 interactions is some mechanism, as you step through
24 the time frame, to look at the interactions between
25 whatever system you are modeling and the plant process

NEAL R. GROSS

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

1 as a whole.

2 In our case, since it was a feedwater
3 control system, we were looking at steam generator
4 level, steam generator pressure, temperature, pump
5 flow, and things like that. In the case of an RPS, it
6 would be the trip functions, whether or not the system
7 had actually tripped or not, maybe --

8 CHAIR APOSTOLAKIS: Otto, wouldn't these
9 things exist already?

10 MEMBER MAYNARD: You have to be a little
11 careful with the simulator. As far as using a
12 simulator for this, a simulator is designed to give
13 you the same indications and views that you get in a
14 plant but the programming may not be totally identical
15 to every step that is going on in there.

16 And so you have to be careful. It really
17 would depend on how the simulator computer system
18 software was all put together and what it was
19 simulating and stuff. But you do have to be careful
20 in using the simulator for things such as this. It
21 can be but not necessarily in all cases can it be.

22 CHAIR APOSTOLAKIS: This is the feedwater
23 system control?

24 MR. ARNDT: This is the controller, yes.

25 CHAIR APOSTOLAKIS: Oh, the controller.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. ARNDT: There are equivalent type of
2 things for the process input variables that we needed.

3 MR. ALDEMIR: This is pretty much directly
4 from the process diagram. This does not have the full
5 system dynamics in it. It doesn't have, for example,
6 what we call the steam generator module that is going
7 to be an additional input into this system.

8 That normally would have come -- this and
9 the level change combined would have come from the
10 plant simulator. But in our case, these are two
11 separate modules. So it will feed -- because we had
12 to test this module first with a simpler process model
13 so that if there are problems, we can identify the
14 problems rather than testing the whole complex thing
15 in one shot.

16 MR. ARNDT: And this, like I say, this
17 gets back to the issue we brought up earlier.
18 Depending upon the functional classification, how much
19 information you need to make the right decision, this
20 might be this complicated or it might be much simpler
21 depending upon the system.

22 The point here is we are modeling it to
23 the level of detail that we think is necessary to
24 capture the unique aspects of the digital system.

25 CHAIR APOSTOLAKIS: So if I were to do

1 then a complete PRA and I have things like high
2 pressure injection, low pressure injection,
3 recirculation, would I develop something like this for
4 each of these systems? Or for the reactor as a whole
5 with all the safety functions?

6 MR. ARNDT: You would develop a reactor
7 model.

8 CHAIR APOSTOLAKIS: A reactor model?

9 MR. ARNDT: A model of the plant system,
10 the plant process. And then --

11 CHAIR APOSTOLAKIS: Which is already in
12 the simulator, right? I mean that --

13 MR. ARNDT: Again, that may not be exactly
14 the case.

15 MEMBER MAYNARD: To give you some examples
16 of the simulator, let's take the reactor protection
17 system. You don't have a complete reactor protection
18 system sitting there with your simulator. You will
19 have that programmed into the software. But it is not
20 identical to necessarily what is -- all the signals
21 and the various things you'd be getting.

22 Again, the main idea is to get the same
23 inputs, the same displays in the control rooms, and
24 get the components, to, you know, get the reactor trip
25 at the same point. But it is not going through the

NEAL R. GROSS

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

1 same logic, the same controllers, the same types of
2 things that you would have going on inside the power
3 plant or a reactor protection system.

4 CHAIR APOSTOLAKIS: Which you will have to
5 do here though.

6 MR. ARNDT: For those systems that you
7 want to model in detail, the issue would be you would
8 make a determination, however you wanted to do it, as
9 to what level of modeling detail you needed for each
10 system --

11 CHAIR APOSTOLAKIS: Okay.

12 MR. ARNDT: -- like this. And then as you
13 step through the initiating event --

14 CHAIR APOSTOLAKIS: I would say, Steve,
15 that this helps with the question of practicality.

16 MR. ARNDT: Yes.

17 CHAIR APOSTOLAKIS: But it does not help
18 with answering the question why do I have to do this.

19 MR. ARNDT: Okay.

20 CHAIR APOSTOLAKIS: Is that correct?

21 MR. ARNDT: That's correct. That is
22 exactly correct.

23 CHAIR APOSTOLAKIS: So if you decide that
24 you need to do it, then developing these simulators
25 makes it practical because now an average user can do

NEAL R. GROSS

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

1 it.

2 MR. ARNDT: Right.

3 CHAIR APOSTOLAKIS: But why go through the
4 effort to do this remains unanswered? Or you have
5 arguments for it?

6 MR. ARNDT: We have arguments for it.
7 There is, obviously, some debate as to whether or not
8 they are convincing or not.

9 CHAIR APOSTOLAKIS: Okay.

10 MR. ALDEMIR: One comment about the plant
11 simulator. It doesn't have to be faithful to the
12 operation of the control system. You can use it also
13 by activating or deactivating the appropriate
14 components simply to see as a model of the process
15 evolution level change, for example.

16 And so -- and that it doesn't matter
17 whether it is faithful to the actual operation or
18 system or not as long as it has the proper level
19 dynamics so to speak.

20 MR. ARNDT: Okay. I'm going to skip
21 through these next few things rather quickly. One of
22 the issues is, of course, you've got to do the model
23 testing. And the model has to be correct.

24 One of the comments we got was associated
25 with the benchmark system and the accuracy of that and

NEAL R. GROSS

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

1 the dynamics of the valve closing and things like
2 that. I mean we have gone back in and proved that.

3 The actual issue associated with how you
4 model in -- this is a Markov model but in DFM or
5 Markov, the various interconnections --

6 MR. ALDEMIR: No, no, this is a state
7 diagram.

8 MR. ARNDT: Oh, I'm sorry. This is a
9 state diagram. Right. You need to understand the
10 states of the system. And this is rather complex and
11 it is -- the point that you need to understand how the
12 system might fail.

13 So in this particular case, we've got a
14 state diagram which looks at state transitions. It
15 doesn't care whether it is a hardware failure or a
16 software failure. We're not modeling hardware and
17 software separately. We're modeling hardware and
18 software in its hardware/software interactions in an
19 integral way.

20 What we do care about is states in the
21 system that would lead to unique failure modes. And,
22 again, this is a matter of determining what level of
23 modeling detail you need. So, for example, there is
24 operations with two computers, the backup and the
25 main-running, operating with one computer with

NEAL R. GROSS

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

1 recovery, operating one computer without recovery, and
2 various other kinds of characterizations.

3 The point here is you model it to a level
4 of detail necessary to capture the unique features of
5 the digital system. I've said that about four times
6 in the last five minutes. The point here is -- it
7 gets to your question of do you need these or not --
8 the issue is if you don't know whether or not a
9 particular unique feature of the digital system will
10 give you a different answer, then you should start as
11 a default with modeling all the unique features that
12 you have.

13 It is very difficult to arbitrarily say
14 these things can be modeled by an on/off switch in an
15 undeveloped basic event if you don't look at the
16 system interactions associated with them. And, again,
17 this is a look at the controllers associated with it.
18 And the communications and issues like that.

19 Why don't I let you do this one, Tunc?

20 MR. ALDEMIR: Well, one of the problems
21 was, of course, everybody knows Markov models, and by
22 the way, when we say Markov models, it is not just
23 Markov models. I distinctly say Markov model but the
24 state transition diagram which is common to both DFM
25 and Markov models and everybody knows that state

NEAL R. GROSS

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

1 models lead to computational complexity but as Steve
2 said, you don't know. You have to do it the best you
3 can. And then decide whether you need that detail or
4 not.

5 So here we are trying to capture
6 everything within the system. And as you see at least
7 to a hundred million states, which is, of course,
8 impractical. Now on the other hand, it is a well-
9 known technique to conglomerate components into super
10 components as long as they don't have individual
11 external interactions. And we use that --

12 CHAIR APOSTOLAKIS: Excuse me, 100 million
13 states --

14 MR. ALDEMIR: States.

15 CHAIR APOSTOLAKIS: -- of what? What
16 system?

17 MR. ALDEMIR: That includes hardware and
18 software in the sense that, for example, we have an
19 arbitrary output failure mode for the computers. That
20 is a software thing. On the other hand, you have
21 power --

22 CHAIR APOSTOLAKIS: These are states of
23 the system?

24 MR. ALDEMIR: States of the system, yes.

25 CHAIR APOSTOLAKIS: So they 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 combinations?

2 MR. ALDEMIR: Yes, yes, yes.

3 CHAIR APOSTOLAKIS: And each parameter or
4 whatever is modeled in a multi-state way?

5 MR. ALDEMIR: Yes.

6 CHAIR APOSTOLAKIS: How many states? Or
7 it is not standard?

8 MR. ALDEMIR: Five pairs -- I cannot
9 recall offhand. The first item lists the hardware
10 components we are considering. And each has about
11 five, six different failure modes. But that is what
12 is leading to 100 million.

13 CHAIR APOSTOLAKIS: That's all I need to
14 know.

15 MR. ALDEMIR: So after we do this
16 conglomeration and census, for example, are regarded
17 part of the computers and there was one argument, one
18 comment it against that. They said well, why are you
19 doing that? You may be needing the information
20 someplace else. If you do, you don't. If you don't
21 join them into the same component.

22 For example, we are both regarding the
23 backup and the main computer as computers because they
24 are identical. We are also using arguments like
25 systems operational whether there is one or two

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 computers so I don't have to have separate states for
2 each computer.

3 Incidentally, we are not trying to be, as
4 I said in the meeting last week, in the public
5 meeting, we are not trying to be system-specific
6 clever here which is a difficult thing to do and which
7 would require engineering judgment. These are well-
8 known techniques in state conglomeration or state
9 reduction techniques. And used for all sorts of
10 different systems.

11 CHAIR APOSTOLAKIS: So the best you could
12 do is 2,200?

13 MR. ALDEMIR: That is very reasonable.

14 CHAIR APOSTOLAKIS: You could do it by
15 hand, I suppose.

16 (Laughter.)

17 MR. ALDEMIR: By the way, French have been
18 doing part of their control systems using Markov
19 models about 15 years ago using 10,000 by 10,000
20 states -- I mean matrix.

21 CHAIR APOSTOLAKIS: Okay.

22 MR. ALDEMIR: We have done two million by
23 two million.

24 CHAIR APOSTOLAKIS: You don't need to.

25 MR. ARNDT: Okay. We are running a little

NEAL R. GROSS

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

1 behind so I'm going to try and step through the rest
2 of this fairly quickly.

3 So the extent of the analysis of the
4 failure scenarios of the benchmark system looks at all
5 the different failure paths. And that's, to some
6 extent, the point. We want to look at all the
7 different system interactions and different system
8 failure paths to look at what interactions we might
9 have.

10 And one of the comments was the need to do
11 a comparison of the DFM and the Markov modeling
12 methods. And we have added that from a qualitative
13 standpoint to look at issue associated with the
14 branches and determinations and things.

15 CHAIR APOSTOLAKIS: Now you said
16 qualitative. You did not quantify anything here.

17 MR. ARNDT: No. We have not quantified in
18 this document. We are going to do quantification in
19 the next document.

20 CHAIR APOSTOLAKIS: But can one look at
21 the results of this exercise here and provide failure
22 modes and argue that these you could not have found
23 using traditional methods?

24 MR. ARNDT: Yes.

25 CHAIR APOSTOLAKIS: Do you have any

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 examples of those?

2 MR. ARNDT: Do you know one off the top of
3 your head?

4 MR. ALDEMIR: Well --

5 CHAIR APOSTOLAKIS: These are the answers
6 to the argument.

7 MR. ALDEMIR: The problem is the
8 following, as you well know, and this was brought up
9 in 1992 workshop. If you know the answer, you can
10 justify using other techniques to arrive at the same
11 answer.

12 CHAIR APOSTOLAKIS: But still, it would be
13 nice to have a few examples.

14 MR. ALDEMIR: Well, yes, well, I mean, we
15 haven't -- as I said, the easiest way to do it is to
16 have an independent group using traditional methods
17 and another group doing dynamic methods. Then compare
18 and see what they have found.

19 And that is the route actually NRC has
20 chosen. So far we haven't had any comparison -- any
21 basis for comparison with static methods yet.

22 CHAIR APOSTOLAKIS: Well, I'm not really
23 asking for a formal comparison. But I mean if I look
24 at your Slide 15, for example, where you have
25 scenarios, a few of those and say look with the

NEAL R. GROSS

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

1 traditional fault tree, chances are you would not have
2 found this.

3 MR. ALDEMIR: I showed you one last time,
4 which is basically depending on when the valve fails,
5 you can either have high level or low level or high
6 level -- failure by high level or bi-level whose
7 consequences are quite different when you do the PRA,
8 overall PRA.

9 CHAIR APOSTOLAKIS: But that is the kind
10 of thing I'd like to see.

11 MR. ARNDT: Okay.

12 MR. ALDEMIR: We had --

13 CHAIR APOSTOLAKIS: I remember from the
14 last time.

15 MR. ARNDT: I'm sorry. We will provide
16 that to you. The point is that is a somewhat subject
17 evaluation.

18 CHAIR APOSTOLAKIS: Absolutely. No
19 question about it. But at least you put something on
20 the table for discussion.

21 MR. ARNDT: Okay.

22 CHAIR APOSTOLAKIS: Because I believe the
23 criticism of today plus, as you know already 15 years
24 or so, has to be addressed. Why do I have to go
25 through this? And if you put a few examples on the

NEAL R. GROSS

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

1 table and start the debate, I know it is a lot of --
2 I mean the reactor safety study had the same reaction.
3 Oh, a good engineer could have found this.

4 MR. ARNDT: Right.

5 MR. ALDEMIR: That is the argument. That
6 is the argument. But, you know, we are coming from
7 the premise that there has been enough experience in
8 the past to show that dynamic methods will discover
9 failure modes that traditional methods cannot. The
10 question that is relevant to this community is it
11 necessary for PRAs -- for power plant PRAs?

12 CHAIR APOSTOLAKIS: Absolutely, yes.

13 MR. ALDEMIR: Now the problem is this.
14 Let's say that for argument's sake, we have shown that
15 we have compared traditional methods against dynamic
16 methods and shown that for all the reactors operating
17 in the world today, everything can be handled very
18 nicely by traditional methods. Okay, let's assume
19 that this is the finding.

20 Does it mean that somebody is not going to
21 come up with a reactor design ten years down the line
22 that will be quite different? So our task -- we are
23 working for the regulator -- our task is to come up
24 with a general methodology that can be used as a
25 basis. But the need will need to be regulated.

NEAL R. GROSS

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

1 MR. ARNDT: Okay.

2 CHAIR APOSTOLAKIS: It was a subtle hint.

3 (Laughter.)

4 CHAIR APOSTOLAKIS: I think even if the
5 ultimate conclusion -- even if the ultimate conclusion
6 is that the existing methods are pretty good or good
7 enough, having gone through this --

8 MR. ARNDT: Yes.

9 CHAIR APOSTOLAKIS: -- will have increased
10 our confidence --

11 MR. ARNDT: That's right.

12 CHAIR APOSTOLAKIS: -- in those methods.
13 I have no problem with that.

14 MR. ALDEMIR: That's exactly right.

15 MR. ARNDT: As I articulated and I won't
16 belabor it too much, that is the point. The point is
17 to understand where the limits are for the particular
18 examples, the cases that we care about.

19 MR. ALDEMIR: We would like to have a
20 defensible methodology basically.

21 CHAIR APOSTOLAKIS: Okay. We all do,
22 Tunc.

23 MR. ARNDT: In the DFM space, dynamic flow
24 graph methodology for those of you who aren't --

25 CHAIR APOSTOLAKIS: Was it applied, too?

NEAL R. GROSS

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

1 MR. ARNDT: Yes.

2 MR. ALDEMIR: Sure.

3 MR. ARNDT: We have applied it, we have
4 looked at it in the inductive mode. We have done some
5 qualitative comparisons of the scenarios. We updated
6 a steam generator simulator package associated with
7 it.

8 One of the nice things about DFM, of
9 course, is it can be used in the deductive mode as
10 well which is particularly useful for investigating
11 failure modes. And looking at these issues associated
12 with is the failure modes and effects analysis really
13 getting you all the information?

14 CHAIR APOSTOLAKIS: Deductive, you mean if
15 the level -- how can the level be such and such?

16 MR. ARNDT: Right.

17 CHAIR APOSTOLAKIS: Then work backwards.

18 MR. ARNDT: Exactly. Then work backwards.

19 CHAIR APOSTOLAKIS: The fault tree.

20 MR. ARNDT: Right. And because DFM
21 integrates the process as well as the failures into a
22 single analysis, it is particularly useful for these
23 kinds of systems.

24 CHAIR APOSTOLAKIS: So you would have
25 examples also from DFM at some point?

1 MR. ALDEMIR: This is already, I think, in
2 the document. We did the comparison. We did the
3 resolution upon your suggestion last time.

4 MR. ARNDT: So --

5 CHAIR APOSTOLAKIS: Well, I can't wait to
6 get that document.

7 (Laughter.)

8 CHAIR APOSTOLAKIS: Is it coming out soon?

9 MR. ARNDT: As soon as I can force it
10 through the process.

11 CHAIR APOSTOLAKIS: You try to avoid dates
12 today desperately. You never give me a date.

13 MR. KEMPER: It will be soon.

14 MR. ARNDT: It will be soon.

15 CHAIR APOSTOLAKIS: Thank you, Bill.

16 MR. ARNDT: That helps a lot. So like I
17 said, you can track through the different process in
18 an inductive or deductive manner to support particular
19 failure scenarios.

20 CHAIR APOSTOLAKIS: Okay.

21 MR. ARNDT: The exact comparison because
22 the --

23 CHAIR APOSTOLAKIS: Those of you who are
24 wondering why I asked Dr. Guarro to be quiet he is the
25 father of this DFM methodology. So he can't really

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 review his own work.

2 MEMBER KRESS: Has he ever done that?

3 CHAIR APOSTOLAKIS: Has he ever reviewed
4 his own work? Yes.

5 (Laughter.)

6 MR. ARNDT: So to date we think we have
7 demonstrated that these approaches can be dealt with
8 in a practical way and they can demonstrate a lot of
9 the different unique aspects associated with it.

10 Now how practical it is and how much of
11 this in terms of uncertainty analysis, unique failure
12 modes, applicability to other systems is still open.
13 And that is why we are going to complete the research.

14 One of the issues -- and I'll step through
15 this rather quickly because I'm running over time --
16 is the issue of as you get more and more different
17 failure modes and different states, you have to get
18 the state transitions and things like that.

19 There is a lot of different ways you can
20 do that with data, with certain expert elicitation and
21 judgment. But one of the ways you can do it is
22 through testing, both traditional testing and specific
23 testing to look at how the system transitions from
24 state to state.

25 One of those techniques is the fault

1 injection testing. You can look at it from a software
2 standpoint, from a hardware standpoint. The concept
3 is not that dissimilar to stress testing or
4 accelerated testing for a piece of hardware. You
5 stress test the hardware/software system by putting in
6 faults in the system and seeing how it executes or how
7 the fault protective systems keep that from becoming
8 a failure.

9 So you develop a set of fault injection
10 space that looks at the type faults, the location of
11 faults, the timing and injection, the duration, and,
12 most importantly, the system's context, which in
13 software space is referred to as the operational
14 profile to understand how these systems would fail and
15 what they would fail.

16 And that allows us to develop a fault
17 coverage parameter which is similar but not exactly
18 the same as testing coverage or something like that
19 that allows you to look at how you partition a failure
20 space.

21 So the process basically is you construct
22 a fault list. You find the failure rate of the device
23 in whatever operational modes you are interested in.
24 You do a fault injection experiment. You look at the
25 response of the system. And you look at the coverage

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 parameters associated with each of the failure modes.

2 You look at the non-coverage parameter.
3 That is basically faults that were not caught by the
4 system architecture or the system parameters and
5 basically transitioned through to the end out put of
6 a failure. And since the availability failure rate
7 can be inferred from the non-coverage, you can then
8 come up with transition rates for the particular
9 failure modes that you are interested in.

10 This is not the only way to do this. This
11 is a particularly powerful methodology and it has got
12 a lot of applications. But there are other ways of
13 doing this.

14 You can do it with non-parametric models.
15 You can do it with software reliability models. But
16 this one is particularly nice because you can actually
17 physically go out and test it.

18 You also need, of course, a statistical
19 analysis methodology because you cannot test every
20 possible failure state. So you look at what the
21 statistical coverage estimate is. And based on
22 certain assumptions, you can come up with a number of
23 injections trials you need to do to cover the system
24 at a particular confidence level and a particular
25 failure rate you are interested in.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: See this is now
2 something that can be tested --

3 MR. ARNDT: Yes.

4 CHAIR APOSTOLAKIS: -- by looking again at
5 the operating experience. If I had applied all the
6 injection techniques say to the Palo Verde incident --

7 MR. ARNDT: Right.

8 CHAIR APOSTOLAKIS: -- would it have
9 prevented what happened?

10 MR. ARNDT: Right.

11 CHAIR APOSTOLAKIS: I think it is really
12 a powerful way of saying something about --

13 MR. ARNDT: It is a very potentially
14 powerful technique. And in point of fact when we
15 originally started looking at this, we looked at it as
16 an augmented inspection technique. Basically we have
17 since started using it to help us provide additional
18 data to support the risk stuff.

19 But when we first started looking at this
20 about four years ago, we started looking at it as an
21 augmentation of our inspection and analysis
22 techniques. So we are currently working -- the second
23 benchmark test has dual purpose.

24 We're looking at it as a what can we learn
25 about this particular system we are testing as well as

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 data can we generate to support this particular
2 project? But that is the discussion for another time.

3 And one of the issues is where do we get
4 the data to start with, which helps augment what the
5 partitioning of the data looks like. And we get it
6 from exactly where you would expect to get it. We get
7 it from actual failure data from this particular
8 system. We get it from commercial failure databases
9 like PRISM and Mil Standard and other things like
10 that, which you heard Brookhaven talk about the last
11 time that we were here.

12 CHAIR APOSTOLAKIS: But if you have a
13 multi-state representation of the components and the
14 systems, how would you get rates for state J? That
15 seems to be --

16 MR. ALDEMIR: You inject faults to
17 stimulate state J.

18 MR. ARNDT: The point is you come up with
19 a --

20 MR. ALDEMIR: Some of those states are
21 going to be covered by the system. Some of the --

22 CHAIR APOSTOLAKIS: We just talked about
23 the fault injection.

24 MR. ALDEMIR: Right. But that --

25 MR. ARNDT: In general --

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: Transition rates from
2 one state to another --

3 MR. ARNDT: To another are difficult.
4 There are other --

5 CHAIR APOSTOLAKIS: It's going to be --

6 MR. ALDEMIR: We have to make something
7 clear. What the fault injection tests give us is
8 coverage which can be used either failure per demand
9 or non-coverage which can be used as failure per
10 demand or multiplied by the transition rate which is
11 hard data from databases gives you the transition
12 rate, whichever model you wish to choose.

13 If you use Markov, you change transition
14 rate --

15 CHAIR APOSTOLAKIS: I hope we're going to
16 have Subcommittee meetings before you finalize any of
17 that.

18 MR. ARNDT: Yes, oh yes.

19 CHAIR APOSTOLAKIS: Okay.

20 MR. ARNDT: We will have lots of meetings.

21 CHAIR APOSTOLAKIS: My biggest objection -
22 - well, not objection, my biggest concern with any of
23 these methods when it comes to numbers is these rates.
24 Where are they coming from? What do they mean? Why
25 are they constant?

NEAL R. GROSS

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

1 MR. ARNDT: Right. Or if they are
2 changing, what is the change? And this method is not
3 wed to a Markovian assumption. You could use semi-
4 Markovian models and things like that.

5 CHAIR APOSTOLAKIS: Today I see the
6 discussion more along the lines of the failure modes.

7 MR. ARNDT: Right.

8 CHAIR APOSTOLAKIS: But not the
9 quantification. So I'm not going to raise any --

10 MR. ARNDT: Okay. When we do the
11 quantification report in a couple of months, we can
12 come back and talk to you in more detail about this
13 particular issue.

14 CHAIR APOSTOLAKIS: Before anything is
15 final I hope.

16 MR. ARNDT: Yes.

17 CHAIR APOSTOLAKIS: Okay.

18 MR. ARNDT: This is basically just a slide
19 and I'm going to skip through it quickly. There is a
20 mechanism that Tunc has developed for integrated DFM
21 and Markov into a event tree for a traditional fault.

22 CHAIR APOSTOLAKIS: So again, what would
23 be the events and the states?

24 MR. ALDEMIR: It is simply --

25 CHAIR APOSTOLAKIS: Are you going to write

NEAL R. GROSS

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

1 a paper on this?

2 MR. ARNDT: Yes.

3 MR. ALDEMIR: Yes. When I get a chance
4 to.

5 MR. ARNDT: We've got a couple of
6 conference articles on this. And we are working on a
7 couple of journal articles on it.

8 MR. ALDEMIR: There are three journal
9 articles that are in preparation but it is just a
10 matter of timing.

11 CHAIR APOSTOLAKIS: With the blessings of
12 Steve?

13 MR. ALDEMIR: Yes but they have been very
14 nice. I mean it doesn't take for them to bless it but
15 for us to put it together is time consuming.

16 CHAIR APOSTOLAKIS: Yes.

17 MR. ALDEMIR: Remember each of these has
18 about six to seven authors so coordinating the authors
19 is not that easy either.

20 MR. ARNDT: In any case, there is a
21 methodology that has been developed. And we are using
22 SAFIRE, not because we think SAFIRE is better than the
23 other methods, it is because we can get access to the
24 source code.

25 CHAIR APOSTOLAKIS: Right.

NEAL R. GROSS

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

1 MR. ARNDT: So let me sum up and then turn
2 it over to my colleagues to talk about the traditional
3 modeling methods.

4 CHAIR APOSTOLAKIS: Well, we have a break
5 in between.

6 MR. ARNDT: Yes, I think you have a break
7 after this.

8 CHAIR APOSTOLAKIS: Yes.

9 MR. ARNDT: So we have developed this
10 methodology. We have submitted to extensive peer
11 review. We resolved as many of the comments as
12 possible. We will have a comment resolution.

13 The first benchmark has been developed.
14 And tested for steady state as well as transient
15 conditions. The results have been compared and we
16 have resolved the initiating events.

17 We are starting to do the preliminary
18 analysis with the data. And that will be available in
19 a few months. And we will come back and talk to you
20 about them.

21 So we believe that this is a -- I should
22 really watch my terminology -- conceptually proof of
23 concept, we are there. In terms of practicality, in
24 terms of effort associated with it compared to the
25 cost benefit that Alex was mentioning, it is obviously

NEAL R. GROSS

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

1 something that we need to look at.

2 And how much we need versus how much level
3 of detail versus the particular regulatory decision we
4 are making is something we are going to have to work
5 out. And let me go back to that for a second -- well,
6 let me finish the last slide.

7 So we are going to do the next benchmark.
8 We are going to do the quantification. We are also
9 going to develop the stand-alone model so we don't
10 have to integrate fully to get some failure mode
11 information and things like that.

12 We are in the process now of putting
13 together the second benchmark and specifying it and
14 all that kind of good things. Some of our engineers
15 and our contractors' engineers are actually at the
16 training on the new system this week. And then when
17 we get that up and running, we'll do the benchmark --
18 the second benchmark problem which, again, is the RPS,
19 which has got different characteristics than the
20 feedwater system.

21 And I know there has been a lot of
22 consternation among the community associated with the
23 fact that we did the feedwater system before we did
24 the RPS but that was simply a matter of that is a
25 system we could get. And in a perfect world, I

NEAL R. GROSS

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

1 probably would have done the RPS first and the
2 feedwater system second. But that is the world we
3 live in.

4 Let me take two seconds to go back and
5 talk about this issue associated with the regulatory
6 decision we are trying to make. If you go back to the
7 three problem statements we talked about when Cliff
8 was presenting, the first one was develop additional
9 clarification on what was needed for the Part 52
10 design cert. and COL applications.

11 We have got a regulatory requirement that
12 basically says if you are going to come in under Part
13 52, you have got to present the results of your PRA.
14 So that is a specific regulatory decision we have to
15 make as to what information do we need from the
16 digital system aspects associated with that.

17 Problem Statement 2 basically says if
18 possible, can we use some risk insights to make the
19 decision criteria on things like D3 or communications
20 or cyber or whatever better? That is a particular
21 regulatory decision.

22 Statement 3 -- Problem Statement 3, which
23 says develop a comprehensive methodology that uses the
24 state of the art, regardless of the debate about what
25 the state of the art is, to come up with a risk-

NEAL R. GROSS

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

1 informed decision-making criteria. That is a much
2 higher threshold in terms of decision-making. We are
3 establishing a 174-type process which allows us to
4 generalize risk-informed applications of digital
5 systems.

6 So as I mentioned when Cliff was talking,
7 the research has basically three objectives. It
8 originally had two, now it has three.

9 One, to get smarter about these systems
10 and to understand the methods and maybe come up with
11 an independent assessment tool for us.

12 Two, to take that information that we got
13 smart about and write that generalized all-
14 encompassing document which will probably be a reg
15 guide but it may be some other document.

16 The third one is to take what we have
17 learned to date and try and have input into that
18 second problem statement associated with short-term
19 improvements based on risk insights to the current
20 regulatory process.

21 Our big debate, I think, is the industry
22 thinks that the current methodologies can be pushed
23 further. We're not sure yet. That is really where
24 we are in that space.

25 As you know, the traditional modeling

NEAL R. GROSS

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

1 methods approach is next and I think you want to take
2 a break.

3 CHAIR APOSTOLAKIS: We'll take a break
4 unless there are questions.

5 (No response.)

6 CHAIR APOSTOLAKIS: Okay. Back at five
7 minutes past three.

8 (Whereupon, the foregoing
9 matter went off the record at
10 2:48 p.m. and went back on the
11 record at 3:08 p.m.)

12 CHAIR APOSTOLAKIS: Now we are talking
13 about traditional methods. Okay.

14 MR. KURITZKY: I'm Alan Kuritzky. I'm
15 from the Office of Research. I guess if you hear Mike
16 Mayfield this morning talking about the speakers
17 coming up, he mentioned that I had 25 years experience
18 in PRA. He definitely didn't mention that I had any
19 experience in digital I&C and there was a reason for
20 that since I don't.

21 And that is the reason why from Brookhaven
22 National Lab we have Gerardo Martinez-Guridi and Louis
23 Chu with me here. They are going to handle the tough
24 questions. The presentation I'm going to give was
25 pretty much prepared by them.

NEAL R. GROSS

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

1 You heard earlier today from Steven and
2 also, I guess, at previous meetings about the dynamic
3 modeling methods for digital systems. What I am going
4 to talk to you about right now is our work on the
5 traditional methods for modeling -- reliability
6 modeling of digital systems, the difference basically
7 being that by traditional we are referring to well
8 established, commonly used modeling methods whereas
9 the dynamic is more of the cutting edge, advanced-type
10 methods.

11 The presentation today is going to -- I
12 will give you a quick status of where we stand on our
13 traditional methods research, what our plans are for
14 this project, our objectives and approach, a short
15 review of some of the traditional methods that we have
16 looked at so far under this work. Also, we developed
17 criteria for evaluating the different reliability
18 models using those methods. So we will go over those
19 criteria.

20 We also selected a number of applications
21 or studies using those methods for comparisons against
22 those review criteria. And comparing those models to
23 the review criteria allowed us to identify the
24 limitations and capabilities of the different methods.
25 And essentially it establishes the state of the art

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 for those methods.

2 And finally we will have some concluding
3 statements including which traditional methods we have
4 selected for a further look.

5 Near the end of last summer, there was
6 some concern that the work being done under the
7 traditional methods research was not totally in line
8 with that being done under the overall Office of
9 Research Digital I&C Reliability Modeling Program,
10 including the dynamic work. So we had a project
11 review meeting in October of that year and the outcome
12 of that meeting was that we were going to refocus the
13 traditional methods work specifically on identifying
14 and demonstrating the capabilities and limitations of
15 existing methods as they stand today.

16 We also -- what came out of that meeting
17 was that we would emphasize and increase the amount of
18 stakeholder interactions with the process. And also
19 that the Office of Research should develop an
20 integrated project plan for the overall digital I&C
21 reliability modeling efforts and coordinate their work
22 with the program offices: Office of New Reactors, NRR,
23 NMSS.

24 We have developed the draft innovative
25 plan for that work. It has somewhat been overshadowed

NEAL R. GROSS

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

1 because in the interim, as you heard earlier today,
2 there was a Steering Committee established on the
3 direction of the Commission, the NRC Digital I&C
4 Steering Committee, and we have been working to supply
5 them with a project plan. And that has kind of
6 superceded the plan that we had worked out initially.
7 Ours kind of feeds into that and maybe offers more
8 detail in some areas.

9 The plan we have for the traditional
10 methods research involves essentially five tasks.
11 There is now a task 1a so I guess it is six tasks.
12 But the first task which we are going to describe
13 today -- it is the work we have done so far --
14 involves identifying what traditional methods have the
15 most promise for use in licensing applications. Or
16 for increasing or accounting for digital systems in
17 current plant PRA models.

18 We have a draft letter report prepared by
19 Brookhaven on that task and we are going to describe
20 or discuss many of the aspects of that report in this
21 presentation.

22 We also have added a task 1a which is
23 going to involve an external peer review of the
24 information from that report. The main focuses of
25 that peer review will be on the criteria that were

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 identified and also on the selection of which
2 traditional methods to pursue.

3 We are now currently working on Task 2 in
4 parallel. And Task 2 advances what we came up with in
5 Task 1 to start developing the selected methods and
6 how we will actually apply then to the test cases.
7 The test cases in Tasks 3 and 4 are the same ones that
8 Steven mentioned for the dynamic modeling methods,
9 which is a digital feedwater control system and a
10 reactor protection system.

11 Lastly, we also have a task to integrate
12 the results into a PRA. In terms of methods involving
13 traditional fault trees and event trees, that should
14 be a pretty straightforward integration. To the
15 extent that we use other types of techniques such as
16 Markov, some variant of Markov modeling, there will
17 need to be some type of -- some techniques used in
18 order to smooth that integration.

19 Okay, Task 1, as I just mentioned, the
20 objectives are to develop criteria for evaluating the
21 reliability models and these draft criteria that we
22 have identified could well find themselves in the
23 future as part of regulatory guidance for what is
24 acceptable in terms of, you know, risk-informed
25 decision-making or use of risk insights.

NEAL R. GROSS

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

1 We are going to use these criteria right
2 now under -- well, we have used them under Task 1 to
3 help us determine which methods have the most promise.
4 But the most important aspect, I think, of those
5 criteria are their potential for use as acceptance
6 guidelines or attributes for modeling for later
7 regulatory uses.

8 CHAIR APOSTOLAKIS: Is the Markov model is
9 what the previous speakers also --

10 MR. KURITZKY: Yes.

11 CHAIR APOSTOLAKIS: So why is it the
12 traditional method?

13 MR. KURITZKY: Okay. We are going to get
14 to that actually in a few slides.

15 CHAIR APOSTOLAKIS: All right.

16 MR. KURITZKY: I think Steven talked a
17 little bit about that in his previous talk. But we
18 will try to amplify a little more about the use of
19 Markov modeling techniques in both parts of the
20 project.

21 Okay, the approach that we used for Task
22 1 we used a search of the literature as well as our
23 experience to identify a number of traditional methods
24 to evaluate. Those methods included fault tree and
25 event tree methods. Again, some variant of Markov

NEAL R. GROSS

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

1 modeling techniques, the SINTEF method, which is used
2 by the Norwegian oil industry and is also some type of
3 simplified Markov modeling, reliability prediction
4 methods, and also we looked at in the NASA PRA
5 procedures guide, there is a section on software
6 modeling that provides what seems like a fairly
7 reasonable idea of how to quantify or include software
8 failure probability into a fault tree model under the
9 PRA.

10 In addition, we also had some information
11 on a simplified analytical method that was used for a
12 Japanese ABWR. And so we looked over that also.

13 After identifying the traditional methods
14 to look at, we developed criteria for evaluating the
15 methods or, more particularly, to evaluate the models
16 that were using those methods. The criteria were
17 focused on capturing all the unique or digital system
18 unique features that might effect system reliability.

19 After coming up with the criteria, we
20 identified applications of each of the methods from
21 the first bullet for comparison to the criteria. In
22 doing so, we have identified the capabilities and
23 limitation of those models. And that would establish,
24 like I said before, essentially where the state of the
25 art exists right now.

NEAL R. GROSS

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

1 We are engaging the technical community in
2 this work. We have, as someone mentioned earlier
3 today, there is a web page, a digital I&C web page on
4 the NRC public website. We also, as was mentioned
5 earlier, had a public meeting. Last week, it was the
6 task working group meeting on digital system risk.
7 That was a public meeting.

8 And we received -- well, we didn't receive
9 a lot of feedback at that meeting. Industry has
10 indicated they would try and supply us some feedback
11 on essentially this presentation today, fairly
12 similar, that we could then post on the website and we
13 would have available to us.

14 Also we are planning, as I mentioned
15 before, to have an external peer review panel go over
16 the criteria and the methods that we selected. And
17 that will probably occur sometime in the May/June time
18 frame.

19 The traditional methods that we selected
20 included fault tree/event tree methods, most standard.
21 That is the one that has got wide use across the
22 entire international PRA community. It has been in
23 use for a very long time. It has been used for a
24 whole different host of activities, different
25 industries, aerospace, chemical has used it, of course

NEAL R. GROSS

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

1 it is the standard for the nuclear industry.

2 It is well suited for identifying plant
3 failure modes, accident sequences, and then cut-sets
4 that identify exactly what failures must occur in
5 order to result in an undesirable state at the plant,
6 i.e., core damage. It also is very useful for
7 quantifying the probability of those various states
8 occurring.

9 One limitation of the method is that it
10 only treats timing events and interacts with plant
11 processes in an implicit way. In an implicit and
12 approximate way.

13 And essentially it deals with the timing
14 based on what events are in the event tree, what order
15 they occur, what if there can be some post-processing
16 of cut-sets if there is a particular timing issue that
17 isn't well treated by the event tree structure. And
18 its interactions with plant processes really come
19 about in the systems and success criteria that are
20 used.

21 The issue of the Markov modeling, as Dr.
22 Apostolakis just mentioned, we are using a type of
23 Markov modeling in the dynamic research. The way that
24 we differ in what we are doing here with Markov
25 modeling is we are using it as essentially a way 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 characterizing the digital system hardware failure
2 probability. In the dynamic work, it is being used as
3 a dynamic technique to model the complex interactions
4 of the various parts of the digital system and, most
5 importantly, the interactions of the system with the
6 plant process dynamics. Something we are not
7 addressing when we use Markov modeling in this regard.

8 So the Markov modeling being done for the
9 traditional methods is a much simpler -- it doesn't
10 have quite the scope that is being used in the other
11 effort.

12 Markov modeling has, in fact, been used
13 for modeling nuclear power plant systems, including
14 digital systems, so it is an established and existing
15 technique. It allows, as you have heard from
16 obviously the discussion that Steven and Tunc had
17 before, it allows for explicit modeling of the
18 different states that a system can be in and it
19 accounts for repair of equipment, explicitly treats
20 failures and repair times within the model.

21 One of the drawbacks of it is that with a
22 complex system, you can quickly get a very large
23 number of states. And so dealing with or resolving
24 the model becomes fairly difficult.

25 It also considers interaction with plant

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 processes implicitly in an approximate way. I think
2 what you saw with the other effort is that they are
3 trying to do a more explicit addressing of those plant
4 processes but it can be done in a more simply way
5 just, again, based on what systems and the success
6 rates that are being used in the model.

7 As I mentioned before, the integration
8 with existing plant PRAs is not going to be nearly as
9 straightforward as it would be with a fault tree
10 approach.

11 The SINTEF method, as I mentioned used by
12 the Norwegian oil industry, it is an adaptation of the
13 method that is laid out in IEC Standard 61508. It is
14 a very, I guess, a simplified, even more simplified
15 Markov model. One of the simplifications is that it
16 entreats -- it breaks the system into subparts or
17 subsystems and evaluates each system on its own,
18 assumption that common cause failures will dominate
19 the system unavailability or the subsystem
20 unavailability.

21 It doesn't treat independent failures.
22 And it also doesn't treat cross-combination of
23 failures between subsystems. So those are some
24 limitations for a more complex redundant system that
25 we have in a nuclear plant that could end up being 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 significant drawback.

2 It does, however, explicitly model fault
3 detection. And makes the distinction between safe and
4 dangerous failures.

5 Another seeming drawback of the method is
6 that apparently, at least from what we were able to
7 see, from what we had documented, all the data that
8 was used in the model for failure fractions, for beta
9 factors, most of it was just based on expert judgment.
10 And that limitation on data is something we are going
11 to see showing up in most of our methods here.

12 Reliability prediction methods estimate
13 the failure rate of circuit boards in terms of failure
14 rates of individual components. It can be used for
15 systems where you have series components. Again, for
16 redundant systems, it is not very effective.

17 It is possible to be used as a source of
18 data for some of the more robust modeling methods.
19 Again, we were not able to identify the technical
20 basis for a lot of the values used with those methods.
21 That may be a limitation of our data gathering
22 technique or it just may be that they are just not
23 publicly available and they are not usually obtained.

24 The RPMs also do not address uncertainty
25 as many of the -- well, certainly many of the models

NEAL R. GROSS

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

1 that use the methods that we are discussing did not
2 address uncertainty.

3 The NASA PRA procedures guide software
4 modeling method provide a framework for considering
5 software failures in the PRA but, again, it just
6 focused on the software. The NASA PRA procedures
7 guide does not address specifically digital systems or
8 hardware modeling. And so as a result, we didn't
9 further pursue any applications of the NASA approach.

10 Some general observations from the review
11 of these various methods, the fault tree, event tree,
12 Markov, and SINTEF methods are fairly general. And so
13 we pursued applications or evaluate applications of
14 those methods in the work we did under Task 1. We
15 also had an application of the simplified analytic
16 method used for the ABWR and included that in our work
17 also.

18 As I mentioned, the RPMs, they may be
19 useful as a source of data for some of the other
20 methods but they, themselves, were not really robust
21 enough to deal with the types of systems we see in
22 nuclear plants. And, again, the NASA approach was
23 just for software and we had no application of that
24 approach to review.

25 The next step in our work after

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 identifying which methods to pursue was to identify
2 the set of criteria that we felt would be useful for
3 evaluating digital systems and also might be useful
4 for regulatory guidance later on.

5 Some of the considerations that went to
6 those criteria or the identification of those criteria
7 are the fact that we felt that the modeling should be
8 supported by a systematic analysis of possible failure
9 modes and effects. And this is particularly important
10 with digital systems where there is a lot of unique
11 aspects of the systems and types of failures that are
12 not common to traditional pump-and-valve systems in
13 the PRA.

14 The analysis should also go deep enough to
15 identify and uncover any potential dependencies both
16 within the system or between that system and any other
17 system that is being used at the plant to mitigate any
18 particular scenario.

19 The model should, of course, include
20 software failures or address them in some manner,
21 including common cause failure. Again, dependencies
22 with the system and any other systems at the plant are
23 important to identify. And human errors, both in
24 terms of -- well, I guess in terms of errors
25 introduced in upgrading hardware or software upgrades

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 or human errors that result from inadequate man-
2 machine interfaces, need to be accounted for in some
3 manner.

4 There was some question in the technical
5 community as was discussed previously as to whether
6 the timing issues need to be treated explicitly in
7 these models. Again, traditional event tree/fault
8 tree models are static and do not explicitly treat
9 timing.

10 The work that is being done under the
11 dynamic research that Steven discussed with you just
12 recently does try to deal with those with timing in an
13 explicit manner. And that is one thing that we will
14 have to try and determine based on looking at both
15 parallel paths is how important that explicit modeling
16 of time is to overall system reliability and to the
17 understanding of potential failure modes of the
18 system.

19 Self tests and self-diagnostic-type of
20 features for digital systems should be included and
21 self correction. However, when they are included, you
22 must also consider not only the benefits of such
23 systems but also some of the drawbacks. I think
24 someone mentioned earlier, it may have been Paul, that
25 while there is definitely benefit to having self-

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 diagnostic features with the system, you also need to
2 be concerned that they can introduce actual failures
3 into your system and they can result in failures that
4 would not have occurred if you didn't have that self-
5 diagnostic capability.

6 So it is important to account for those
7 features. But they need to be accounted for both in
8 the positive and potentially negative aspects.

9 Quality data is a big key. Obviously with
10 any type, if you want to quantify the models, you need
11 data of good quality and that is something that right
12 now is somewhat lacking. And by quality data, we mean
13 it should be applicable both in terms of the system
14 application and the system operating environment. The
15 sources of the data should be provided. And they
16 should be well documented, the analysis of the data
17 and the parameter estimations should be well
18 documented.

19 Uncertainty analysis is also something
20 that we need to address. Many of the models that we
21 looked at did not address uncertainty analysis. And
22 by that we want to look at modeling uncertainty in
23 terms of what assumptions were used and the impact of
24 those assumptions as well as identifying what sources
25 of uncertainty exist in the models. And the parameter

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 uncertainty, evaluating and then propagating it
2 through the model.

3 I think we had one model that did, in
4 fact, do a fairly decent job with parameter
5 uncertainty. I think it was the AP 1000, a vendor PRA
6 which propagated uncertainties.

7 And, again, ideally the model should be
8 easily integratable into existing plant PRAs. One of
9 the goals of this work is to have -- to upgrade the
10 PRA models so they can account for digital systems.
11 And so we want to be able to integrate those into
12 existing plant PRA models.

13 What is listed on this slide are the eight
14 categories of criteria that we identified. We
15 identified a total of 48 criteria. They fell into
16 these eight different categories. If you look at
17 these eight categories, they have a remarkable
18 similarity to the challenges that were listed on
19 Cliff's slide when he was discussing Problem Statement
20 2.

21 Again, level of detail of the model, how
22 far down do you go, do you go down to the
23 microprocessor level, do you do it a higher level?
24 Very important, again, as I mentioned before, is a
25 systematic identification of failure modes of the

NEAL R. GROSS

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

1 digital system. You know the unique digital features
2 and aspects of those systems, we need to understand
3 them so we can identify how the system can fail and
4 include it in our models.

5 Software failure is obviously a big issue.
6 The dependencies. Human errors, as we just discussed.
7 Ease of integration. Data. And documentation
8 results. All the same issues we just discussed in the
9 previous slides are the genesis for where we came up
10 with these 48 criteria.

11 Right now in the work done so far we did
12 not give any relative weights to those criteria. We
13 just kind of evaluated each of the models against them
14 just scoring how many criteria they met or didn't
15 meet. We did not assign any type of partial meaning
16 of criteria. It was just pretty much a binary you met
17 it or you didn't meet it -- yes, no. And we didn't
18 give any weights to the different criteria.

19 But if these criteria are to be used in
20 the future for regulatory guidance or other purposes,
21 we will need to revisit that and determine not only do
22 we hope to have feedback that may modify this exact
23 list of criteria but also it may become evident that
24 certain criteria are much more important for modeling
25 or determining what the system unavailability is or

NEAL R. GROSS

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

1 failure probability is as well as which criteria are
2 most important for understanding how the system works
3 and understanding how to model the different features.

4 CHAIR APOSTOLAKIS: Yes, two through five
5 it seems to me are essential.

6 MR. KURITZKY: Yes. Well, right now we
7 believe all of them are essential. But you are right.
8 Two through five are the guts of digital system
9 modeling.

10 Just an example of some of the criteria,
11 this is Criterion 2.2 dealing with -- I think this was
12 -- identification of failure modes. Communication,
13 voting, synchronization, those are specific aspects of
14 digital systems, particularly ones that can lead to
15 dependent failures. So that is an important
16 consideration when putting together a digital
17 reliability model.

18 A couple more examples of criteria. This
19 is from Category 7, which is with the data, 7.1 is a
20 question of whether or not you have actually what I
21 consider plant-specific but application-specific or
22 operating environment-specific data that can be used
23 for the components as opposed to 7.4 which says if you
24 don't have that data, if you are using generic data,
25 is it applicable?

1 And, again, obviously to the extent we can
2 get it, application and operating environment-specific
3 data would be of much better value. Using generic
4 data will lead to, of course, fairly large
5 uncertainties and open up to all kinds of arguments as
6 to whether it is applicable at all.

7 Okay, after we identified the methods and
8 the criteria that we wanted to evaluate the models
9 against, we went and looked for which types of models
10 we could find for these different methods. In the
11 fault tree methods, we identified three models. We
12 have the AP 1000 reactor vendor PRA that was here at
13 the NRC, and the ESBWR reactor vendor PRA.

14 And we also had a plant-specific model for
15 a Westinghouse or a CE 80+ design for the ESFAS of a
16 Korean plant.

17 Again, as I mentioned before, we did have
18 a simplified model of a combined RPS ESFAS for a
19 Japanese ABWR. It was a very simplified version or a
20 simplified analytic model. We took a look at that as
21 well as we had the Markov model of the Tricon platform
22 that was our entry in the Markov arena. And then we
23 also took a look at an example of the SINTEF method.

24 We evaluated all those against the list of
25 the 48 criteria but our evaluation focused just 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 whether those models met those criteria. We did not
2 attempt to evaluate or validate the models for the
3 purpose of which the developers of the models actually
4 used them. So we were not evaluating whether the AP
5 1000 was a good PRA or was the SINTEF application was
6 a good application of the SINTEF method. Just rather
7 whether those applications or those models, how well
8 they met our criteria.

9 Again, as I mentioned, we evaluated each
10 of the models against those criteria. There was
11 obviously a large amount of qualitative judgment and
12 subjective judgment in doing that assignment. This is
13 one of the things that can be looked at as part of the
14 expert review panel although more important is not so
15 much how well the different -- or how we assigned the
16 models to the criteria. It is the actually list of
17 are these the right criteria? And are these the right
18 methods to pursue?

19 The importance of knowing how well we did
20 score the existing models against those criteria is in
21 the fact that it helps us establish what is the
22 current state of the art with these different methods.

23 Now the extent to which those applications
24 that we collectively had for any given method, how
25 well they collectively met those criteria kind of

NEAL R. GROSS

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

1 gives us that basis for where the state of the art
2 stands right now. However, that is based, again, on
3 those limited models that we looked at. So if there
4 are other models out there that have done a better job
5 at any of these particular criteria, then that could
6 be collectively synthesized into future modeling
7 efforts and, therefore, demonstrate that the state of
8 the art is a little bit more advanced.

9 We made a strong effort to try and get
10 some of these more international models of PRAs. To
11 date we have not been too successful. We made contact
12 with a couple of foreign agencies. We discussed some
13 of the topics with them.

14 Generally what we are hearing back is that
15 in past history, they have attempted to model digital
16 systems and after throwing a lot of money at it, grew
17 very frustrated in their inability to do a good job of
18 modeling particularly the software. But we have not
19 yet been able to obtain actual PRA models to see what
20 actually went into their fault trees if they did, in
21 fact, develop them.

22 But, again, we have an open invitation to
23 all stakeholders that any type of information they can
24 provide on other models, we would be happy to look at
25 to see whether or not there are other criteria. As

NEAL R. GROSS

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

1 you can see from the fourth bullet, the most criteria
2 that any single model that we looked at met was 16 out
3 of the 48 criteria. So 21 of the criteria were not
4 addressed by any of the applications. And an initial
5 nine were only addressed by one application.

6 So to the extent that there can be other
7 applications or models that address more of those
8 criteria, we'd love to see it.

9 The fault tree/event tree models, the
10 three fault tree/event tree models satisfied the most
11 number of criteria.

12 MEMBER ABDEL-KHALIK: How much as your
13 familiarity with these models contributed to that last
14 bullet?

15 MR. KURITZKY: Well, I was going to say
16 something. I don't know so much about whether or not
17 our familiarity with those models contributed to that
18 last bullet but they certainly had impact. But the
19 development of the criteria was by people who are most
20 familiar with those models.

21 And in honesty are -- envisioning again
22 one of objectives is to be able to include digital
23 system models in a plant PRA and so there is kind of
24 a pre-bias towards, you know, we are obviously all
25 eager to integrate that into a PRA model if it is 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 fault tree-type thing. So I'm sure there was some
2 bias. I don't want to speak for Brookhaven, who did
3 that work. But there is a potential for bias there.

4 But nonetheless, we tried to keep a pretty
5 open mind as to how well the other methods or the
6 applications of the other methods met the criteria.

7 MR. MARTINEZ-GURIDI: Yes, I mean the
8 potential for the bias exists but I think we tried to
9 be as impartial as possible.

10 MR. KURITZKY: Okay. Some of the --

11 MR. ARNDT: One thing I want to point out
12 before we go on, when we talked about, in the first
13 presentation, the fact that the short-term goals would
14 be influenced by our research to date, the opposite is
15 true as well. The industry has committed to provide
16 us input on some of their techniques.

17 And we are trying to work with EPRI to do
18 more collaborative work with them. So as we learn
19 more from the industry, we are committed to factoring
20 that into our research effort.

21 MR. KURITZKY: Yes. It is a living
22 process.

23 MR. ARNDT: A living process.

24 MR. KURITZKY: Okay. Some of the
25 observations after we applied the various models to

NEAL R. GROSS

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

1 the criteria, main strengths of the applications
2 across the board mostly were that common cause failure
3 of hardware within a system was included. It was
4 typically modeled. However, again, the data for
5 quantifying those contributions was somewhat suspect.

6 Individual and common cause failures of
7 software were explicitly included in the models for
8 most of the studies that we looked at. However, the
9 extent to which they were included and the
10 quantification of those events was, again, something
11 that needs work. There was definitely a lacking.

12 Some of the main limitations across all of
13 the studies, again, as I mentioned before, it is very
14 important to have a systematic evaluation of the
15 possible failure modes based on the very unique
16 features, characteristics, and components of the
17 digital systems. And we did not see that in the
18 majority of the -- or pretty much in all of the
19 studies that we looked at.

20 Again, I need to caveat some of these
21 limitations by the fact that we are basing these
22 comments, these review comments on the information we
23 had available to us. So whether or not there are some
24 proprietary or some other data that the developers of
25 the models used and they did not release or it was not

NEAL R. GROSS

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

1 publicly available or we could not find, may, in fact,
2 ameliorate some of these concerns.

3 But from the information we saw, there
4 appeared to be a lack of systematic evaluation of the
5 unique failure modes and effects for these digital
6 systems.

7 Also in the failure parameter data, there
8 just was not a lot of good quality data for
9 quantifying these models. And what data was used,
10 there was generally lacking any documentation or
11 documented basis for the data.

12 Quantitative software reliability methods,
13 of course lacking across the board. It is obviously
14 a big issue. There are arguments as to how and if you
15 can quantify software reliability or at least a
16 failure probability for use in a PRA. So it is just
17 a big open issue.

18 Treatment of uncertainties, again it was
19 one that was found across the board for most of the
20 applications with the exception of the Westinghouse AP
21 1000 PRA.

22 Just to go into a little more detail on
23 some of the main limitations that we identified. The
24 level of detail in the PRA models that we looked at
25 did not appear appropriate to model all the different

NEAL R. GROSS

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

1 unique features and components of digital I&C systems.
2 In some cases, aspects such as communication network
3 voting, synchronization were not considered in the
4 models.

5 The propagation of the failures, to
6 propagate from the digital system out into other
7 systems in the plant were not typically considered.
8 Also, the basis for the effectiveness of some of the
9 fault tolerance features was not provided.

10 And, again, as I mentioned earlier, some
11 of the negative -- potential negative aspects of some
12 of these features were not considered in the models.

13 The lack of failure parameter data, again,
14 the raw failure data, as I mentioned, was not publicly
15 available or at least we couldn't get a hold of it.
16 Very likely proprietary manufacturer data. So most of
17 the estimated hardware failure probabilities that were
18 in these models were based on proprietary data.

19 The analysis is not documented,
20 particularly, for instance, in the advanced reactors
21 periods we have from Westinghouse and the ESBWR PRAs,
22 there was nothing in there about where the data came
23 from.

24 We did end up extracting some data from
25 PRISM but that data had very large variability to it.

NEAL R. GROSS

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

1 B&L estimates and failure rates using that data and
2 obviously came up with some very large error factors.
3 So I think also Steven mentioned they used some of
4 that data for the dynamic method. I mean there is
5 just a dearth of good data out there so it is what it
6 is. But that is definitely an area that improvement
7 is definitely welcome.

8 Some of the important parameters such as
9 the hardware failure rates and the common cause
10 failure parameters, again, just scarce. There's not
11 much out there. So expert judgment is used to
12 quantify a lot of these models.

13 Again, I'm not going to belabor the
14 software issue. It is well known. The National
15 Research Council or as we referred to previously as
16 the National Academy of Science Report, recommend that
17 software failures be included in the reliability
18 model.

19 There was one dissenting opinion in that
20 report. I guess Nancy Levinson felt that you just
21 could not quantify software failure probabilities.
22 But in general, the Council recommended they do be
23 included in models.

24 Our comparison of the models that we
25 looked at to the criteria just further underscored the

NEAL R. GROSS

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

1 fact that right now there is no consensus method for
2 doing that.

3 So conclusions, we went through and
4 identified a detailed set of criteria, again 48 of
5 them, from what we felt would be the appropriate
6 attributes for a digital system reliability model to
7 be used in a PRA.

8 These criteria that we identified would
9 apply to all reliability models of digital systems,
10 not just necessarily traditional models. And they can
11 be used to develop regulatory guidance -- either
12 regulatory guidance specific for digital system
13 licensing applications or for general PRA guidance
14 such as Reg Guide 1200 or whatever other guidance
15 would be applicable.

16 Again, we looked at six different models
17 and applied them to the criteria to determine where
18 the state of the art existed. As I mentioned before,
19 even the best of models only met 16 of the 48
20 criteria. And there were a large number of the
21 criteria that were not met by any of the models.

22 Nonetheless, even though the statistics on
23 the criteria may be somewhat negative, it really, in
24 our estimation, it boils down to three main areas that
25 need to be improved upon for use of traditional

NEAL R. GROSS

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

1 methods. The first is, again, the systemic evaluation
2 of failure modes, specifically digital systems. And
3 regardless of whether we quantify or not, it is just
4 an important thing to do to understand how the systems
5 can fail.

6 The second thing is getting -- if we do
7 want to quantify is getting appropriate data that we
8 can use for the models.

9 And third is dealing with the 800-pound
10 gorilla, the software reliability.

11 There is also the issue of uncertainty
12 analysis. Again, that one is more in the application
13 of the methods. It is not an inherent limitation of
14 the methods themselves. Any of those methods you can
15 perform uncertainty analysis for them even if the
16 models we looked at did not do that.

17 Bottom line, we identified the fault
18 tree/event tree methods and our version of the Markov
19 methods as the two most promising methods for being
20 able to model digital systems in a PRA.

21 Those two methods do not themselves
22 inherently have the limitations that we just described
23 above. The methods themselves don't. But any models
24 you want to use applying those methods is still going
25 to need to address those items.

NEAL R. GROSS

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

1 So our bottom line conclusion is it may be
2 possible to use those two methods to develop
3 reasonable digital system reliability models but we do
4 need to address those three main bullets at the top of
5 this slide.

6 Next steps, as I mentioned previously,
7 we're going to set up a peer review panel to go over
8 the work that we just did under Task 1, essentially
9 seeing whether or not we have the right criteria. And
10 also seeing whether we have come up with the right
11 methods for pursuing.

12 And then secondly, as you saw from the
13 slide on the tasks coming up, we are going to go ahead
14 and further develop these two methods and apply them
15 to two test case systems so that we can further
16 demonstrate the capabilities and limitations of these
17 methods and establish where the state of the art
18 exists.

19 CHAIR APOSTOLAKIS: Any comments?

20 MR. KEMPER: Yes, this is Bill Kemper. I
21 just wanted to add that unrelated to this, we went off
22 and had Oak Ridge try to ferret out some of this
23 failure data for different purposes so that we could
24 use it in terms of review, you know trying to target
25 our reviews more effectively on digital systems.

NEAL R. GROSS

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

1 And they, too, are struggling with trying
2 to find some data that is usable. So this is clearly
3 a big issue here.

4 CHAIR APOSTOLAKIS: Didn't Brookhaven also
5 look at some data?

6 MR. KEMPER: Yes. Brookhaven did their
7 own data search. But we had Oak Ridge do yet another
8 one for an unrelated reason to this project and was
9 hoping that the data would be usable maybe at some
10 point once we looked at it for this, too, and we are
11 not having much luck there either.

12 MR. KURITZKY: Yes, I think there are two
13 aspects. The Brookhaven work -- the work that
14 Brookhaven did previously on data, similar, I think,
15 to what Oak Ridge did, they looked at data. In their
16 search of LERs or in other software failure events,
17 they were identifying -- not to come up with failure
18 probabilities but just to see description of the
19 events to see how the software can fail to understand
20 different mechanisms of failure.

21 CHAIR APOSTOLAKIS: Which is the most
22 important thing right now.

23 MR. KURITZKY: Right. It is a very
24 important thing, exactly. And the second thing they
25 looked at was also for hardware failure databases.

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 They actually looked at databases. Because with the
2 software, again, you are just looking at events. You
3 are not getting failure probabilities. With the
4 hardware, we were actually looking to see whether or
5 not there were some actual failure parameters, some
6 actual failure rates, failure probabilities like we
7 used for the hardware part of the digital system.

8 And so they were evaluating certain
9 databases in that regard. And even that, again, was
10 not too promising. But that's where we are.

11 MR. ARNDT: At the risk of overstating the
12 point, there has also been several studies looking at
13 software failure rates, if you will excuse the
14 expression.

15 CHAIR APOSTOLAKIS: That's fine.

16 MR. ARNDT: NIST has done a study. Bev
17 Littlewood has done a study. There have been a number
18 of studies out there. The biggest problem with that
19 is almost all of it is very application specific.

20 We heard this morning in detail the
21 quality of the development process, the specific
22 application, the amount of testing, the amount of V&V,
23 software failure rates, if you are going to actually
24 look at an independent software model, is extremely
25 dependent upon what the application -- intended

NEAL R. GROSS

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

1 application is.

2 CHAIR APOSTOLAKIS: The context.

3 MR. ARNDT: Yes. Well, both the context
4 and also the development process. So it continues to
5 be a challenge. We are looking at it. We are working
6 on it. We are obviously interested if we get
7 applications from the industry that includes that kind
8 of thing, we're going to have to be smart enough about
9 it to be able to make an assessment. But it ain't
10 easy.

11 DR. GUARRO: This is Sergio Guarro. One
12 thing that kind of bothers me a little bit is this
13 reference to digital systems without distinguishing
14 what is inside a digital system because there is the
15 hardware on which it runs. There is the software
16 self-management as to the timing, memory, location, et
17 cetera, et cetera. And then there is the function
18 itself that the software hosted on the system
19 accomplishes.

20 And it is not clear to me that the same
21 matters would be good to model these three different
22 aspects. I think evaluating a method against "digital
23 system" without, you know, looking at the pieces of
24 the digital system as they stand rather distinguished
25 from one another may be not the right way to look at

NEAL R. GROSS

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

1 them.

2 MR. ARNDT: Yes, that is certainly an
3 issue, Sergio. And this study, as well as others, is
4 making certain implicit assumptions about that in
5 essence because we are looking at the specific
6 application, in this case the AP 1000 or whatever.

7 One of the reasons why we are exposing
8 both of the variety of methods in traditional and
9 dynamic to two specific benchmarks is to try and get
10 a handle at least a little bit on the application-
11 specific, the hardware-specific, the amount of V&V and
12 those kinds of issues.

13 DR. GUARRO: But you see the thing is
14 there are methods out there that may be good for one
15 aspect. But if you evaluate them against something
16 for which they were not even intended or at least for
17 which they were not applied because the developer was
18 interested in one of the three aspects -- in fact I
19 know that some of the NASA work that I have been
20 involved in was focusing on software. It was not
21 focusing on the hosting hardware, for example.

22 So there is other work done at NASA on
23 that. But, you know, I'm just saying so those were
24 handled in separate ways. And so when you look at the
25 results of a particular application that was intended

NEAL R. GROSS

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

1 for one purpose and you try to make a judgment across
2 your definition of digital system, yes, that method
3 will fail in the sense that it was not even tested in
4 that direction so to speak.

5 So I think I would be a little bit more
6 careful in the way you go about judging, you know,
7 against your 48 criteria. Maybe you should partition
8 for different aspects of the model.

9 MR. MARTINEZ-GURIDI: Well, I think we
10 share your concern.

11 CHAIR APOSTOLAKIS: Who are you?

12 MR. MARTINEZ-GURIDI: Gerardo Martinez-
13 Guridi.

14 CHAIR APOSTOLAKIS: Now you can speak.

15 (Laughter.)

16 MR. MARTINEZ-GURIDI: I think, in fact, we
17 share your concern. Out of the eight categories that
18 we have, the first category is the level of detail of
19 the model. So in the level of detail, we are
20 concerned that all the important details of the model,
21 all the different aspects are taken into account.

22 So, for example, when we reviewed the
23 different applications, we saw that there were at the
24 fairly high level, that is actually one of our
25 concerns, we feel that the necessary level of detail

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 of the analysis has to be evaluated for the model to
2 be actually, you know, good enough for the evaluation.

3 So we are aware of that. And we share
4 your concern.

5 MR. KURITZKY: And this is Alan Kuritzky.
6 Also, Sergio, I think to keep in mind is that what
7 we're doing now is we are just looking at where the
8 state of the art exists. We are not advancing it. We
9 want to look at a snapshot of where we are right now
10 in time.

11 DR. GUARRO: I understand. But I guess
12 you should be careful in how you characterize, you
13 know, some of these results. Maybe you want to say
14 okay, this was untested in this area rather than, you
15 know, marking it as not good for that area, you know,
16 because as I said, in some cases, some of these
17 methods were simply not intended or applied in the
18 direction which you need applied.

19 MR. KURITZKY: Right. And again, this is
20 Alan Kuritzky. Actually the results of our comparison
21 had yes and no put in the table. But we also had a
22 lot of N/As or not applicable or not available. So we
23 recognized that not all the models that we looked at
24 matched up exactly with the criteria, with all the
25 criteria.

1 CHAIR APOSTOLAKIS: But I think we should
2 -- we understand Sergio's concern.

3 DR. GUARRO: My concern is simply
4 hopefully, you know, this evaluation is not a
5 preclusion for, you know, some further evaluation in
6 the future if there is a need and a benefit in looking
7 at something. And it may be extrapolating it from
8 where it was originally applied to a useful
9 application in the nuclear plant area.

10 MR. KURITZKY: Okay.

11 MEMBER ABDEL-KHALIK: I have a question
12 about the systematic evaluation of possible failure
13 modes and effects. And the question in my own mind is
14 whether this is really a problem with the analyst or
15 a problem with the method.

16 But I sense that if you have an analyst
17 who is familiar with the dynamic methodologies and so
18 on, would that analyst be able to do a better job
19 using traditional methods?

20 MR. KURITZKY: Yes. Well, it definitely
21 goes to the quality of the analyst. What we were
22 looking for specifically is having it somewhat
23 systematic so that whoever happens to be -- there may
24 be -- certainly it is very, you know, subjective in
25 the sense that one analyst is going to go and do his

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 failure modes and effects analysis for the system and
2 come up with whatever failure modes he thinks of.

3 Another analyst could go and look at that
4 same system and come up with not exactly the same
5 list.

6 And what we want to do is because what we
7 saw from the applications that we looked at was that
8 no one seemed to do a fantastic job, that there should
9 be some systematic, you know, some tools or something
10 to help people do a systematic identification of the
11 failure modes.

12 That way it would be a little more
13 consistent across the board. And we wouldn't end up
14 with certain models having well possibly lower failure
15 probabilities because they just didn't consider
16 certain failure modes that are more detailed -- you
17 know, a better analyst, you know, did a more detailed
18 look and found other failure modes.

19 So the idea was that it is definitely a
20 function of the analyst but we want to have -- we feel
21 there should be some kind of systematic method that
22 would kind of level the playing field.

23 MR. ARNDT: Yes, actually there are three
24 issues here. One is the one that Alan just mentioned.
25 One is the fact that some methods are more likely to

NEAL R. GROSS

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

1 yield a broader set than others. And that is an issue
2 associated with what is the best method? What is an
3 acceptable method? And what is not an acceptable
4 method? And that is something we have to work on and
5 evaluate.

6 The third thing is, quite frankly, this is
7 not a terribly mature area right now. And we can
8 argue how mature it is but as we get better at this
9 and as we do more of them, it is likely that we will
10 get a better feel for what needs to be included and
11 what doesn't need to be included. And have more
12 examples and things like that. So I think that is
13 part of the challenge we have right now.

14 MR. MARTINEZ-GURIDI: Yes, let me add my
15 two cents here. I think another important aspect is
16 that digital systems are just extremely complicated.
17 And, therefore, for an analyst just to be able to
18 think -- even if he is very prepared, very
19 knowledgeable, just to be able to out of his -- off
20 the top of his head come up with the failure modes is
21 almost impossible.

22 For some of the systems, it is fairly
23 straightforward because, for example, you may have
24 valves. And the failure modes of the valves are
25 pretty easy. It either closes or opens.

1 For digital systems, you have dozens of
2 hundreds of signals going around communicating with
3 the microprocessors, communicating with the actuating
4 devices, getting feedback. So it is very difficult to
5 find out in a reasonably complete way all the
6 applicable failure modes.

7 That is really the main issue. I mean if
8 you do an analysis, how do you get some assurance, at
9 least have some level of confidence that you have been
10 able to encompass all of the important failure modes
11 that can actually lead to failure of the system?

12 And I think that is one of the greatest
13 issues in this field. Just coming up and modeling a
14 digital system in terms of an analog system is not
15 going to do the job.

16 MEMBER ABDEL-KHALIK: Thank you.

17 CHAIR APOSTOLAKIS: Okay. Thank you.
18 We'll move on to the last presentation. Let's try to
19 wrap it up by five o'clock please.

20 MR. ARNDT: This shouldn't be very long.

21 CHAIR APOSTOLAKIS: Not just your
22 presentation. The whole meeting.

23 MR. ARNDT: I understand.

24 This won't be very long and then, of
25 course, you have to have whatever deliberations you

NEAL R. GROSS

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

1 want to have.

2 CHAIR APOSTOLAKIS: We have discussed more
3 or less the presentation.

4 MR. ARNDT: I think we are closed on that.
5 We can have an offline discussion if you think we
6 should. And I think we probably should next week to
7 make sure that we have -- we are covering everything
8 you need.

9 CHAIR APOSTOLAKIS: Okay.

10 MR. ARNDT: This is relatively short
11 presentation. Last time we were before the
12 Subcommittee last year, I gave a somewhat longer
13 presentation on where we were going on the development
14 of regulatory guidance. And I'm going to -- this is
15 a summary of that but it also updates it.

16 As we talked about earlier in the
17 presentation, we have three goals. We've got Goal 1,
18 Part 52 clarification of the guidance, Part 2, how
19 much can we do in the short term using current
20 methods, and Part 3 is the development of detailed,
21 comprehensive risk-informed decision-making.

22 So the idea is as part of the risk
23 program, we want to develop that guidance. Because --
24 and I think this says it in the next slide but I'll
25 say it here anyway -- we want to look at the specific

NEAL R. GROSS

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

1 long-term issues and that we have short term issues.
2 The longer term issues are going to get kind of pushed
3 back a little bit in terms of schedule one because we
4 want to understand what we can about the current
5 applications to make ourselves smarter about it but
6 also because of resources.

7 Now let me make a couple of quick comments
8 about the point in the second bullet here. To develop
9 the guidance, there are several steps we've got to
10 look at. We've got to understand the failure data.

11 We've got to understand what possible
12 methods might be usable. And that's a factor of two
13 things. One, the research -- what we think is
14 available. And two, what the industry brings to us.
15 Because it doesn't make any sense to write a
16 regulatory guidance on something the industry is not
17 going to bring to us.

18 The third bullet is the whole issue that
19 we've talked about a couple times today about
20 categorization of the system. What systems really do
21 need to be modeled and at what level of detail? And
22 what are the criteria or guidelines associated with
23 that? And we are going to come and talk to you about
24 that as that develops.

25 The acceptable methods in the actual

NEAL R. GROSS

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

1 guidelines, what we would like to do is reference
2 specific acceptable methods. Obviously in reg guide
3 or regulatory guidance if the industry wants to bring
4 a different method to us that has the same
5 performance, that is perfectly acceptable.

6 But it makes everyone's life easier if we
7 can reference a particular acceptable methodology.
8 And hopefully we will come to that as part of either
9 the dynamic or traditional methods research or both.

10 A third this is the actual performance-
11 based regulatory acceptance criteria. Or acceptance
12 guidelines if you prefer that terminology. That is an
13 evolutionary kind of process.

14 And I wanted to mention this. If you
15 followed our work in the last three years, the first
16 hack at that was the paper that Nathan and I worked
17 for the PSAM meeting a few years ago. The second hack
18 at it was some of the criteria that we developed in
19 NUREG-6901.

20 The most recent version of that is the
21 criteria you just heard about. So we are learning
22 more. We are evolving. We are developing a better
23 understanding associated with that. So I'll give you
24 an example. In the PSAM paper we wrote three years
25 ago, the criteria was you need to include all the

NEAL R. GROSS

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

1 important failure modes or be able to capture failures
2 that have happened.

3 In what we heard today, we had specific
4 criteria associated with particular failure modes have
5 to be included. So as we get smarter about this, we
6 are trying to include or exclude various requirements
7 or criteria based on what we have learned. So that is
8 the process.

9 To remind you, these are the criteria. So
10 I won't belabor that.

11 We are working on -- I think I mentioned
12 this earlier -- we've shifted some of our resources to
13 the shorter term activities. One, because we want to
14 learn from those activities, and two, because they
15 have a shorter-term priority.

16 When you see the problem statements and
17 detailed deliverables, this is the document -- the
18 version you will see for Problem Statement 2. And I
19 put this up -- or 3 rather -- and I put this up here
20 for a very specific reason.

21 The points in that first tick there review
22 the current models, characterize the acceptance
23 criteria, assess the failure data. That is the same
24 kind of thing that we are doing to develop the
25 regulatory guidance. So that is something that is

NEAL R. GROSS

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

1 specifically articulated in the third problem
2 statement.

3 MR. STONE: Steve, can I ask a question or
4 make a comment?

5 MR. ARNDT: Sure.

6 MR. STONE: The one issue -- and Mr.
7 Kuritzky pointed it out as the 800-pound gorilla here
8 is that I like the process we have been going through
9 here with doing the comparison between the dynamic
10 modeling and the traditional modeling.

11 But the one issue that seems to be driving
12 the risk or uncertainty in the risk is the software
13 modeling. And I don't see a success path in this
14 research program to reaching that at this time. That
15 was my main comment. I'm just wondering how we are
16 planning to address that?

17 MR. ARNDT: That is obviously a big issue.
18 And we hope to, yes, get a success path. Any you can
19 see in here review current modeling methods, including
20 software modeling is one of the big efforts associated
21 with trying to develop that.

22 We are taking two tacts right now which
23 this may not be super satisfying but this is what we
24 have got so far. One is in the dynamic reliability
25 modeling methodology, we are looking at an integrated

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 state space solution. That is to say not explicitly
2 modeling the software or explicitly modeling the
3 hardware. But modeling it as a joint state space.

4 There are some advantages to that and
5 there are some disadvantages to that in both
6 practicality issues and in theoretical analysis
7 issues.

8 In the traditional modeling methods, we
9 are looking at separate hardware models and software
10 models and then the integration associated with them.
11 How do you integrate the failure spaces associated
12 with them? So that is going to address that specific
13 aspect.

14 Obviously you can do traditional modeling
15 methods in an integrated way or you can do dynamic
16 methods in a non-integrated way. We are not currently
17 looking at that specifically simply because there are
18 only so many resources and that's what seemed to make
19 sense to us at the time from both theoretical and
20 practical considerations.

21 In Problem Statement 2, which is the
22 short-term things, we are probably going to address
23 that specifically. How we are going to address that
24 specifically, I don't know. I think it will depend a
25 little on what the industry brings to us in terms 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 their opinion on what can be done. And lessons
2 learned. Lessons learned to date in that area is not
3 very satisfying from the NRC side. So that very well,
4 as we evolve our work in Problem Statement 2 on short-
5 term usability of the current methodologies, that may
6 be something that we say we can't do much until we
7 solve that so let's find a short-term solution to that
8 particular problem.

9 I'm getting ahead of myself because I
10 haven't seen what the industry is going to bring to us
11 yet. So I don't know exactly how much work we are
12 going to be doing associated with that.

13 MR. KURITZKY: Steve, this is Alan
14 Kuritzky again. I think also to get to Jeff's
15 comment, there is a good point, right now the work
16 that we are doing on the traditional methods research
17 is identifying and demonstrating the capabilities and
18 limitations as they are today.

19 So it is fair to assume that given that we
20 are going to run into that 800-pound gorilla and are
21 going to have to tackle him at some point, that that
22 is something that likely will need to be addressed.
23 So, you know, that is something that we will have to
24 keep in consideration as this work progresses.

25 At some point we're going to have to say

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we can only dance around that gorilla for so long.
2 Then we are going to have to dance with him.

3 MR. ARNDT: Okay. So basically to recap
4 the strategy as we have it now, we are looking at
5 understanding the characteristics of the systems that
6 need to be modeled as articulated in 6901 and the
7 equivalent traditional modeling NUREG, which is the
8 past two output NUREG that Alan just talked about and
9 other issues input from industry and others,
10 identifying the methodologies that could be used,
11 developing an understanding of the data, integrating
12 the information developed from Problem Statements 1
13 and 2, supporting research and input from external
14 stakeholders, develop the reg guide and send it out.

15 We were originally planning on doing that
16 this year. Both inputs from our industry counterparts
17 that basically said let's not get ahead of ourselves.
18 I think they were concerned about the fact that we had
19 published more on the dynamic modeling methods than
20 the traditional modeling methods as you heard earlier
21 as well as the priorities associated with the short-
22 term issues, we have pushed those milestones out.

23 So basically this is just a summary of
24 what I have said. And our intention right now is that
25 the final regulatory guidance will be performance-

NEAL R. GROSS

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

1 based. That is to say we are not going to mandate a
2 particular methodology. We may point to a methodology
3 as acceptable but the guidance will be in terms of
4 what are the characteristics of the methodology that
5 is necessary to model the systems.

6 CHAIR APOSTOLAKIS: Very good. Thank you.

7 MR. ARNDT: Okay?

8 CHAIR APOSTOLAKIS: Thank you.

9 Shall we go around the table again to
10 record first impressions?

11 MEMBER ABDEL-KHALIK: Well, I guess I'm
12 still stuck on the first step. On the one hand, we
13 have a very well thought out report by the National
14 Academy that said there is not generally applicable
15 effective way to evaluate diversity between two pieces
16 of software performing the same function which implies
17 that whatever backup system you would provide to the
18 operators, whether that is safety related or non-
19 safety related, has to be an analog system.

20 Now I was told that that is not true.
21 And, therefore, you essentially disagree with the
22 statement made in the National Academy report. And
23 yet you haven't really shown me at least why and how
24 you can support that conclusion. That is my biggest
25 concern.

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 CHAIR APOSTOLAKIS: Thank you.

2 MEMBER ABDEL-KHALIK: Thank you.

3 CHAIR APOSTOLAKIS: Tom?

4 MEMBER KRESS: Well, I think it is
5 possible to define diversity in terms of non-analog
6 backups. And it would have to do with the various
7 attributes of the diverse systems.

8 As far as -- you are never going to
9 quantify diverse -- you are never going to say how
10 much diversity is enough, how much is necessary. I
11 think you will just have to use judgment and say if a
12 given system has these characteristics and has
13 followed these procedures and so forth, it is
14 acceptable to us.

15 You do this all the time anyway in
16 regulatory space. You are not going to be able to do
17 what is implied in the statement that you are going to
18 determine the risk implications of the diversity of
19 the different levels. You are just not going to be
20 able to do that I don't think.

21 Now I understand that is possibly the
22 intent of some of the research processes you are
23 looking at to actually be able to develop software
24 reliability. But, you know, I think you are going to
25 be a long way off from that.

1 So I support your approach in saying I
2 want to develop the attributes of diversity and the
3 attributes of defense-in-depth. And use judgement and
4 expert opinion and say these are what I want to see in
5 terms of these attributes.

6 And if the systems meet these attributes,
7 then they are acceptable to us. So I think that is
8 the only approach you are going to have.

9 MEMBER ABDEL-KHALIK: Well, I do fully
10 recognize the complications of having both. I mean
11 that doesn't necessarily enhance safety. But yet I'm
12 just trying to resolve this dilemma.

13 MEMBER KRESS: I think you are going to be
14 likely be in design-based space forever. You put
15 together a deterministic way to evaluate these things
16 with the hope that you render it to a safe level.
17 That's a hope. And it seems to have worked in severe
18 accident space in terms of design basis.

19 And there's a good -- I think there is a
20 good possibility if you use the right judgments and
21 the insights that you know, that would probably work
22 here. You are never going to be able to validate it
23 and say yes, we know that this system with this
24 diversity and this defense-in-depth has a certain
25 reliability. I'm just doubtful you are ever going to

NEAL R. GROSS

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

1 get there.

2 But I do support the research in that area
3 because I think you learn a lot whether you ever get
4 to that final point or not. You are learning a lot
5 about software systems and how they operate and
6 possible failure modes.

7 So I think you guys have a good plan. And
8 you are working in the right direction.

9 CHAIR APOSTOLAKIS: Otto?

10 MEMBER MAYNARD: Well, first of all on the
11 National Academy of Science Report, I thought it was
12 an outstanding report, a lot of good conclusions and
13 recommendations. I don't necessarily agree that you
14 have to have an analog backup system. I'm not sure
15 that is exactly what they were saying.

16 If you read their words, they are saying
17 you could not have diversity in the software aspects
18 of it but I think it is up to the NRC to take that
19 report, make their own judgements. If they are not
20 going to do something that is in there, whatever needs
21 to be justified or discussed there, because I think
22 the report also acknowledged that you can certainly
23 make the systems too complex or make it less safe by
24 doing too many things and stuff, too.

25 So I think it is up to the regulator to

NEAL R. GROSS

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

1 decide what aspects we do. And I think there are some
2 other ways of dealing with that issue that ultimately
3 ends up with a safer and better system.

4 But I just think that issue needs to be
5 addressed head on and dealt with. Not necessarily say
6 that you have to have an analog backup system because
7 I personally think that would not be the right way to
8 go.

9 Overall, I'm impressed with the effort.
10 This is the first meeting I have sat in on. The first
11 time I've been here. And overall with the effort to
12 date, a lot of good things are going on. I think
13 overall a reasonable plan on the aspects of it that we
14 have heard here.

15 I'm glad to see some schedules associated
16 with these things. I was glad to see that included in
17 some of the presentations as to when you are really
18 going to be trying to deliver a product. And so I was
19 appreciative of that.

20 My concern overall would be with ultimate
21 timing on this whole thing. And both for the
22 industry's input and for the regulator's input. You
23 know this isn't a new issue. It is a new issue for
24 the NRC but it is something that other industries have
25 had to deal with.

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 I know that we have researched that. My
2 concern is that if we take too long on this that we
3 are going to end up -- things are going to be done by
4 default rather than by actually making decisions up
5 front. And putting the criteria in place.

6 At some point, we are going to have to
7 recognize that we have reached the point of
8 diminishing returns and decisions are going to have to
9 be made. We know this. We don't know that. Let's
10 admit that. Let's take a look at where we stand
11 overall.

12 There are consequences for being too
13 conservative. And there are consequences for not
14 being conservative enough. And it is ultimately going
15 to end up with a management decision on some of these
16 things.

17 We are not going to find a perfect model
18 or a perfect solution that we plug something in and it
19 gives us an answer. It is going to ultimately come
20 down to judgments by people using the best available
21 information that they have. And doing that in a
22 timely manner to support the next generation of plants
23 and what we're doing so that we end up -- what I
24 believe we are going to end up with with safer systems
25 overall.

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 I have gone through this in the aviation
2 side of things. Of having better, more reliable,
3 safer digital systems available but not legal. And
4 so, you know, what do you use and stuff? And I think
5 that the sooner we could transition into the digital
6 world, we are going to ultimately end up with a safer
7 system.

8 There may be a slight decrease in risk --
9 or a slight increase in risk for a short period of
10 time. I don't think that is going to be significant
11 while we are going through our learning process. But
12 it is going to end up with so much better from a risk
13 and a reliability standpoint in the future.

14 I would like to make just a couple more
15 comments on the simulator because I'm not real sure I
16 understand how that was being proposed to be used in
17 the dynamic modeling there. Simulator is very
18 beneficial for a lot. It is very useful. It is very
19 beneficial for training. It can be used for
20 identifying potential issues in design and evaluation
21 of safety analysis and stuff.

22 But you really do have to recognize the
23 limitations of the simulator. I can change from an
24 analog to a digital feedwater control system in the
25 plant without ever making a change to my simulator

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 whatsoever. I can do the same thing with the reactor
2 protection system. Therefore, it may not be modeling
3 exactly the digital I&C aspects of things unless your
4 simulator is actually designed and is set up to do
5 this.

6 So we have to recognize the limitations.
7 I don't discount the simulator. But we also need to
8 recognize the limitations of that, too.

9 But overall it is a good plan. Again,
10 timing and making some decisions would be the biggest
11 thing. I think that both the industry and the NRC
12 have got to do it and make it happen.

13 CHAIR APOSTOLAKIS: Sergio? You will send
14 me -- are you there?

15 DR. GUARRO: Yes, I am.

16 CHAIR APOSTOLAKIS: Yes, you will send me
17 comments in writing. But would you like to say
18 anything now?

19 DR. GUARRO: Just one observation on the
20 analog backup question. I think it was a question of
21 you know, how diverse is diverse enough because in
22 reality I think when people say the digital backup
23 would not be acceptable, when those people say that,
24 they think of the fact that the specification process
25 may be effected by the same flaws for the original

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 and so the backup system will fail by design
2 the same way.

3 Well, that poses the question wouldn't
4 similar logic specification, for example, being used
5 for the analog, I mean, you know, if you think of a
6 reactor protection system essentially the
7 specification if for a logic that then, you know, you
8 can implement with relays or things of that nature.
9 Or you can implement with digital software.

10 And so I just want to note that it really
11 is not the black and white of digital versus "analog"
12 because I don't even know if the word analog applies
13 for that particular example, but it is really a degree
14 of gray. In fact, as you probably -- most of you
15 know, we have this devices, you know, in our field-
16 programmable gator rays, are they software or are they
17 hardware, you know? They are something in between,
18 right?

19 So I just wanted to note that because in
20 considering the question of, you know, how far you
21 have to go in diversity, I think this issue of analog
22 versus digital, quote-unquote, falls in that category.

23 CHAIR APOSTOLAKIS: Okay. Thank you.

24 Well, I think I expressed most of my
25 comments during the meeting. And I'll just repeat

NEAL R. GROSS

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

1 that I really would like to see more use of the data,
2 the experience, the operating experience.

3 Maybe as you were talking about
4 simulators, the human reliability group of the agency
5 is planning to have a major benchmark exercise in
6 Halden using their simulator.

7 You might want to think about whether you
8 might do something similar. Not necessarily the
9 simulator that you mentioned earlier but some
10 collaboration with you simulator and their simulator
11 and see whether you can look at some accident
12 sequence, some initiating events and see what you get
13 out of it since we have this agreement with the Halden
14 people.

15 Other than that, I think you are on the
16 right path. And overall it sounds good. I think
17 forming this senior group has been very beneficial to
18 the whole effort. And we'll see.

19 And we have discussed your presentation to
20 the full Committee so we don't need to go back to it.

21 MR. ARNDT: And we will get back to you
22 later next week --

23 CHAIR APOSTOLAKIS: Okay.

24 MR. ARNDT: -- to make sure we are on
25 track.

1 CHAIR APOSTOLAKIS: And you will send us
2 some documents. Send them to Mr. Hammer and he will
3 make sure everybody gets a copy.

4 MR. ARNDT: Yes, sir.

5 CHAIR APOSTOLAKIS: So with that I think
6 we are near the end of the meeting unless there are
7 any more comments from the audience perhaps?

8 MR. ENZINNA: I'd like to make one comment
9 please. I'm Bob Enzinna. I'm a PRA practitioner at
10 ERIVA. I'm of the school of opinion that we are never
11 going to be able to put a precise probability on the
12 failure of software. But that doesn't mean we can't
13 do things to reduce that probability.

14 When you are talking about software,
15 there's two parts. There is the application software
16 and there is the operating system. And Steve
17 mentioned earlier, you know, things that can be done
18 and are done to reduce the probability of failure in
19 the application software, you know, V&V and tools for
20 development, functional blocks, things like that.

21 The other part of it is the operating
22 system. And the important thing about the operating
23 system and the safety-related design is to make sure
24 that the application software failures don't propagate
25 via the operating system to other diverse functions.

1 And there are the attributes that are
2 mentioned. And the other technical working groups
3 should be telling us what those attributes are. The
4 attributes of the operating system that provide
5 robustness and things we are putting in our safety-
6 related designs like cyclic processing, you know,
7 constant bus loading, static memory allocation, there
8 is a whole list of features like this that prevent an
9 application or a specification error in the software
10 of one function from defeating other functions by
11 taking down the operating system.

12 And that's what I think we should be
13 looking at is to find those attributes so that we can
14 make the numbers better not necessarily define what
15 they are, the numbers I mean.

16 CHAIR APOSTOLAKIS: But wouldn't you say
17 though that the question what is the unreliability of
18 a safety function or a safety system with embedded
19 software, that that could be answered? Could be
20 answered at some point in the future without saying
21 that the contribution from the software is such and
22 such?

23 But I can still talk about the
24 unreliability of the system or the function knowing
25 that because software -- in other words, again, this

NEAL R. GROSS

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

1 comes back to the software-centric versus system-
2 centric approach. About the system, I should be able
3 to say something. Or I take your argument to the
4 extreme and say that, you know, the moment you put
5 digital software in the system you cannot quantify,
6 then, of course, I can't have PRAs any more. I can't
7 have anything, risk-informed regulation.

8 I should be able to say something about
9 the unavailability of these systems and their
10 reliability during the required time, knowing that
11 they are driven by software. So I think that is where
12 the staff is trying to go.

13 MR. ENZINNA: Yes, I was talking about
14 predictively. I mean we have operating systems in the
15 product we sell. And, you know, this system has, you
16 know, years of experience. You know 62 million hours
17 of operating experience we have on the processor, the
18 product we are selling now.

19 So we know the operating system. It has
20 never had a common cause failure. It has never had a
21 failure at all in all that time. So we can put a
22 number on that based on operating experience.

23 The problem is with the application
24 software is that every time you do it it is unique.
25 And so as was said on one of the very first slides, 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 key thing is the functional diversity. The NAS has
2 said this. You know Steve and Cliff said it.
3 Industry consensus standards, they all come down on
4 the side of, you know, functional diversity is
5 important.

6 And it is important to make sure that the
7 functionally diverse, you know, functions are actually
8 -- are diverse. And the independent trains are
9 independent. And that's where, you know, these
10 attributes in the design can make sure that, you know,
11 a failure doesn't propagate to other functions.

12 CHAIR APOSTOLAKIS: And that should lead
13 me to some estimate of the probability. Otherwise, we
14 are going back to the traditional system. The train
15 has left the station already. We have to say
16 something.

17 MR. ENZINNA: Our approach is to come up,
18 you know, a conservative estimate. And from a
19 sensitivity and uncertainty, you know, perspective.

20 CHAIR APOSTOLAKIS: You will be happy with
21 a conservative estimate until it causes pain. Then
22 you will come to think the way I think.

23 (Laughter.)

24 MR. ENZINNA: Fair enough.

25 CHAIR APOSTOLAKIS: Thank you very much

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 for the comment. And I think we have a very useful
2 meeting today. And I appreciate everybody's
3 contributions. And we shall see you gentlemen again
4 in two weeks or something like that.

5 MEMBER KRESS: Two short weeks.

6 CHAIR APOSTOLAKIS: Thank you very much.

7 (Whereupon, the above-entitled meeting was
8 concluded at 4:29 p.m.)

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CERTIFICATE

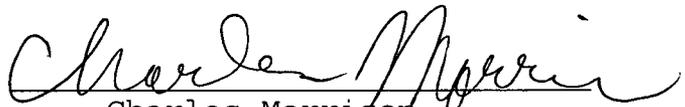
This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission in the matter of:

Name of Proceeding: Advisory Committee on
Reactor Safeguards

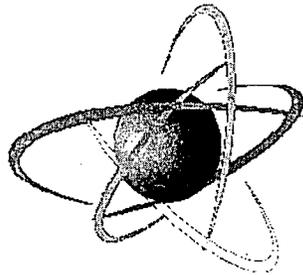
Docket Number: n/a

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.



Charles Morrison
Official Reporter
Neal R. Gross & Co., Inc.



U.S. NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Promoting People and the Environment

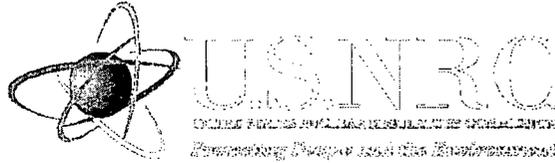
Development of Regulatory Guidance Risk-Informing Digital System Reviews

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

April 18, 2007

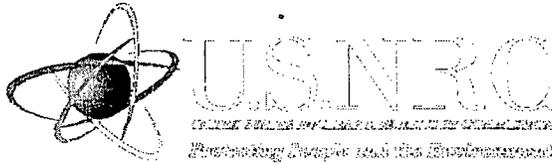
Steven A. Arndt

Division of Fuel, Engineering & Radiological Research
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)



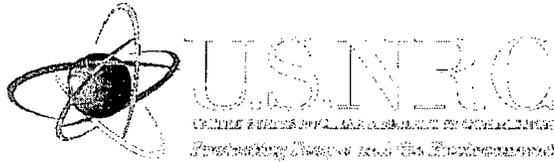
OVERVIEW

- As part of the overall Digital System Risk Program the NRC will develop needed regulatory guidance to support risk-informing digital system reviews
- To develop this guidance the NRC is working to
 - Understand the status of failure data
 - Assess which modeling methods might be usable
 - Determine which systems need to be modeled and at what level of detail
 - Develop acceptable methods
 - Develop regulatory acceptance criteria



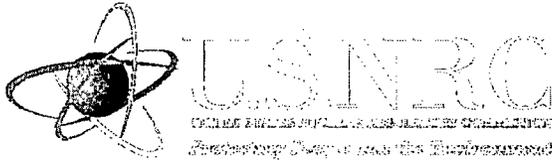
PROBLEM STATEMENTS

- 1. Existing guidance does not provide sufficient clarity on how to use current methods to properly model digital systems in PRAs for design certification applications or license applications (COL) under Part 52.**
- 2. Using current methods for PRAs, NRC has not determined how or if risk-insights can be used to assist in the resolution of specific key digital system issues in operating reactor licensing action requests.**
- 3. An acceptable state-of-the-art method for detailed modeling of digital systems has not been established. An advancement in the state-of-the-art is needed to permit a comprehensive risk-informed decision making framework in licensing reviews of digital systems for current and future reactors**



STATUS

- **As a result of the new priorities in this area, resources have shifted to the shorter term activities (Problem Statements 1 and 2) and the schedule for completion of regulatory guidance has be extended**
- **Development of final guidance will be part of Problem Statement 3**



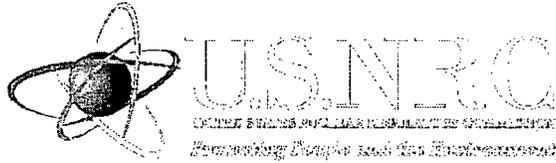
DELIVERABLES

- **For Problem Statement 3**
 - Issue NUREG/CR's that provide the technical bases, in support of risk-informed decision-making for digital systems, including (1) review of current modeling methods (including software modeling), (2) characteristics of acceptable modeling methods, (3) assessment of failure data, (4) criteria for level of modeling detail, (5) assessment of uncertainties, and (6) defining how to interface digital system models with the rest of the PRA
 - Issue regulatory guidance on Risk-Informed decision-making review methods applicable to digital systems.
 - Update NRC PRA data, models and tools to support NRC assessment of digital system risk and reliability.



STRATEGY FOR DEVELOPMENT

- Develop an understanding of the characteristics of digital systems that need to be modeled (NUREG/CR-6901 and equivalent traditional modeling NURG/CR)
- Identify methodologies for modeling digital systems and incorporating these models into existing PRA's
- Develop an understanding of the data issues associated with digital system reliability modeling
- Use the information developed as part of resolving Problem Statements 1 and 2, ongoing research and input from external stakeholders to support the development of regulatory positions
- Draft regulatory guidance, with input from the public
- Publish for comment draft regulatory guidance



SUMMARY

- Research into current state of data, analysis methods, and acceptance criteria will support the development of regulatory guidance for risk-informing digital system reviews
- Research and TWG work is looking look at a number of potentially viable methods for developing acceptable digital system risk models
- Program is assessing the capabilities and limitations of the state-of-the-art and will develop appropriate regulatory requirements
- Regulatory guidance will be performance-based



REVIEW OF TRADITIONAL METHODS FOR MODELING DIGITAL SYSTEMS

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee
April 18, 2007

Alan S. Kuritzky

Division of Risk Assessment and Special Projects
Office of Nuclear Regulatory Research
(301-415-6255, ask1@nrc.gov)

Tsong-Lun Chu, Gerardo Martinez-Guridi, Meng Yue, and John Lehner
Brookhaven National Laboratory

Brookhaven National Laboratory
U.S. Department of Energy



Outline of Presentation

- Current status and plan for traditional methods research
- Objectives and approach
- Review of traditional methods
- Development of criteria for evaluating reliability models of digital systems
- Selection of applications of the methods for review
- Comparison of applications against criteria
- Identification of capabilities and limitations in state-of-the-art of modeling digital systems
- Conclusions, including traditional methods selected



Current Status of Traditional Methods Research

- Project review meeting held on October 3, 2006
 - Traditional PRA methods project to refocus on demonstrating capabilities and limitations of existing methods
 - Project to involve increased stakeholder interactions
 - RES to develop integrated project plan and coordinate Program Office involvement
- Draft integrated plan and schedule developed
- Staff has drafted the risk-informed digital I&C section of the NRC Digital I&C Project Plan (in support of the NRC Digital I&C Steering Committee)



Task Plan for Traditional Methods Research

- Task 1 – Traditional methods selection
Product: Letter report – Draft completed
- Task 1a – External peer review panel for criteria identification and traditional methods selection
Product: Letter report
- Task 2 – Candidate method illustration
Product: Peer-reviewed NUREG/CR (documents Tasks 1, 1a, and 2)
- Task 3 – Apply methods to Benchmark No. 1
Product: Peer-reviewed NUREG/CR
- Task 4 – Apply methods to Benchmark No. 2
Product: Peer-reviewed NUREG/CR
- Task 5 – Integration into PRA
Product: Letter report



Objectives of Task 1

- Develop criteria for evaluating reliability models of digital systems.
 - These draft criteria could eventually provide input to the technical basis for risk-informed decision-making.
- Review of applications using 'traditional' risk methods, such as fault tree and Markov methods, against the criteria to determine the capabilities and limitations of the state-of-the-art.
- Identify the most promising traditional methods for modeling and quantitatively assessing the reliability of digital systems.



Approach for Task 1

- Review traditional methods for modeling digital systems
 - Fault Tree / Event Tree, Markov, SINTEF, Reliability Prediction Methods, NASA (software reliability approach)
 - In addition, review a simplified analytical method used for a Japanese ABWR.
- Develop criteria for evaluating PRA models of digital systems
 - Capture the unique features of digital systems that affect system reliability
- Identify existing applications of the methods
 - Advanced reactor PRAs, plant specific models
- Identify the capabilities and limitations of the existing applications by comparing them against the developed criteria.
- Engage technical community
 - NRC Digital I&C web page
 - Public meeting (April 11-12, 2007)
 - External peer review panel (May-June 2007)



Review of Traditional Methods (1/4)

Fault Tree/Event Tree (FT/ET) Method

- Standard for reliability modeling by the PRA community throughout the world.
- Has been used for a wide variety of applications for many years (computer, aerospace, chemical, and many other industries).
- Well-suited to identify detailed failure modes of the plant, represented by combinations of failures of system components, by combining system models into an overall model of the NPP.
- Can quantitatively evaluate the detailed failure modes of the plant.
- Treats timing of events and interactions with plant processes implicitly in an approximate way.



Review of Traditional Methods (2/4)

Markov Method

- Has been used for modeling NPP systems, including digital systems.
- Allows explicit modeling of the different states that a system can reach during its operation, regardless of the type of system.
- Explicitly treats failure and repair times within the model.
- Number of states can grow very rapidly usually due to the complexity of the system, making the analysis of the model very difficult.
- It considers interactions with plant processes implicitly in an approximate way.
- Integration with a fault tree / event tree model is not straightforward.



Review of Traditional Methods (3/4)

SINTEF Method

- Adaptation of a method specified in international standard IEC 61508 for the Norwegian oil industry. The method uses data that was collected from offshore platforms that is provided in a companion handbook.
- Models a system in terms of a Markov model and solves the model by introducing some simplifying assumptions, such that analytical expressions can be derived.
- Explicitly models fault coverages, and safe and dangerous failures.
- Considers that common-cause failure (CCF) dominates the subsystem unavailability, and independent random failures of components are not considered.
- Ignores the combinations of failures of components from different subsystems.
- Estimates on coverages and hardware failure fraction of the dangerous failure rates, and the beta factors, are based on expert judgment which is not documented.



Review of Traditional Methods (4/4)

Reliability Prediction Methods (RPMs)

- Estimates the failure rate of a circuit board in terms of the failure rates of its components.
- Estimates the failure rates of components at a detailed level taking into consideration such adjustment factors as operating environment.
- Cannot be used to model systems with configurations of components in parallel.
- Technical basis for values derived is not publicly available.
- Does not address uncertainty

NASA PRA Procedures Guide Software Reliability Approach

- Framework for considering software failures in a PRA.
- Does not address modeling of digital system hardware.



Observations from the Review of Methods

- Fault Tree / Event Tree, Markov, and SINTEF methods are general, and some of their applications are reviewed in detail in this study.
 - In addition, an application of a simplified analytical method used for a Japanese ABWR is reviewed.
- RPMs can be considered sources of failure data for probabilistic analysis. Applications of the associated methods were not further examined as part of this study.
- The NASA approach is used only for including quantitative software reliability measures in a PRA, and no applications of this approach were reviewed.



Considerations Supporting the Model Evaluation Criteria

- The goal of a reliability model of a digital system is to account for those design features that have the potential to affect its reliability.
- The modeling should be supported by an analysis, such as an FMEA, which:
 - Identifies different failure modes of the components
 - Identifies potential ways the failure could propagate
 - Identifies potential dependencies
 - Determines how the failures could be detected and mitigated
- The model should include:
 - Software failures (including CCF)
 - Dependencies within the digital system and with other plant systems and equipment
 - Human errors



Considerations Supporting the Review Criteria

- No consensus in the technical community as to whether timing issues need to be treated explicitly in digital system reliability models.
- The model should consider digital system capability to self-test on line and the potential to mitigate detected failures
- Quality data (e.g., applicable, source provided, parameter estimation documented) should be provided, especially in the case of modeling fault tolerance features and CCFs.
- Uncertainty analyses should be performed.
 - Modeling uncertainty
 - Parameter uncertainty
- Ideally, a reliability model of a digital system should be easily integrated with the existing PRA, such that the dependencies of the digital system and the rest of the modeled plant are properly accounted for in the PRA.



Evaluation Criteria of Reliability Models of Digital Systems

- Eight main categories of criteria were identified, and a total of 48 detailed criteria were developed.
 - 1 Level of Detail of the Probabilistic Model
 - 2 Identification of Failure Modes of the Digital System
 - 3 Modeling of Software Failures
 - 4 Modeling of Dependencies
 - 5 Modeling of Human Errors
 - 6 Ease of Integration with a PRA Model
 - 7 Probabilistic Data
 - 8 Documentation and Results
- The relative importance of individual criteria varies.
 - This variation will need to be evaluated when they are considered as input to the technical basis for risk-informed decision making.



Example Review Criteria

Criterion:

2.2 Are the failure modes of features, such as communication, voting, and synchronization, identified to support modeling?

Important because:

- These design features are potential sources of dependencies between redundant channels and between systems
- To a large extent these design features are unique to digital systems



Example Review Criteria

Criteria:

7.1 Were the data obtained from the operating experience of the same component being evaluated?

7.4 If generic data is used, is it of the same generic type of component?

Important because:

- It is desirable to use data that represents realistically the failure characteristics of the component being evaluated
- Generic data may not be fully applicable to the component being evaluated
- Generic data have large uncertainties



Selection of Applications for Review

- Relevance to domestic nuclear industry
- Availability of documentation
- Selected applications (6):
 - Fault tree models
 - AP1000 reactor vendor PRA
 - ESBWR reactor vendor PRA
 - ESFAS of Korean National Standard Plant (Westinghouse 80+ design)
 - Simplified model of RPS and ESFAS of a Japanese ABWR
 - Markov model of Tricon platform
 - Example of SINTEF method
- The characteristics of the digital system model were compared to the criteria.
 - No attempt was made to validate the models.



Comparison of Applications Against the Criteria

- Each application was evaluated against each criterion to determine if the application satisfied the criterion.
- The evaluation involved considerable judgment so it was fairly subjective.
- The extent to which the applications for a given method collectively satisfied the 48 criteria represents the current state-of-the-art for that method as determined by this review.
- The maximum number of criteria satisfied by any one application was 16 (out of 48).
- Twenty-one criteria were not addressed by any of the applications; nine criteria were only addressed by one application.
- The 3 FT/ET models satisfied the highest number of criteria.



Observations Common to All Applications Reviewed

- Main strengths of applications
 - CCFs of hardware within a system were usually modeled. However, data for CCF of digital components appears scarce.
 - Individual failures and CCFs of software were explicitly included in the logic model. However, quantification of these failures is still an issue.
- Main limitations of applications
 - Lack of systematic evaluation of possible failure modes and effects.
 - Lack of applicable failure parameter data.
 - Inadequate quantitative software reliability methods.
 - Inadequate treatment of uncertainties.



Lack of Systematic Evaluation of Possible Failure Modes and Effects

- The level of detail of the PRA models did not appear to be appropriate to model potential failure modes in digital I&C applications.
- Potential failures due to use of communication network, voting, synchronization, e.g., inter-channel communication, were not considered.
- Propagation of failures through interconnections within a digital system and with the rest of the plant was not considered.
- Basis for effectiveness of fault tolerance features, e.g., self-diagnostics, watchdog timers, and surveillance tests, was not provided.



Lack of Applicable Digital Failure Parameter Data

- Raw failure data is not publicly available, e.g., proprietary manufacturer data.
- Estimated hardware failure parameters are based on proprietary data. The analysis of the data is not publicly documented, e.g., in advanced reactor PRAs and reliability prediction methods.
- Data extracted from PRISM have large variability, and BNL estimated failure rates with very large error factors.
- Important parameters, such as hardware failure rates, CCF parameters and fault coverages are scarce.
 - In some cases, the applications derived some parameters using judgment without any additional documentation.



Inadequate Quantitative Software Reliability Methods

- National Research Council recommended that software failures be included in a reliability model.
- The comparison of the applications to the criteria further confirmed that no commonly accepted quantitative software reliability methods exist for safety critical applications.



Conclusions

- A detailed set of criteria was developed to assess the PRA models of digital systems.
- The review criteria are applicable to all reliability models of digital systems, and can be used to support:
 - Development of a regulatory guide (RG) that is specific to digital systems.
 - Update of general PRA guidance to address digital systems.
- The criteria were applied to six applications of four traditional reliability modeling methods, and the applications were assessed to the extent they satisfied the criteria.



Conclusions (2)

- Limitations that appear applicable to all applications:
 - Lack of systematic evaluation of possible failure modes and effects.
 - Lack of applicable failure parameter data.
 - Inadequate quantitative software reliability methods.
- The evaluation of the applications revealed limitations in the way methods are applied, e.g., uncertainty analysis.
- Fault tree / event tree (FT/ET) and Markov methods were selected as the most powerful and flexible traditional methods for modeling digital systems
 - The methods themselves do not inherently have the limitations of the applications studied.
 - It may be possible using FT/ET and Markov methods to develop reasonable digital system reliability models if the limitations above are addressed.



Next Steps

- External peer review of the criteria for evaluating reliability models of digital systems and of the selection of traditional methods.
- The application of traditional FT/ET and Markov methods to two digital systems using the insights from this review and the best features from the current state-of-the-art.



DYNAMIC RELIABILITY MODELING OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS FOR NUCLEAR REACTOR PROBABILISTIC RISK ASSESSMENTS

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee
April 18, 2007

Steven A. Arndt

Division of Fuel, Engineering & Radiological Research
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)

Tunc Aldemir

Nuclear Engineering Program
The Ohio State University
(614-292-4627, aldemir.1@osu.edu)



Presentation Organization

- Background
- Progress since June 27, 2006 meeting
 - Revision of the NUREG/CR – XXXX to address comments
 - Modeling efforts using the Markov/cell-to-cell mapping technique (CCMT) methodology
 - Modeling efforts using the dynamic flowgraph methodology (DFM)
 - Comparison of Markov/CCMT and DFM results for an example initiating event
 - Failure data estimation
 - Integration of Markov/CCMT and DFM results into an example plant PRA model
- Conclusion to date and next steps



Background

- The Office of Nuclear Regulatory Research has a program that is evaluating and developing modeling methods needed to support risk-informed regulation of these systems
- NAS study recommended that the preferred method of evaluating a digital system would include modeling system interaction as well as hardware and software modeling
- For near term PRA applications, a digital I&C system reliability model needs to be compatible with the structure of current nuclear power plant PRAs, which use the static event-tree/fault-tree (ET/FT) approach
 - Research to understand what can be done using traditional method
 - Parallel research to develop advanced methods that directly account for hardware, software and process interactions and can still be linked to static ET/FT models



Objectives of Digital Systems Risk Assessment Research Program

- To identify and develop methods, analytical tools and regulatory guidance (regulatory guides, Standard Review Plan [SRP] updates, NUREG/CR publication of acceptance criteria) to support
 - Use of digital system risk information in nuclear power plant (NPP) licensing decisions
 - Inclusion of digital system models into NPP probabilistic risk assessments (PRAs)
 - Review of Part 52 future reactor PRAs



Overview of Tasks and Responsibilities for Digital Systems Risk Assessment Research Program

1. Overall program coordination (DFERR)
2. Development of regulatory guidance (DFERR lead)
3. Interface with Digital I&C Steering Committee (DFERR lead)
4. Investigate and refine methods involving traditional methods supported by traditional FMEA and data analysis (DRASP)
5. Investigate and develop a method involving Markov models and dynamic flowgraph method (DFM) supported by advanced digital system test-based methods (DFERR)
6. Develop two “benchmark” test cases to support development of acceptance criteria, tools, and methods (DFERR)



Overall Approach for Dynamic Methods

- Investigate the capabilities and limitations of the current static event tree/fault tree (ET/FT) methodology to digital I&C systems
- Investigate the advantages and limitations of available dynamic methodologies as they pertain to digital I&C systems relevant to reactor protection and control
- Review other industry practices used for reliability modeling of digital I&C systems
- Review the existing regulatory framework with regard to requirements that a digital I&C control system must meet
- Identify the minimum requirements a digital system model must meet for successful incorporation into an existing PRA
- Identify available methodologies that meet these requirements
- Demonstrate the identified methodologies using relevant benchmark systems



Current Status

- NUREG/CR-6901 *“Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments”*
 - identified the Markov/CCMT methodology and the DFM as methodologies that rank as the top two with most positive features and least negative or uncertain features when evaluated against the requirements for the reliability modeling of digital I&C systems
 - concluded that benchmark systems should be defined to allow assessment of the methodologies proposed for the reliability modeling of digital I&C systems using a common set of hardware/ software/ firmware states and state transition data
- Two benchmark digital I&C systems (a feedwater controller and a RPS) have been specified for the assessment of the methodologies proposed for the reliability modeling of digital I&C systems using a common set of hardware/software/ firmware states
- An example initiating event (turbine trip) has been used with the first benchmark system to illustrate how the DFM and the Markov/CCMT methodology can be used for the reliability modeling of digital I&C systems
- The findings of these efforts have been compiled in a NUREG/CR-XXXX draft titled *“Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments”*
- Preliminary results of failure data estimation trials for the DFWCS have been obtained

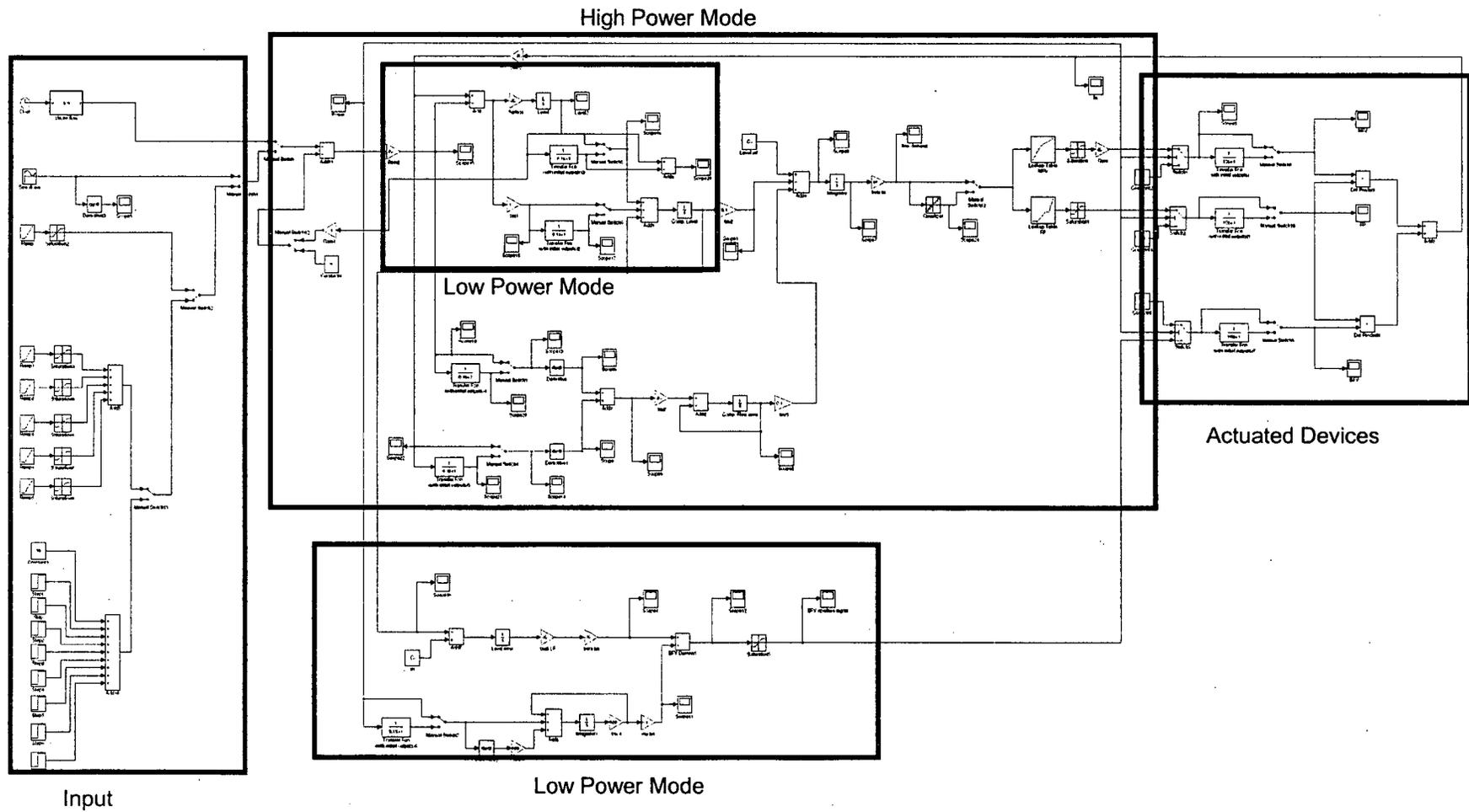


Revision of the Draft NUREG/CR

- The draft has been reviewed by 10 external reviewers from the academia, national and international laboratories and the industry
- Approximately 180 comments have been received
 - Regulatory Issues
 - Benchmark System
 - Data Collection and Generation
 - Dynamic Methodologies and there Practicality
 - Incorporation of Models into PRA
- A comment resolution document has been prepared
- The draft has been revised to incorporate responses to these comments, as well as the responses to comments from the internal reviewers and the ACRS, and is in the final approval process

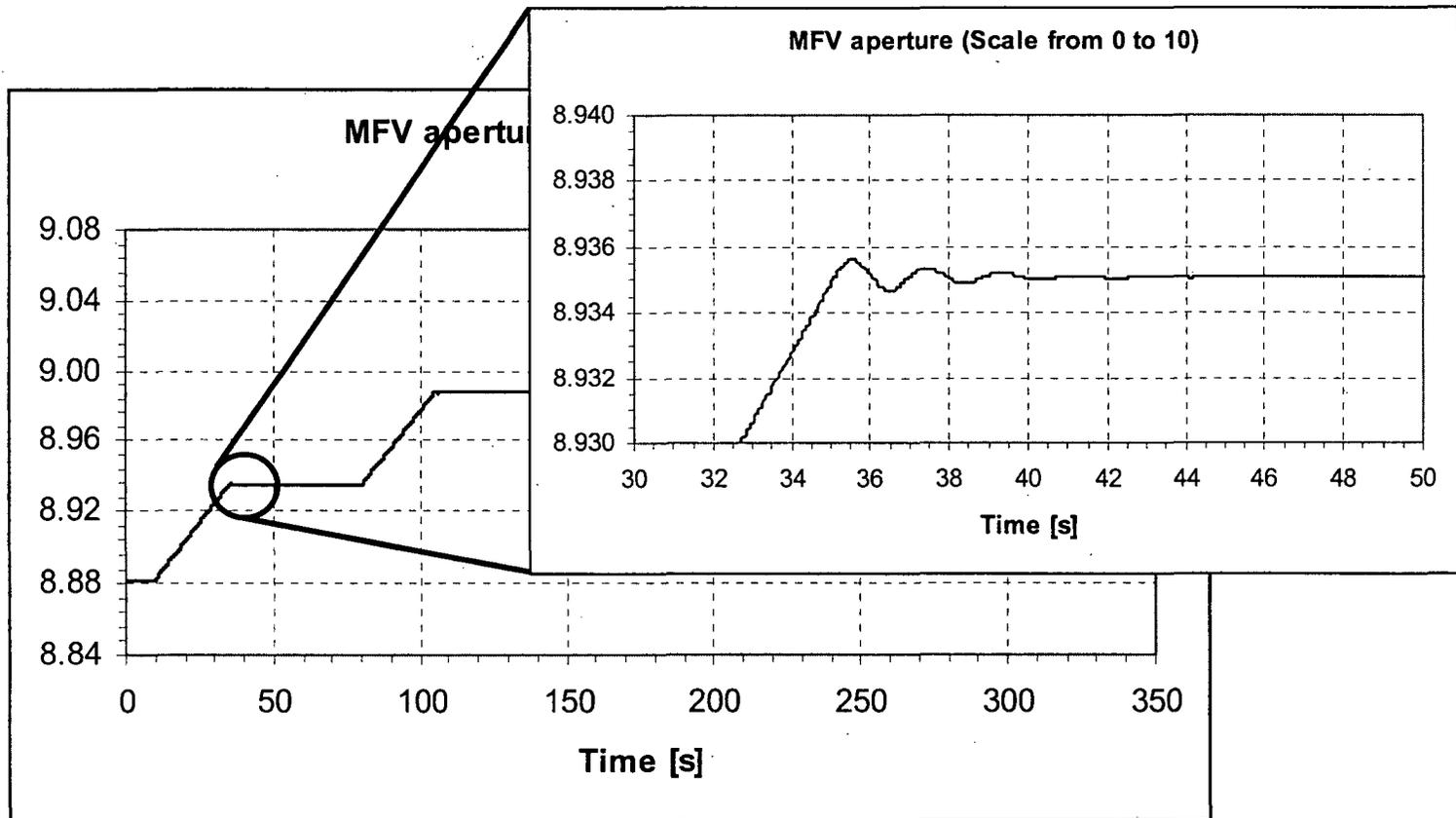


Benchmark System Model



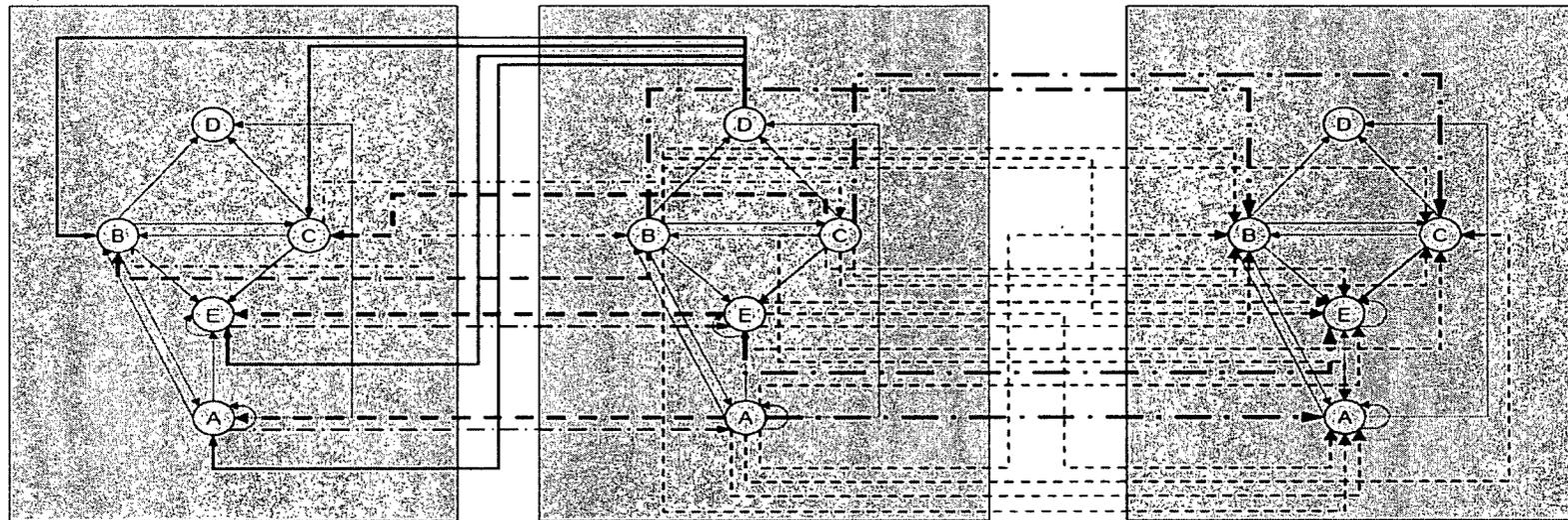


Model Testing





Hardware/Software/Firmware States: Computers



2: Operating with 1 computer, possible recovery

1: Operating w/ 2 computers

3: Operating with 1 computer, no recovery

Computer States

- A: Operating
- B: Loss of one input
- C: Loss of both inputs
- D: Computer down
- E: Arbitrary output

Macro States

- 1: Controller is receiving data from both computers
- 2: Controller is receiving data from 1 computer while the other one can be recovered
- 3: Controller is receiving data from 1 computer while the other one can not be recovered
- Freeze: Controller sends the same data to the valves from the previous time step

-----	Secondary goes down (recoverable)	-----	Primary release control of the process.	-----	Secondary computer watchdog timer trips or loss of output to controller	-----	Common cause sensor failure
-----	Secondary recovers	-----	Primary computer watchdog timer trips or loss of output to controller.	-----	Primary goes down. Secondary unavailable		



Hardware/Software/Firmware States:

Summary

- 5 Pairs of sensors, 2 Computers (MC,BC), MFV Controller, BFV Controller, FP Controller, PDI Controller
- Total of 100, 018, 800 states
- Reduces to 46 080 states by conglomeration into super components
 - Sensors -> MC
 - Sensors -> BC
 - Actuated device (valve, pump) -> controller
 - MC+BC -> Computer
- Reduces to 2250 states by merging states with similar effects on the controlled process (e.g., system is operational whether there is 1 or 2 computers)



Markov/CCMT Methodology

- Extended analysis of failure scenarios for benchmark system to include all possible failure paths
- Added comparison of DFM and Markov/CCMT methodology results to address reviewer's comment
- Addressed reviewers' concern about size of generated dynamic event trees: Branches are terminated if
 - scenario time exceeds system mission time
 - controlled/monitored variables fall outside ranges
 - scenario probability falls below threshold
 - system is restored to its nominal state



Number of Failure/Non-Failure Scenarios for an Example Initiating Event

Time (in seconds) (Depth of DET)	Number of LOW failure scenarios		Number of HIGH failure scenarios		Number of scenarios without failure
	With Process Variables	Configuration Only	With Process Variables	Configuration Only	
1	0 (0.0%)	0	0 (0.0%)	0	243 (100.0%)
2	0 (0.0%)	0	0 (0.0%)	0	1,242 (100.0%)
3	530 (10.8%)	33	0 (0.0%)	0	4,384 (89.2%)
4	1,480 (9.3%)	45	0 (0.0%)	0	14,439 (90.7%)
5	4,999 (10.2%)	46	186 (0.4%)	0	43,727 (89.4%)
6	14,811 (10.2%)	46	2,518 (1.7%)	41	127,292 (88.0%)
7	47,881 (11.5%)	49	6,531 (1.6%)	41	362,153 (86.9%)
8	140,644 (11.9%)	49	18,559 (1.6%)	41	1,022,695 (86.5%)
9	411,240 (12.3%)	49	50,259 (1.5%)	41	2,871,468 (86.2%)
10	1,126,498 (12.0%)	49	143,922 (1.5%)	41	8,091,530 (86.4%)



DFM

- Demonstration of the inductive DFM analysis engine
- Comparison of DFM results with Markov/CCMT results
- Update of the SG simulation package
- Modeling of the full benchmark system



Demonstration of Inductive DFM Analysis Engine

- Inductive DFM analysis can be used to verify intended behavior or to track the effects of possible combinations of component failures on overall system operation / behavior
- Inductive failure and fault analyses were executed for the example initiating event
 - These inductive analyses identified the progression of the system states from different combinations of initial component states
 - Similar to an automated Failure Modes and Effects Analysis (FMEA)
 - One of the initial conditions analyzed corresponds to the failure of the BFV in the stuck position while there is a mismatch between the steam flow and the feed flow (steam flow > feed flow)
 - After tracking through 2 time steps, the inductive analysis showed a low SG level condition
- The results demonstrated the usefulness of the inductive technique. This technique will also be applied to more complicated scenarios for the full benchmark system model



Comparison of DFM Results with Markov/CCMT Results

- An exact comparison of the DFM outputs and Markov/CCMT outputs cannot be performed due to the differences in the output formats
- DFM and Markov/CCMT clearly agree on the high level, summary assessment of the system failure modes
- Application of these two techniques to the benchmark system showed that:
 - The deductive DFM analysis offers a more compact and efficient description of the high-level failure behavior of the system
 - The Markov/CCMT approach can produce the detailed information about all possible failure paths and exact timing of the events
 - The Markov/CCMT approach can also be useful for epistemic uncertainty quantification



Defining The Fault Injection Space

- Faults must be representative of the types of faults that can occur in the system context
 - Hardware: Permanent and transient
 - Common mode: Activation of a hardware fault, that can trigger a SW fault
 - Software: un-initialized pointers and variables, memory leaks, stack overwrites
- The fault injection space is characterized by five parameters
 - Types of faults
 - Location of injection
 - Time of injection
 - Duration of fault
 - System state – operational profile
- These five parameters are controlled by the fault injection experiment.
- Estimation of critical model parameters via fault injection are governed by statistical models
- Coverage (C) is the principle parameter estimated
 - $C = Pr(\text{fault detected and properly handled} \mid \text{fault occurred})$



Use of the Fault Injection Data in The Models

- Construct a list of faults that are known to cause the system to fail in a specific failure mode.
- Find the failure rate λ_{fm} of the device in mode m from operational data or data bases.
- A fault is injected into the system to stimulate a failure mode m .
- The response of the system is measured as the coverage parameter C_{fm} which is the probability that the system detects the failure mode m , given that the fault occurred in device f .
- The non-coverage parameter $(1-C_{fm})$ is then the probability that the system will not detect the fault m in device f so that the fault will propagate through the system. Then $\lambda_{fm}(1-C_{fm})$ is the failure rate of device f in the mode m .
- Since the available failure rate is often irrespective of the failure mode, the frequency of occurrence of any one failure mode from the set of all possible failure modes f_m is less than total failure rate of the device f , and subsequently the approach is conservative.



Statistical Model

- This statistical model supports four specific needs
 - Quantify and characterize the uncertainty of model parameters.
 - Characterize and define the assumptions of model parameters.
 - Statistically estimate based on the assumptions of the model and model parameters the number of observations are required to estimate a parameter to a known confidence level.
 - Calculate the number of fault injection trials in a fault injection campaign required to calculate the coverage estimate of the component
- Statistical fault coverage estimation
 - Number of fault injection trials needed (n) to estimate coverage parameters of the analytical models can be found from

$$n = \frac{\ln(1-\gamma)}{\ln C_1}$$

- To estimate a coverage factor of $C_1 = .99995$ at a $\gamma=0.99$ confidence level requires 92,000 fault injections



Obtaining Hardware (HW) Failure Rate Data

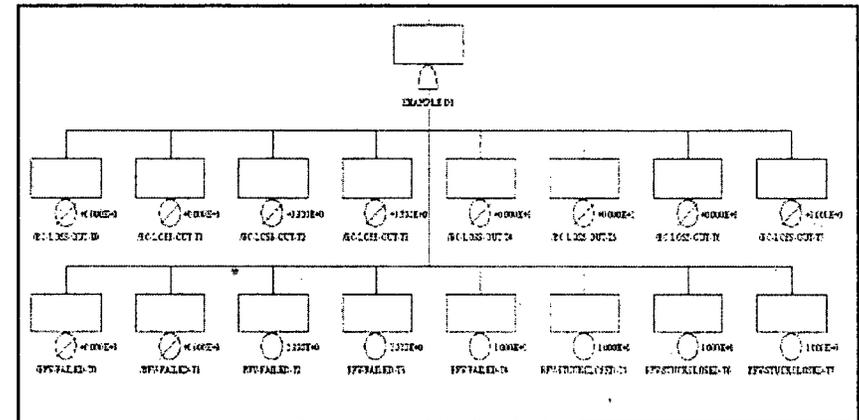
- Our approach to acquiring the hardware failure rate of the components was to use three key pieces of information:
 - Acquire and analyze the actual failure data from the DFWCS
 - Use a commercial failure data base (PRISM, Mil Handbook 217, etc.)
 - Conduct interviews with selected vendors to acquire failure data information
- The HW failure rates were calculated for major components of the benchmark system.



Integrating Dynamic Methodology Results into PRA - A Sample Failure Scenario

Time (s)	System Configuration	Process State	Explanation
t = 0	BFV: OK BC: OK	$-0.17 \leq X_L < 0.17$ $-1.587 \leq E_{LR} < 4.203$ $-100.0 \leq C_{LR} < 100.0$ $0.0 \leq S_{BR} < 30.00$	Both BFV and BC are in their operational state, and all process variables are in their nominal range
t = 1	BFV: OK BC: OK	$-0.17 \leq X_L < 0.17$ $4.203 \leq E_{LR} \leq 1000.0$ $-100.0 \leq C_{LR} < 100.0$ $70.0 \leq S_{BR} \leq 100.0$	Level error is high, so BFV opens more
t = 2	BFV: ARB/OUT BC: OK	$0.17 \leq X_L < 2.5$ $4.203 \leq E_{LR} \leq 1000.0$ $-100.0 \leq C_{LR} < 100.0$ $0.0 \leq S_{BR} < 30.0$	BFV controller fails and starts generating arbitrary outputs to the valve, in this case a low value. The level is higher than the nominal level interval.
t = 3	BFV: ARB/OUT BC: OK	$-2.0 \leq X_L < -0.17$ $4.203 \leq E_{LR} \leq 1000.0$ $-100.0 \leq C_{LR} < 100.0$ $70.0 \leq S_{BR} \leq 100.0$	BFV controller is still generating arbitrary outputs, in this case a high value. The level is lower than the nominal level interval.
t = 4	BFV: ARB/OUT BC: OK	$0.17 \leq X_L < 2.5$ $4.203 \leq E_{LR} \leq 1000.0$ $-100.0 \leq C_{LR} < 100.0$ $0.0 \leq S_{BR} < 30.0$	BFV controller is still generating arbitrary outputs, in this case a low value. The level is higher than the nominal level interval.
t = 5	BFV: ZYDC/OUT BC: OK	$-2.0 \leq X_L < -0.17$ $4.203 \leq E_{LR} \leq 1000.0$ $-100.0 \leq C_{LR} < 100.0$ $0.0 \leq S_{BR} < 30.0$	Communication between the BFV controller and the valve is lost; this effectively tells the valve to close completely, and the level is already lower than the nominal level interval
t = 6	BFV: ZYDC/OUT BC: OK	$-2.0 \leq X_L < -0.17$ $4.203 \leq E_{LR} \leq 1000.0$ $-500.0 \leq C_{LR} < -100.0$ $0.0 \leq S_{BR} < 30.0$	The valve remains closed and the level keeps decreasing
t = 7	BFV: ZYDC/OUT BC: OK	$X_L < -2.00$ (LOW) $4.203 \leq E_{LR} \leq 1000.0$ $-500.0 \leq C_{LR} < -100.0$ $0.0 \leq S_{BR} < 30.0$	The level falls below the LOW setpoint and the system fails

=



This failure scenario has been formatted and inserted into SAPHIRE where it can be linked with the plant PRA



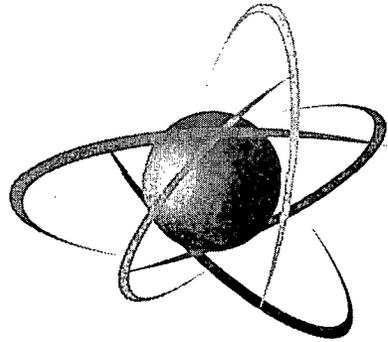
Summary and Conclusion

- The NUREG/CR-XXXX draft titled “*Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments*” has been revised per reviewer comments and is in the final approval process.
- A model for the first benchmark system has been developed and satisfactory tested for steady-state as well as transient conditions
- A discrete state model has been developed based on FMEA and expected data availability
- The DFM and Markov/CCMT results have compared and resolved for an example initiating event of the benchmark system
- Preliminary results of failure data estimation trials have been obtained
- A methodology has been developed to incorporate Markov/CCMT and DFM results into an existing plant PRA



Next Steps

- A standalone reliability modeling of the benchmark system using the DFM and Markov/CCMT methodology
- Qualitative comparison of the event combinations that lead to the benchmark system failure as obtained by the DFM and the Markov/CCMT methodology
- Quantitative evaluation of the models using data obtained through the fault injection procedure, as well as other means (e.g. field data, data libraries)
- Incorporation of models into an existing PRA for selected initiating events (e.g. turbine trip, station blackout, loss of main feedwater)
- Detailed specification of the second benchmark problem reflecting the properties of the reactor protection system
- Performing analyses for the new benchmark problem



U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

**Digital I&C
Risk Task Working Group (TWG)
Short Term Task**

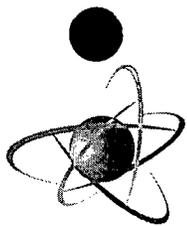
April 18, 2007

Cliff K. Douth
PRA Licensing Branch
Division of Risk Assessment,
Office of Nuclear Reactor Regulation

- Background
- Problem Statements
- Goals
- Project Plan
- Deliverables
- Approach
- Application of PRA (Digital Systems)
- Digital I&C PRA Insights
- Challenges
- Schedule
- Conclusion

The NRC and industry currently use a deterministic approach that relies on:

- Specific digital I&C system development, design, testing, maintenance, and staff review processes
- Process is intended to ensure adequate quality, reliability, and diversity and defense-in-depth when implementing a digital I&C system.
- Staff Requirements dated December 6, 2006 Identified risk-informing as a topic for deployment of digital I&C



Risk TWG - Short Term Task

1. Existing guidance does not provide sufficient clarity on how to use current methods to properly model digital systems in PRAs for design certification applications or license applications (COL) under Part 52.
2. Using current methods for PRAs, NRC has not determined how or if risk-insights can be used to assist in the resolution of specific key digital system issues in operating reactor licensing action requests.

Risk TWG - Long Term Task

3. An acceptable state-of-the-art method for detailed modeling of digital systems has not been established. An advancement in the state-of-the-art is needed to permit a comprehensive risk-informed decision making framework in licensing reviews of digital systems for current and future reactors

RISK TWG GOALS

- Improve the NRC review process
- Improve insight into vulnerabilities (including diversity and defense-in-depth)
- Provide interim guidance on the use of current PRA methods in modeling digital systems (design certification and COL applications)
- Provide an interim approach for the use of risk insights in licensing reviews

- Industry Technical Papers – methods and lessons learned
- Staff PRA risk insights, key principles, and methods
- Research (Wide Focus)
- Other TWG recommendations

For Problem Statement 1:

- Issue interim guidance addressing use of current methods in modeling of digital systems for design certification and COL application PRAs
- In the longer term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.)

For Problem Statement 2:

- Develop, if possible, an acceptable approach for using risk insights in licensing reviews of digital systems, including consideration of proposed industry methods.
- If an acceptable approach can be established, issue interim guidance and acceptance criteria for use of risk insights in licensing reviews of digital systems.
- In the longer term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.)

Risk TWG Ground Rules - Short term Task:

- SRM to SECY 93-087
- Commission Policy Statement on PRA
- Commission Safety Goals
- Current Methodology (FT/ET)
- Review process

RG 1.174 and 1.177

- Risk Informed Decisionmaking

Non-Risk-Informed Applications

- Operating Reactors – To date, risk insights have not been incorporated into digital I&C system licensing submittals by either staff or industry
- New Reactors – Some have included digital systems (software CCF) and/or performed uncertainty, importance, and sensitivity studies of digital systems including software
- Other

- Uncertainty, sensitivity and importance studies show importance of diversity (diverse actuation functions) in reducing the impact of uncertainties associated with digital systems (i.e., software failure probabilities) on PRA conclusions/insights when implementing digital I&C systems
- Standard fault tree/event tree methods
- Level of detail to circuit board level
- Failure modes identified at the circuit board level
- Hardware failure data derived from proprietary or generic databases
- Common cause failures (CCF) of hardware considered boards and boards across systems
- Software CCF considered for individual modules and across multiple modules

- Software Reliability
- Common Cause Failures (including software)
- Hardware/Software Interactions
- Modeling
- Failure Modes – Including unknown or unforeseen Failure Modes
- Failure Data
- Human Reliability –
Updates/Interfaces/Manual Actions
- Interfacing a digital system into a PRA
- Diagnostics/Fault Tolerance/Coverage

- Low Probability but credible event
- Time Dependencies
- External Initiating Events (Fire)
- Review Process
- Acceptance Guidelines
- PRA Quality – Attributes for digital system Implementation
- Policy Issues
 - Use of PRA with a deterministic defense-in-depth philosophy/methodology
- Consistent with current regulations/guidance

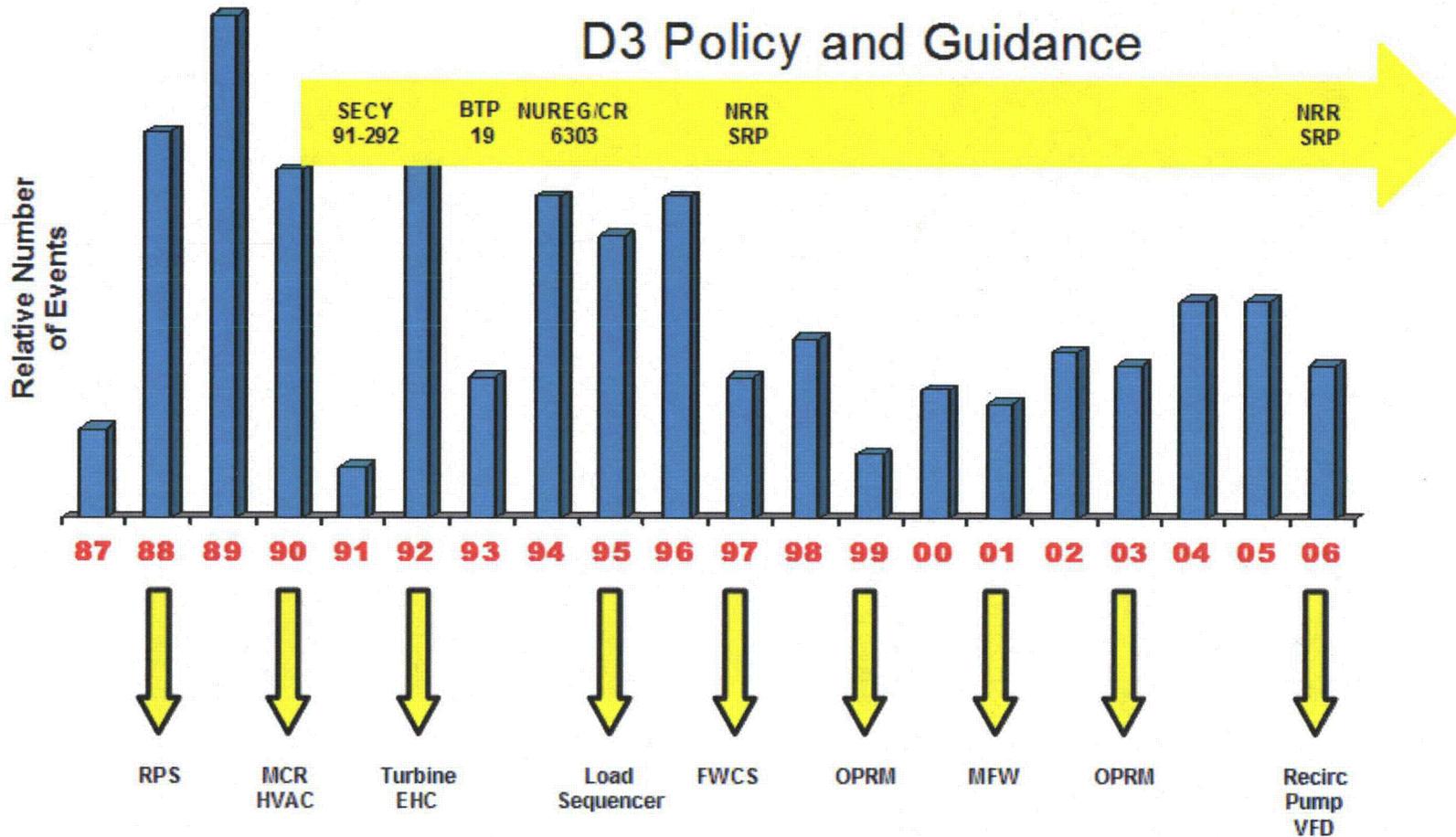
- Timeline – TBD
 - As part of providing comments on the draft Project Plan, it is critical that industry include priorities for resolution, and requested target dates for completion.
- The update of regulatory guidance (SRP and Regulatory Guides, etc.) are Long Term.

- Provide interim guidance on the use of current PRA methods in modeling digital systems (design certification and COL applications)
- Provide an interim approach for the use of risk insights in operating reactor licensing reviews

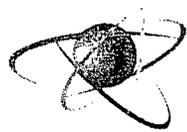
However:

- The incorporation of PRA in digital system reviews presents significant challenges.
- But there may be advantages in using risk insights in digital system reviews including improved identification of vulnerabilities including diversity and defense-in-depth assessments

Historical Perspective



While the U.S. nuclear industry has an excellent safety record, digital system failures and upsets have been reported.



U.S.NRC

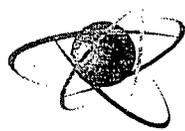
UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

DIVERSITY AND DEFENSE-IN-DEPTH RESEARCH

April 18, 2007

**Michael E. Waterman
Instrumentation and Electrical Engineering Branch
Division of Fuel, Engineering, and Radiological Research,
Office of Nuclear Regulatory Research**



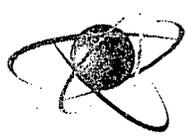
U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

INTRODUCTION

- **Issue**
- **Background**
- **Research approach and schedule**
- **Preliminary results**



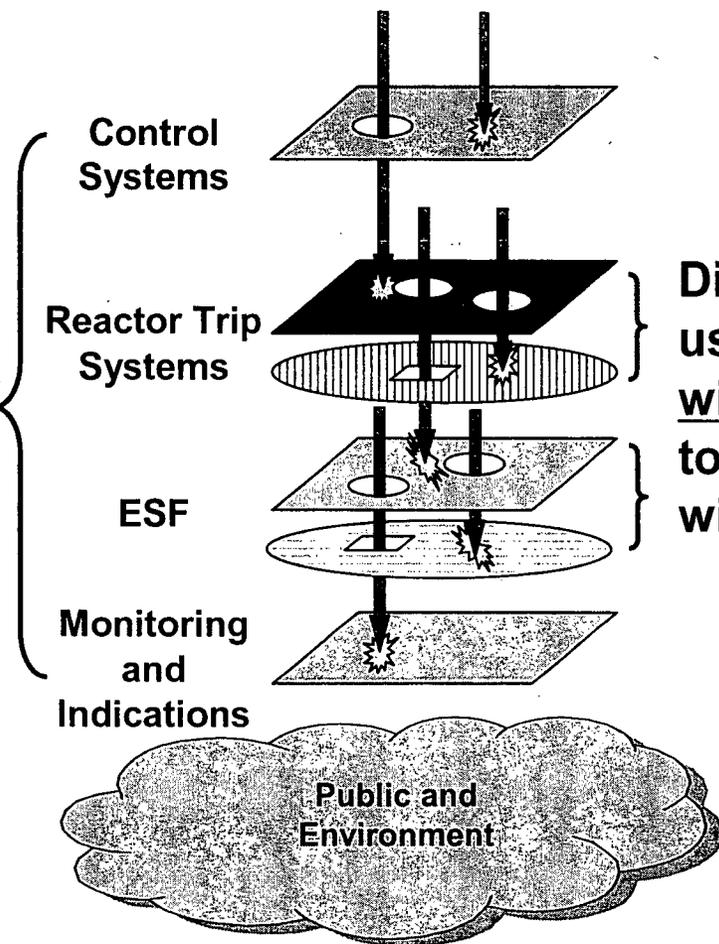
- **Adding diverse systems and/or defense-in-depth features can mitigate the effects of a common cause failure (CCF)**
- **How much diversity and defense-in-depth are enough? For example**
 - **Are there precedents for good engineering practice?**
 - **Can sets of attributes provide adequate diversity?**
 - **Are there standards that can be endorsed?**

- **Diversity and defense-in-depth (D3) policy established in 1990's**
- **Experience to date indicates the need for more specific guidance for assuring adequate diversity and defense-in-depth**
- **Research on diversity strategies started in late FY 06**
- **Preliminary results are now available**

DIVERSITY AND DEFENSE-IN-DEPTH

Hazardous Condition(s)

Defense-in-Depth is a strategy that uses different functional barriers to compensate for failures in other barriers.



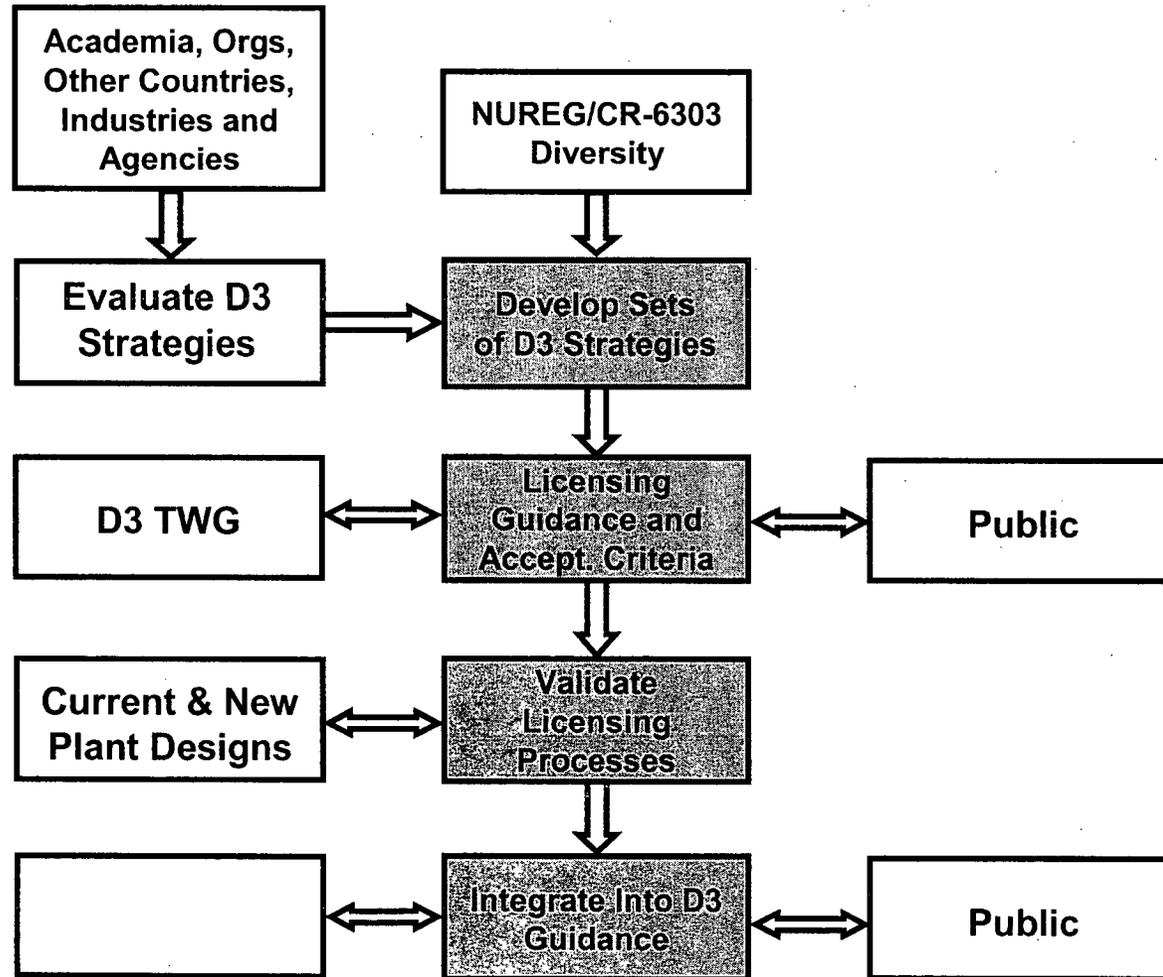
Diversity is a strategy that uses different means within a functional barrier to compensate for failures within the same barrier.

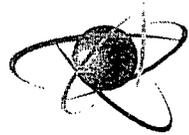


OVERALL DIVERSITY APPROACHES

- **Avoidance**
 - Produce high-quality (error-free) systems
 - Minimize common elements
 - Limit fault propagation
- **Mitigation**
 - Add defense-in-depth to compensate for failures in other systems
 - Provide diverse systems that will not fail at the same time

RESEARCH APPROACH

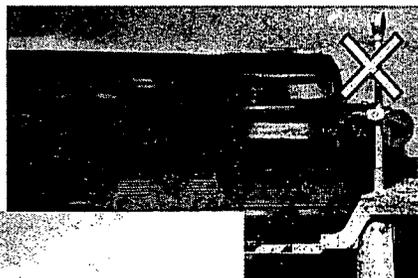




- **Identify diversity strategies**
 - Evaluate diversity attribute strategies used by other countries, industries, and agencies and recommendations from academia and scientific organizations – May 2007 (Draft)
- **Draft licensing guidance**
 - Refine attribute strategies – July 2007
- **Validate results**
 - Use nuclear industry applications to validate guidance – August 2007
- **Propose NRC guidance**
 - Integrate research into diversity guidance – September 2007

SOURCES OF INFORMATION

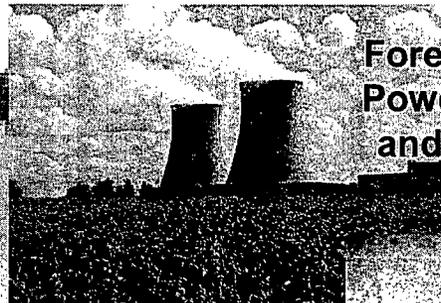
Federal Railroad Administration



Federal Aviation Administration



Foreign Nuclear Power Agencies and Licensees



Chemical Industry



Academy of Sciences Organization

Department of Defense



Power grids & Petrochemical power grids

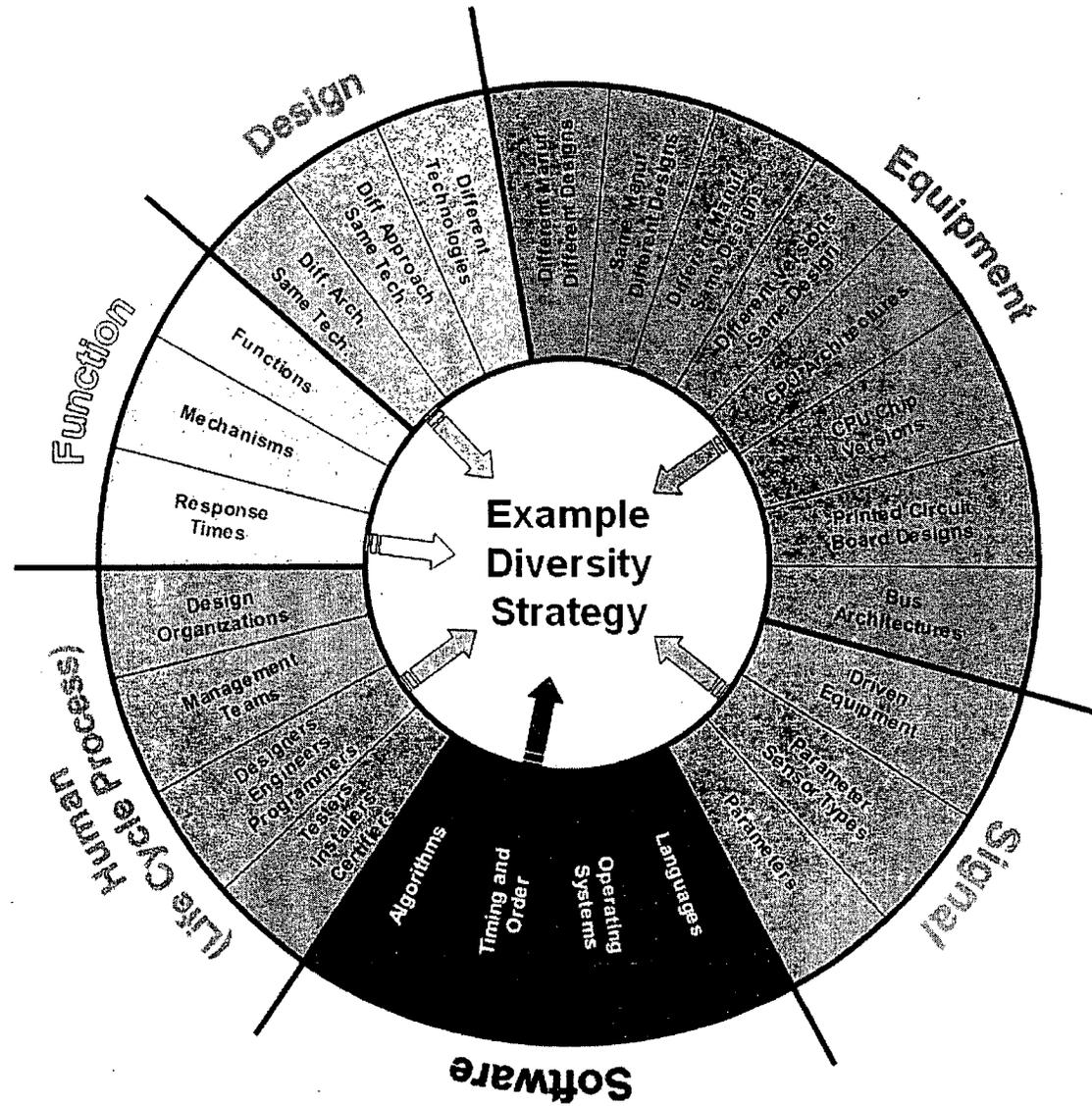


National Aeronautics and Space Administration



- **Evaluate system diversity strategy recommendations from academia and the scientific community, and diversity approaches used by other countries, industries, and agencies**
- **Use the recommendations and approaches to develop diversity attribute criteria strategies**

DIVERSITY ATTRIBUTES AND CRITERIA



SUMMARY OF DIVERSITY STRATEGIES

	Space Shuttle	Space Station	Mission Control JSC	FAA Flight Control System	Airbus A320	Boeing 777	DoD Battlefield	Electrical Grids	Chemical Industry
Design				Shaded	Shaded				Hatched
Equipment		Shaded		Shaded	Shaded	Shaded			Hatched
Function	Shaded	Shaded		Shaded	Shaded	Shaded	Shaded		Shaded
L.C. Process	Shaded	Shaded	Shaded	Shaded	Shaded	Shaded	Shaded	Shaded	Hatched
Signal									Hatched
Software	Shaded		Shaded	Shaded	Shaded	Shaded			Hatched

* Strategies may not be industry-wide

SUMMARY OF DIVERSITY STRATEGIES*

	Sizewell B UK	Temelin Czech	Dukovany Czech	Ringhals Sweden	Beznau Switz.	Chooz-b France	Darlington Canada	Paks Hungary	Lungmen Taiwan
Design	Shaded		Shaded	Shaded			Shaded		
Equipment	Shaded	Shaded		Shaded		Shaded	Shaded		Shaded
Function	Shaded	Shaded	Shaded	Shaded	Shaded	Shaded	Shaded	Shaded	
L. C. Process	Shaded	Shaded				Shaded	Shaded		Shaded
Signal	Shaded								
Software		Shaded		Shaded		Shaded	Shaded		Shaded

* Preliminary information



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

SUPPLEMENTAL INFORMATION

SPACE SHUTTLE

Diversity Attribute	Description
Design	Requirements specify fault-tolerance with consideration of common mode failures
Equipment	Six identical IBM AP-101 general purpose computers (GPCs) (five in use; one spare); therefore, no equipment diversity Time-shared computer data bus network
Functional	The four Primary Avionics Software System (PASS) GPCs contain identical software; the Backup Flight System (BFS) GPC contains a reduced software package written by a different vendor ("take me home")
LC Process	Astronauts carry a manual called <i>Program Notes and Waivers</i> that details software idiosyncrasies and describes unworkable anomalies (that is, bugs) (manual can be up to 200 pages); Astronauts make all final decisions (except during launch and ascent when control is fully autonomous)
Signal	All five GPCs receive the same data from the same sensors; therefore, no signal diversity
Software	The PASS software was written in HAL/S (high order assembly language/Shuttle) by IBM The BFS software was written in HAL/S by Rockwell

Diversity Attribute	Description
Design	Requirements specify fault-tolerance with consideration of common mode failures; the command and control computers use the same technology with the same architecture; therefore, no design diversity
Equipment	The three command and control computers (Tier 1) use identical 80386 processors. The five system control computers (Tier 2) are also identical. The computers that run individual devices (Tier 3) are all different. Thus, at the lowest level, the equipment is diverse
Functional	At Tier 1, identical inputs to identical computers running identical software are expected to produce identical results. Tier 2 computers can assume command for their specific functions given the failure of Tier 1 computers. Tier 2 computers also have a "save the day" reduced functionality program to load on to the Tier 1 computers
LC Process	The hardware and software are COTS, therefore no human diversity (i.e., same company, designers, and programmers) at this level. However, ISS crew and MCC operators can override control computers and provide uploads
Signal	No redundancy at the signal level because all values are shared
Software	The computer hardware and software are COTS with minimal changes, therefore no software diversity (i.e., same company and same programmers)

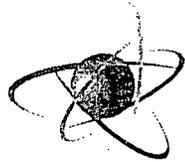
Diversity Attribute	Description
Design	Requirements specify fault-tolerance with consideration of common mode failures. The computers are connected by fiber optic lines to a network and are considered to be peripherals to the network
Equipment	197 work stations are interconnected via a LAN that can be used to control both the Space Shuttle in flight and the ISS. Maintenance is performed by replacing a workstation in its entirety
Functional	The same functions and mechanisms are used for each computer connected to the network
LC Process	The flight controllers are the primary mechanism for detection of malfunctions and attempts to resolve them and double-check every number; handsets and instant messaging keeps all controllers in contact with each other
Signal	The same signals are shared between computers via a LAN; therefore, no signal diversity
Software	The flight control software is COTS with minimal changes for unique flight control tasks; however, the flight controller support teams perform calculations using other computers, software, and paper and pencil to provide backup to the flight controllers

Diversity Attribute	Description
<i>Design</i>	<p>Substantial differences between the designs in terms of the means to prevent the top level failure condition.</p> <p>An analysis should substantiate the dissimilarity and independence of: implementation, requirements, algorithms, data, environment, and other potential sources of design error.</p>
<i>Equipment</i>	<p>The technology through which the designs are implemented must be different.</p>
<i>Functional</i>	<p>The operations through which the function is used must be diverse.</p> <p>Both the primary and secondary systems can execute full time, or the secondary system can be a "hot spare" that is reverted to after failure of the primary portion.</p>
<i>LC Process</i>	<p>The methodology by which the designs are created must be different.</p>
<i>Signal</i>	<p>No discussion of requirement for diverse signals other than the functional attribute requirement.</p>
<i>Software</i>	<p>Validation of any assumptions of independence must demonstrate compliance.</p>

AIRBUS 320 AVIONICS

Diversity Attribute	Description
<i>Design</i>	Same requirements were used for all teams, otherwise the detailed design was independent.
<i>Equipment</i>	Channels used different processors (Intel 80186 and Motorola M68000).
<i>Functional</i>	Voting logic was different in each computer. Each flight command channel was monitored by another system which detected faults in that command channel.
<i>LC Process</i>	Employed different teams of developers for different parts, with particular care in keeping them independent.
<i>Signal</i>	No diversity was noted.
<i>Software</i>	Independent software development teams. Different languages used to implement the control channel and the monitor of that control channel. Different compilers used by different teams.

Diversity Attribute	Description
Design	Not used due to perceived expense of development and maintenance.
Equipment	Diverse equipment if manufactured without Boeing's oversight & control, manufactured using different technologies. Channels used different processors.
Functional	Upon loss of sufficient signals to fully control the plane, the system reverts to a simpler "pilot assist" mode.
LC Process	Employed developers with different backgrounds and training.
Signal	No diversity was noted. Signals are cross-validated between channels.
Software	Different Ada compilers used for each of 3 channels (same source code). Formal methods of specification and verification used in some critical and simple algorithms (other attempts to use provided no useful result).



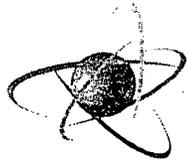
Diversity Attribute	Description
Design	No requirement or prescription of any form of defense in depth or diversity Reach-back to higher echelons for diversity; decision making, communications, etc
Equipment	Size, weight and power constraints severely limit redundant or diverse equipment on the same platform/system in-the-field Rigorous IV&V protocols, testing and field demonstrations
Functional	Overlap in multi-system performance (e.g. rockets, bullets, bombs, different radios and different frequencies for same and different purposes) Overlap in effects (e.g. IR imaging to detect humans, Radar and foliage penetration to detect people) Communications redundancy with detailed frequency management
LC Process	All fielded systems include human-in-the-loop as fail safe and recovery agent Specialties overlap and teams are designed for cross-training
Signal	Frequencies are the same for same tasks and functions, refined frequency management spans the range of ~25 Hz to ~10 ¹⁵ Hz
Software	Fine communications network management for fault tolerance & optimal band-width Refined Modeling & Simulation for digital systems software performance, testing, etc. Careful & detailed Inter- & Intra-Systems compatibilities for sharing, redundancy, etc



ELECTRICAL GRID

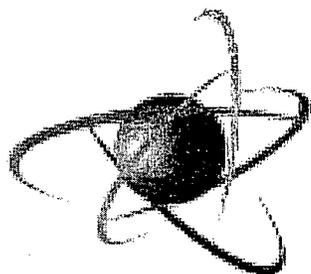
Diversity Attribute	Description
Design	Microprocessor-based digital protection relays provide over-current protection. Common design used within individual organizations for economic reasons.
Equipment	<p>ASIC technology using System-on-Chip hardware avoids use of distributed components to increase reliability.</p> <p>Ethernet network for SCADA interaction. Settings are remotely programmable and data is transferred to control centers</p>
Functional	Identical relays deployed at branching points; therefore, no equipment diversity. The underlying mechanisms, purpose, and function are the same for each unit. Trip settings and response times for backup units set to trip after primary protection relay has had time to respond.
LC Process	<p>Protective function firmware verified independently</p> <p>Geographically distributed diverse maintenance organizations</p>
Signal	Units in series perform identical function on common signal with redundant sensor set
Software	No diversity.

Diversity Attribute	Description
<u>Design*</u>	CCPS recognizes use of diverse hardware, system software, and application programs can combine to minimize common mode faults.
<u>Equipment</u>	CCPS recognizes the potential value of using different computational hardware to perform the same safety function.
<i>Functional</i>	The goals of the basic control system and primary safety system are different. This is a recommended attribute for safe automation of chemical processes.
<u>LC Process</u>	CCPS recognizes that increased diversity and improved safety can result from diverse design and maintenance teams.
<u>Signal</u>	CCPS indicates that diverse measurements of the same process whether directly through a diverse sensor or indirectly through a process model is a significant diversity mechanism
<u>Software</u>	CCPS recognizes that diverse software between the control and each layer of the safety systems provides additional protection against common mode failures.



INTERNATIONAL REACTOR DIVERSITY STRATEGIES

Plant	NPP Vendor	Primary DPS Vendor	Voting logic	Licensing basis				
Sizewell B	<u>W</u>	<u>W</u>	2-oo-4	Risk*				
Temelin	VVER	<u>W</u>	2-oo-3	SF**				
Ringhals	Framatome	<u>W</u>	2-oo-4	SF				
Dukovnay	VVER	Fram.	2-oo-3	SF				
Beznau	<u>W</u>	Fram.	2-oo-4	SF				
Chooz-b	Framatome	Fram.	2-oo-4	SF				
Darlington	AECL	AECL	2-oo-3	SF				
Paks	VVER	Siemens	2-oo-4	SF				
*Risk-based licensing means the safety case is based on probabilistic safety assessment (=PRA)								
**SF means that there is no identified single failure in hardware or design which could prevent the protection function								



U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

**NRC ACTIVITIES TO ADDRESS
SHORT TERM
DIVERSITY AND DEFENSE-IN-DEPTH
ISSUES**

Gene Eagle

Instrumentation, Control, and Electrical Engineering Branch

Division of Engineering

Office of New Reactors

4/17/2007

1

- Overview
- Problem Statements
- Deliverables
- Conclusions



OVERVIEW

- Diversity and Defense-in-Depth Task Working Group (TWG)
- Basis for diversity and defense-in-depth present in regulatory requirements
- Guidance currently in place and workable for NRC staff review of diversity and defense-in-depth
- Guidance used for design certifications
- Advances in technology: industry desire for clearer and more detailed guidance



PROBLEM STATEMENTS

Overall Issue:

Nuclear industry and NRC guidance does not explicitly identify what constitutes acceptable diversity and defense-in-depth in nuclear facility safety system designs.

Specific Statements:

1. Adequate Diversity – Additional clarity is desired on what constitutes adequate diversity and defense-in-depth
2. Manual Operator Actions – Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action time
3. Credit for Leak Detection – Additional clarity is desired for crediting leak detection as part of a diversity and defense-in-depth coping strategy



continuation of **PROBLEM STATEMENTS**

4. BTP-19 Position 4 Challenges – Industry has proposed that further clarification is needed relative to when and if credit can be taken for component-level verses system-level actuation of equipment
5. Effects of Common-Cause Failure (CCF) – Additional clarity is desired regarding the effects that should be considered (e.g., fails to actuate and/or spurious actuation)
6. Common-Cause Failure Applicability – Clarification is desired on identification of design attributes that are sufficient to eliminate consideration of CCFs (e.g., degree of simplicity)



continuation of **PROBLEM STATEMENTS**

7. Echelons of Defense – Additional clarification is desired regarding how the echelons of defense for maintaining the safety functions should factor into diversity and defense-in-depth analyses
8. Single Failure – Additional clarification is needed regarding the acceptance criteria for addressing CCFs versus the acceptance criteria for addressing single failures in safety system designs



DELIVERABLES

Near Term

- Issuance of interim guidance (e.g., Regulatory Issue Summary) describing the results of the diversity and defense-in-depth TWG activities
- Goal: to deliver additional guidance to enhance efficiency and effectiveness in handling safety issues and schedules for simulators

Long Term

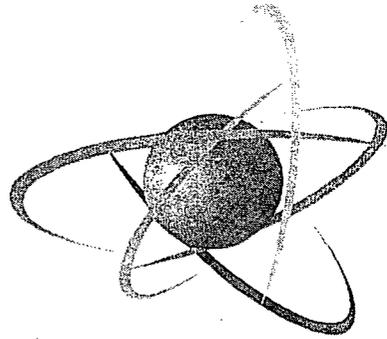
- Updates to staff guidance documents (e.g., Standard Review Plan)
- Implementation of other TWG recommendations (e.g., policy changes)

CONCLUSIONS

- Regulatory basis for and staff guidance on diversity and defense-in-depth are in place for new reactor submittals
- Additional details, flexibility, and clarification are needed in some areas as technology has advanced
- The staff, in principal, is in agreement with industry in advocating the use of digital computer based I&C with the potential of providing greater safety; the challenge is in the details
- NRC and nuclear industry continue to work closely to resolve identified problems
- Goal is to deliver additional guidance to enhance efficiency and effectiveness in handling safety issues and schedules for simulators



QUESTIONS?



U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Current Regulatory Position on Diversity and Defense-in-Depth for Digital Safety Systems

ACRS Presentation - April 18, 2007

Paul J. Loeser
Instrumentation and Controls Branch
Division of Engineering
Office of Nuclear Reactor Regulation

SAFETY CONCERN

- **The concern is that an error in common software could cause all channels of all protection systems where this software is used to malfunction.**
 - **Consolidation of many safety functions into a single four channel system has increased the concern.**
- **High-quality design is still considered the most important method to defend against potential common-cause failures. High-quality software and hardware reduce the failure probability.**
- **Despite high quality of design and use of defensive design measures, software errors may still defeat safety functions in redundant, safety-related channels.**

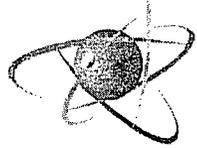


SAFETY CONCERN

(CONTINUED)

- **This was confirmed by the 1997 National Academy of Science report “Digital Instrumentation And Control Systems In Nuclear Power Plants: Safety And Reliability Issues.”**
 - **The NAS study concluded that: “The USNRC position of assuming that common-mode software failure could occur is credible, conforms to engineering practice, and should be retained.”**
 - **The NAS study recommended that:**
 - 1. The USNRC should retain its position of assuming that common-mode software failure is credible.**
 - 2. The USNRC should maintain its basic position regarding the need for diversity in digital I&C systems as stated in the draft branch technical position, Digital Instrumentation and Control Systems in Advanced Plants, and its counterpart for existing plants.**

-
- **Basis for Diversity and Defense-in-Depth**
 - **10 CFR 50.55a(h), "Protection and Safety Systems,"**
 - **10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram"**
 - **10 CFR Part 50, Appendix A, General Design Criterion**
 - **GDC 21, "Protection Systems Reliability and Testability"**
 - **GDC 22, "Protection System Independence"**
 - **GDC 24, "Separation of Protection and Control Systems"**
 - **GDC 29, "Protection Against Anticipated Operational Occurrences"**



POLICY FROM SECY 93-087

-
- **NRC has established the following four-point position for common mode failures in digital I&C systems. This was originally in SECY 93-087 dated April 2, 1993 and was modified by the SRM dated July 21, 1993:**
 - 1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.**
 - 2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.**



POLICY FROM SECY 93-087

(Continued)

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.



POLICY FROM SECY 93-087

(Continued)

- **Regarding the application to digital modifications at operating reactors, at the time this policy was made, it was thought that operating reactors would replace one analog system with a digital system.**
 - **Each digital system would perform only one safety function.**
 - **Other analog based safety functions would still be available.**
 - **The D3 analysis would show that other safety functions would mitigate an accident or transient, i.e., if the level trip did not function, the pressure trip would.**
- **Current digital upgrades are for many or all safety functions being performed by the same digital system.**
 - **Diverse analog systems are no longer available.**
 - **The D3 analysis often shows that diversity is required due to CCF possibility.**
 - **This leads to the question of how diverse must the diverse system be?**



STAFF REQUIREMENTS MEMORANDUM

- The primary differences between the SECY and the SRM deals with common cause software failures. The SRM stated:

“First, inasmuch as common mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis.”

- The result of CCF being beyond design basis is that:
 - The diverse or different function required in the third point may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions .
 - The displays and controls required by the fourth point do not need to be safety grade.

- **The current policy is that the applicant/licensee should perform a Diversity and Defense-in-Depth assessment of the proposed digital I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.**
 - **In this assessment, the applicant/licensee should analyze design basis events (as identified in the SAR).**
 - **If a postulated common-cause failure could disable a safety function that is required to respond to the design basis event being analyzed, a diverse means of effective response (with documented basis) is necessary.**
 - **The diverse means may be a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.**
- **Method for performing Diversity and Defense-in-Depth Assessment is contained in NUREG/CR 6303, December 1994**

- **Diversity Analysis**
 - **The two systems should be compared considering each diversity attribute.**
 - **Design diversity**
 - **Equipment diversity**
 - **Functional diversity**
 - **Human (life cycle process) diversity**
 - **Signal diversity**
 - **Software diversity**
 - **The combined assessment should be used to present an argument that the one is either diverse or not diverse from the other.**
 - **The basis for claiming that a particular combination of diversity attributes constitutes sufficient diversity should be documented.**



ACCEPTANCE CRITERIA CONTAINED IN BTP-19

-
- **For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-cause failure, the analysis using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary.**
 - **For each postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure, the analysis using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).**



ACCEPTANCE CRITERIA CONTAINED IN BTP-19

- **If failure of a common element or signal source shared by the control system and RTS is postulated and the CCF can requires a reactor trip and also impair that trip function, than diverse means should be provided to perform the safety function. The diverse means should assure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary.**
- **No failure of monitoring or display systems should influence the functioning of the RTS or ESFAS.**
- **The adequacy of the diversity provided with respect to the above criteria must be justified.**