

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (not applicable)

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005

SISP REVIEW COMPLETE

Location: Rockville, Maryland

Date: Wednesday, June 15, 2005

Work Order No.: NRC-461

Pages 1-195

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

TRM

DISCLAIMER

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

June 15, 2005

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on June 15, 2005, as reported herein, is a record of the discussions recorded at the meeting held on the above date.

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

1 UNITED STATES OF AMERICA
2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

5 DIGITAL INSTRUMENTATION AND
6 CONTROL SYSTEMS SUBCOMMITTEE

7 + + + + +

8 WEDNESDAY, JUNE 15, 2005

9 ROCKVILLE, MARYLAND

10 + + + + +

11 The Subcommittee met at the Nuclear
12 Regulatory Commission, Two White Flint North, Room
13 T2B1, 11545 Rockville Pike, at 1:30 p.m., George E.
14 Apostolakis, Chairman, presiding.

15 COMMITTEE MEMBERS:

16 GEORGE E. APOSTOLAKIS, Chairman

17 MARIO V. BONACA, Member

18 THOMAS S. KRESS, Member

19 ACRS STAFF PRESENT:

20 MICHAEL R. SNODDERLY

21 ERIC A. THORNSBURY

22
23
24
25
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 NRC STAFF PRESENT:

2 STEVEN A. ARNDT, RES

3 HOSSEIN HAMZEHEE, RES

4 TODD HILSMEIER, RES

5 WILLIAM E. KEMPER, RES

6 MICHAEL E. WATERMAN, SR., RES

7

8 ALSO PRESENT:

9 TUNC ALDEMIR, Ohio State University

10 TSONG-LUN CHU, Brookhaven National Laboratory

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

	<u>AGENDA ITEM</u>	<u>PAGE</u>
1		
2	<u>OPENING REMARKS:</u>	
3	George Apostolakis	4
4	<u>SOFTWARE QUALITY ASSURANCE:</u>	
5	William Kemper	5
6	Steve Arndt	6
7	Hossein Hamzehee	7
8	Todd Hilsmeier	22
9	<u>AUDIENCE COMMENTS:</u>	63
10	<u>INVESTIGATION OF DIGITAL SYSTEM FAILURE/ASSESSMENT</u>	
11	<u>METHODS/RISK CHARACTERISTICS & RELIABILITY ASSESSMENT:</u>	
12	Steve Arndt	78
13	Tunc Aldemir	84
14	<u>NSIR:</u>	
15	Scott Morris	175
16	<u>BOARD MEMBER COMMENTS:</u>	186
17	<u>ADJOURN:</u>	
18	George Apostolakis	195
19		
20		
21		
22		
23		
24		
25		

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

1:31 p.m.

CHAIRMAN APOSTOLAKIS: This is the second day of the meeting of the Advisory Committee on Reactor Safeguards on Digital Instrumentation and Control Systems. I'm George Apostolakis, Chairman of the Subcommittee. Members in attendance are Mario Bonaca and Tom Kress.

The purpose of this meeting is to discuss the NRC staff's draft Digital Systems Research Plan and two specific research programs discussed in the plan: Software Quality Assurance and the Risk Assessment of Digital Systems. The Subcommittee will gather information, analyze relevant issues and facts and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee.

Mike Snodderly is the designated federal official for this meeting and Eric Thornsbury is the cognizant staff engineer.

The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in the Federal Register on May 31, 2005. A transcript of the meeting is being kept and will be made available as stated in the Federal Register notice. It is requested 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 speakers, first, identify themselves and speak with
2 sufficient clarity and volume, so that they can be
3 readily heard.

4 We have received no written comments or
5 requests for time to make oral statements from members
6 of the public regarding today's meeting. Now, we will
7 proceed and Mr. William Kemper will start us off.

8 MR. KEMPER: Yes, as you said, we
9 concluded our discussions yesterday on Software
10 Quality Assurance. Today, we're going to continue on
11 where Steve Arndt left off with his overview of our
12 Digital System Risk Assessment Project. This is a
13 project that has been collaborated with our PRA Branch
14 for the research. Hossein, he is here to speak on
15 behalf of the section. So basically, we're going to
16 give you more details on each of the initiatives
17 associated with that effort.

18 So, Steve, do you want to make a few
19 comments before we get started?

20 CHAIRMAN APOSTOLAKIS: So is the first
21 topic development and analysis of digital system
22 failure data?

23 MR. ARNDT: Yes, I'll explain that in a
24 second.

25 MR. KEMPER: Yes.

1 MR. ARNDT: Just to clarify the agenda and
2 to remind you of where we left off last night, I gave
3 a brief overview of the program plan as a whole. The
4 program plan, as you remember, that diagram we had
5 included both analysis and data, evaluation of models,
6 separate programs to look at whether or not it is
7 feasible to do digital system modeling, both from a
8 traditional fault tree of entry aspect as well as
9 using more dynamic methodologies.

10 So today what we have scheduled is three
11 presentations. The first two will be together. Those
12 will go over the data project as well as the first
13 part of the effort for the traditional fault tree of
14 entry modeling analysis. The third presentation will
15 be from the difference perspective looking at the
16 dynamic modeling methodologies. So without further
17 ado, let me turn it over to our colleagues from the
18 PRAB.

19 CHAIRMAN APOSTOLAKIS: So all these three
20 presentations are done jointly with a PRA group?

21 MR. ARNDT: The first two presentations
22 will be led by the PRA group. The third presentation
23 will be led by myself and Professor Aldemir.

24 CHAIRMAN APOSTOLAKIS: Thank you.

25 MR. ARNDT: The whole program is a joint

1 program. We're just leading it.

2 CHAIRMAN APOSTOLAKIS: Are we ready?

3 MR. HAMZEHEE: Well, again, my name is
4 Hossein Hamzehee. I am the section chief with the PRA
5 Branch, Office of --

6 UNIDENTIFIED SPEAKER: This one here?

7 MR. HAMZEHEE: -- Nuclear Regulatory
8 Research. With me is Todd Hilsmeier. He is the
9 reliability and risk engineer and also we have Louis
10 Chu from Brookhaven National Lab. And all three of us
11 are going to help each other today to go over our
12 effort in the PRA Branch.

13 CHAIRMAN APOSTOLAKIS: Where are the
14 slides?

15 MR. HAMZEHEE: I'm sorry?

16 CHAIRMAN APOSTOLAKIS: Any questions?

17 CHAIRMAN APOSTOLAKIS: Why are the slides
18 this way, Hossein?

19 MR. HAMZEHEE: I have no control.

20 CHAIRMAN APOSTOLAKIS: Okay.

21 MR. HAMZEHEE: Sorry. The purpose of this
22 presentation is to describe our Digital Systems PRA
23 Project Plan and also provide you with the status of
24 our activities and have some discussions of some of
25 the work that has been completed or is in the progress

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 be completed. We plan to quickly -- I will try to
2 speak no more than 15 to 20 minutes to provide some
3 background and then the objective of our work and talk
4 about our overall integrated project plan.

5 And then Todd will talk in more detail
6 about each element will pass in our overall program
7 plan. And then we have Louis Chu here if there are
8 some more detailed questions and status of what will
9 be done and some more technical issues. So I believe
10 all three of us together will provide a reasonable
11 overview of the work that has been going on for some
12 time now.

13 With that, I am sure you may have already
14 heard that as we speak some nuclear power plants have
15 expressed interest in replacing some of their analog
16 I&C systems with digital. And as you may know, the
17 advance reactors are already using digital or are
18 planning to use digital I&C systems. And we have
19 heard that right now Oconee, Callaway, Wolf Creek and
20 Comanche Peak have shown some interest in operating
21 their RPS system with a digital RPS.

22 And also, when these utilities submit
23 their studies, then the NRR has to review and provide
24 some technical evaluation and that would require some
25 further research. And for us to provide the risk-

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 informed approach to evaluate these submittals, we
2 need to better understand how to model and quantify
3 the reliability of these digital I&C systems.

4 And as you may also know, EPRI has
5 completed a document. You may have talked about it
6 earlier today or yesterday, so they are with me if you
7 already know this, that they have provided report
8 entitled "Guideline for Performing Defense-in-Depth
9 and Diversity Assessments for Digital I&C Upgrades."
10 Now, currently, we are working with NRR to do an
11 acceptance review to see if the package as is is
12 adequate for us to review. And if it is, then NRR
13 will usually provide the schedule and perform the
14 review and then give some comments.

15 CHAIRMAN APOSTOLAKIS: What criteria do
16 you use in your acceptance review?

17 MR. HAMZEHEE: Well, I need to have NRR to
18 talk about that. Is anybody from NRR here that can
19 help us with that question? Is Matt here? Matt, do
20 you know what that may entitle? Because I am not
21 sure. They usually have some criteria that they make
22 sure that when utility or EPRI provides a technical
23 document, does it have enough information in certain
24 areas, does it provide adequate details so somebody
25 can review and see if it is acceptable. So usually,

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 first, they do that performance and then if they find
2 it adequate, then they do the detailed review. And
3 what the exact criteria are, I'm not sure.

4 CHAIRMAN APOSTOLAKIS: Okay. Thank you.
5 But ultimately, if the staff reviews this document,
6 there will be an SER?

7 MR. HAMZEHEE: Correct.

8 CHAIRMAN APOSTOLAKIS: And then it would
9 come back to us?

10 MR. HAMZEHEE: Right.

11 MR. SNODDERLY: We would review the
12 staff's SER.

13 CHAIRMAN APOSTOLAKIS: Yes, okay.

14 MR. HAMZEHEE: But usually before we spend
15 time and resources, we want to make sure that that
16 document is acceptable.

17 CHAIRMAN APOSTOLAKIS: Sure.

18 MR. HAMZEHEE: For review. And then Todd
19 will talk about we have a task associated with this
20 for two different purposes and we'll talk about it
21 more later on during this presentation.

22 Now, the objective of our work here is to
23 -- our goal is to develop a probabilistic method for
24 modeling the potential failures of a digital I&C
25 system that can later be integrated with 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 probabilistic risk assessment using some of the
2 traditional methods, such as long event trees and
3 fault trees. And based on what we have seen so far at
4 our work, it's obvious that currently the digital
5 systems have not been treated uniformly and adequately
6 in the PRAs.

7 And in some cases when they did do some
8 modeling, they used like black-box approach with some
9 point estimate for failure of probability. And the
10 data and current methods that are available don't seem
11 to be adequate and that's what's driving our work
12 here. Now, we skipped a lot this one, because we
13 talked about this and if need be, we'll come back to
14 this. But let's go back to the next flow chart.

15 Now, I am going to spend no more than 10
16 minutes to explain how we put our program and task
17 plan together. And as I said, then Todd will talk
18 about each of those tasks and elements in more detail.
19 For us to have a risk-informed approach, we have to be
20 able to model the digital I&C and PRAs and be able to
21 tell or quantify the reliability of a digital I&C. In
22 order to be able to quantify the reliability of a
23 digital I&C, we have to have models and we have to
24 have data.

25 So these are the two elements then first

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 see in our work. We have to see if they are
2 available, fine. If not, then we need to develop
3 them. As we looked at the digital I&C, then we
4 realized that they are different from other mechanical
5 systems or other mod systems that we model and
6 evaluate in PRAs, in the sense that they are hardware
7 and software, and each has different characteristics.

8 Right now, we need to have models and data
9 to hardware and software and then when we put the
10 program plan together, if we look at the two blocks on
11 the right and left and ignore anything to the top and
12 bottom, for the time being, then you see that we broke
13 our work, broke it down into two parts. On the left
14 side, you see the hardware block that we have and the
15 task plan the numbers represent the task in our task
16 plan.

17 The first block is block number 5. If I
18 can read it from here. And that is to gather and
19 evaluate the reliability data. This is one of our
20 tasks. And once we gather and evaluate data,
21 hopefully, at some point, we feel like we have
22 adequate data. Then we have to go back and see what
23 kind of models and methods are available.

24 If there isn't sufficient methods, then
25 we're going to develop and evaluate appropriate

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 methods, such as George's favorite model, Markov, or
2 others, fault trees or some others that can be
3 adequate. We will use them and then at the end of
4 this task, we will be able to at least recommend what
5 method is appropriate for digital I&C.

6 CHAIRMAN APOSTOLAKIS: But why is Box 5 --

7 MR. HAMZEHEE: Yes, the first box --

8 CHAIRMAN APOSTOLAKIS: -- gathering an
9 analysis of reliability data? Can you use the cursor
10 to point to the box?

11 MR. HAMZEHEE: Yes.

12 CHAIRMAN APOSTOLAKIS: The cursor, the
13 cursor.

14 MR. HAMZEHEE: The cursor?

15 CHAIRMAN APOSTOLAKIS: Yes, you can do
16 that. Yes, that's the one. That's the one. That's
17 the one. Why is that under hardware? I mean, do we--
18 don't you need data on the software failures?

19 MR. HAMZEHEE: Yes.

20 CHAIRMAN APOSTOLAKIS: It should be a
21 common box feeding into both.

22 MR. HAMZEHEE: Correct. Now, what we're
23 seeing is when it comes to data, we need two types of
24 data. One is for hardware, one is for software.

25 CHAIRMAN APOSTOLAKIS: But that's not 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 the figure says.

2 MR. HAMZEHEE: But it does. If you look
3 at the right block, the counterpart of that block on
4 the right says software on the top and then it has a
5 similar block.

6 CHAIRMAN APOSTOLAKIS: No, it doesn't.

7 MR. HAMZEHEE: If you want to look at the
8 one that Todd has pointed to.

9 CHAIRMAN APOSTOLAKIS: No, it says develop
10 software failure probabilities.

11 MR. HAMZEHEE: Yes, that is common.

12 CHAIRMAN APOSTOLAKIS: The Box 5, it seems
13 to me, should be in the middle feeding both hardware
14 and software. That's what you told us and that's what
15 it is. It's just misplaced there.

16 MR. HAMZEHEE: Let me go over it and then
17 when we talk about the detail, you'll see how they
18 fall into the -- it doesn't matter how we put it here.
19 But the reason we put it here is because we want to
20 make sure if there are some more availability or
21 products in one area, that doesn't impact the other
22 one.

23 CHAIRMAN APOSTOLAKIS: It seems to me --

24 MR. HAMZEHEE: But technically it doesn't
25 matter where you put those boxes.

1 CHAIRMAN APOSTOLAKIS: As long as you do
2 it right, yes.

3 MR. HAMZEHEE: Yes.

4 CHAIRMAN APOSTOLAKIS: But the point is
5 that we can't really claim that we understand the
6 failure modes of software.

7 MR. HAMZEHEE: That's correct.

8 CHAIRMAN APOSTOLAKIS: So you know,
9 collecting as much data as we can is probably a good
10 idea.

11 MR. HAMZEHEE: Yes.

12 CHAIRMAN APOSTOLAKIS: Yes.

13 MR. HAMZEHEE: And that is what the Block
14 8. Would you put the cursor on Block 8? If you put
15 the cursor on Block 8, the one running parallel is
16 we're going to look at the hardware failure data,
17 evaluate, analyze, gather and do the same thing for
18 software. So technically, we're doing what you're
19 saying, but we simply need to do hardware and
20 software.

21 CHAIRMAN APOSTOLAKIS: Anyway, I suggest
22 that Box 5 be moved to the middle. That's all.

23 MR. HAMZEHEE: All right.

24 CHAIRMAN APOSTOLAKIS: And that is the
25 same way you are blocking for with two arrows? One

1 leading to hardware and one to software, that's all.

2 MR. HAMZEHEE: That's right. That can be
3 done, too.

4 CHAIRMAN APOSTOLAKIS: But will it?

5 MR. HAMZEHEE: Yes.

6 CHAIRMAN APOSTOLAKIS: It's a big deal.
7 It's not a big deal, Hossein.

8 MR. HAMZEHEE: Yes, we'll do that if it's
9 not a big deal. And then Block 6 is looking at the
10 modeling techniques and what methods to apply. And
11 then the next block, Block 7 is then to combine the
12 two and try to quantify the reliability of the
13 hardware. Now, again, you may say why do this
14 separately? As we make progress, we may find out that
15 we can combine them in the earlier stage. So this is
16 just for presentation purposes, not done logically.
17 It has to be separated.

18 And then if you move to the right drop
19 under software, the Block A talks about developing,
20 analyzing data for software. And then try to develop
21 some methods for modeling the software. And then at
22 the end, Block 9 is the software model quantification.
23 And then you provide these two in a proper logical
24 manner. Then you do the overall digital system
25 reliability quantification.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: Now, hardware model
2 quantification. You mean the hardware of the
3 computer, not the pumps of it?

4 MR. HAMZEHEE: Of the RPS digital system.
5 Of the digital system.

6 CHAIRMAN APOSTOLAKIS: The digital system?

7 MR. HAMZEHEE: Yes. Not the pumps.

8 CHAIRMAN APOSTOLAKIS: Oh, is it --

9 MR. HAMZEHEE: Not the --

10 CHAIRMAN APOSTOLAKIS: Is this only for
11 RPS protection?

12 MR. HAMZEHEE: Well, as an example, it's
13 for RPS, but you can have the --

14 CHAIRMAN APOSTOLAKIS: Yes, so it's --

15 MR. HAMZEHEE: -- control for monitor.
16 The digital I&C systems utilities plan to operate to.

17 CHAIRMAN APOSTOLAKIS: Because they are
18 the ones saying that is again box number 9 may be
19 mislabeled, in the sense that there is a school of
20 thought that says you will not have a software model
21 quantification, because you are amending the software
22 in the box system.

23 MR. HAMZEHEE: That's why I said we don't
24 know right now how logically the boxes are connected.

25 CHAIRMAN APOSTOLAKIS: Yes.

1 MR. HAMZEHEE: But that's a good point
2 though. You are right. So data Block 10, we try to,
3 if it makes sense, combine it and come up with the
4 overall system reliability quantification. And then
5 Block 11 will make an attempt to integrate it with the
6 PRA, so that we can come up with the risk contribution
7 and risk assessment of a digital system with respect
8 to planned risk, such as CDF and other risk matrix.

9 And then finally, our goal is at some
10 point in time, and Todd will talk about schedule,
11 we'll try to document all these things in the NUREG
12 report. Now, let's go --

13 CHAIRMAN APOSTOLAKIS: I would expect --
14 I mean, this is a big task. I would expect that you
15 will publish reports before NUREG.

16 MR. HAMZEHEE: I'm sorry?

17 CHAIRMAN APOSTOLAKIS: Wouldn't you be
18 publishing reports say after you finish the data
19 evaluation?

20 MR. HAMZEHEE: Probably not --

21 CHAIRMAN APOSTOLAKIS: Really?

22 MR. HAMZEHEE: -- public report. But we
23 may have some intermediate technical reports, yes.

24 CHAIRMAN APOSTOLAKIS: Hum.

25 MR. HAMZEHEE: But at the end, we want to

1 put them all into a NUREG report.

2 CHAIRMAN APOSTOLAKIS: But wouldn't you
3 like to have some comments from the public on your
4 data collection and conclusions that you draw from it?
5 I mean, why do you want to have to wait until the very
6 end?

7 MR. HAMZEHEE: That can be -- that's an
8 option, yes.

9 CHAIRMAN APOSTOLAKIS: That's a good idea,
10 I think.

11 MR. HAMZEHEE: Bill?

12 MR. KEMPER: This is Bill Kemper. We do
13 have plans to convene a public meeting, at some point.
14 We're not exactly sure exactly where perhaps we're
15 going to do it. But we do intend to engage the
16 public.

17 CHAIRMAN APOSTOLAKIS: Okay.

18 MR. KEMPER: We just have reason for it.

19 CHAIRMAN APOSTOLAKIS: Okay.

20 MR. HAMZEHEE: But hopefully before it
21 becomes a NUREG report it has to go through public
22 review and comment, more interactions with ACRS and
23 others, before we can call it a NUREG report. And so
24 now let's go back to the top of the block. If you
25 look at Block 1, when we started this project it was

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 about a year ago and again Todd will talk about it,
2 but quickly, there was a draft EPRI report and we
3 wanted to review that and gain some insight to see if
4 that can help us with the work we are doing. So that
5 was the purpose of that Block 1.

6 And then Todd, he will tell you where we
7 are and the documentation that we have. And then
8 Block 2, we also wanted to make sure we don't reinvent
9 the wheel. So we went ahead and tried under that task
10 to look at available data from other agencies, such as
11 NASA, find out what else is going on, who has done
12 what and then use them as applicable. So that was the
13 purpose of Block 2, and then Todd again will tell you
14 where we are and what we have done with those two.

15 And Block 3 is basically trying to figure
16 out then how we would put all these things into a
17 report. And now go back down to the -- all the way to
18 the right. And those are again sensitive research.
19 We try to envision what else can happen or the work
20 that we may have to do. We haven't planned for the
21 last block that says future activities yet in our
22 current plan, but we have defined some potentials. So
23 as the interest and the need arises and if the budget
24 allows, then what we want to do is the first one is to
25 support NRR when they do review the EPRI report.

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 And that actually when we put this block
2 together was a year ago, and we were not sure if that
3 was going to happen, but today when we're talking
4 about it, it did happen. So most likely that future
5 work is going to happen earlier. And then below it is
6 once this work is complete, then we like to provide
7 some guidance, because most likely even if we come up
8 with one or two methods once the licensees start
9 operating their systems to digital, they are going to
10 come up with other methods.

11 So we want to be able to provide some
12 guidance on acceptable methods, so that others can
13 apply those guidance and develop their own models.

14 CHAIRMAN APOSTOLAKIS: So what is the time
15 frame of all of this?

16 MR. HAMZEHEE: Todd is going to tell you.
17 He is going to go over all of them. And then the last
18 one is again as time goes on and we get more real
19 applications from licensees, we're going to learn more
20 and as we learn more, we may come up with new methods
21 and applications. And that's again in the future
22 activities. Now, this is all I'm going to say. If
23 there aren't any questions, I'm going to turn it to
24 Todd. If you have any questions?

25 MR. HILSMEIER: Am I registering okay? My

1 name is Todd Hilsmeier from research and I work in the
2 PRA Department. And a little background on myself.
3 I've spent 6 years in consulting business doing PRA
4 and then 6 years at plants Salem, Hope Creek, Diablo
5 Canyon working in PRA. Then I joined NRC last
6 September and the first project was the Digital
7 Systems PRA Project.

8 And I'm going to continue where Hossein
9 left off at. And the first task that we are working
10 on is Task 1, which is review of the EPRI 1002835
11 report. And the purpose of reviewing this report is
12 to obtain insights on the reliability methods for
13 modeling digital systems. Our focus was not revealing
14 the report for review and approval by NRC, but to gain
15 insights on how we can use the report to develop
16 reliability models.

17 And some observations that we observed
18 from the reports is that the EPRI Technical report
19 advocates risk-informing digital I&C systems by
20 proposing the use of a simplified and a standard risk-
21 informed method as it turns to current deterministic
22 methods. And also we observed that the simplified
23 risk-informed method should be clarified and
24 demonstrated with examples.

25 I should note that we reviewed an earlier

1 version of EPRI guide, it's final version, the current
2 version does provide examples of a simplified method.
3 And so this statement is no longer up to date. The
4 simplified risk-informed method may not necessarily
5 provide conservative risk values. And also the EPRI
6 Technical report does not provide information on how
7 to develop models needed for standard risk-informed
8 traditional PRA methods.

9 However, the EPRI report does provide some
10 characteristics to consider in reliability model
11 development. The current schedule for Task 1 is the
12 research division reviewed comments on our draft
13 report and the final report for Task 1 will be
14 completed June 30th.

15 CHAIRMAN APOSTOLAKIS: So I don't
16 understand that. I mean, Hossein just told us that
17 you are in the process of deciding whether to review
18 it. This is a research review, not NRR review.

19 MR. HILSMEIER: But in itself --

20 MR. HAMZEHEE: There are two parts. There
21 are two reasons we are looking at this EPRI report.
22 One is to gain insight as Todd said to help us with
23 our work to see if they've done some good work that we
24 can benefit from. The other one is to support NRR in
25 their review. So I think Todd is talking about 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 first purpose of that review. Am I right, Todd?

2 MR. HILSMEIER: Yes, that's correct. The
3 review of the EPRI report for approval by NRC is a
4 future task. The primary purpose of our review is
5 just to gain insight on the report.

6 CHAIRMAN APOSTOLAKIS: This review was
7 done within the Agency?

8 MR. HILSMEIER: Excuse me?

9 CHAIRMAN APOSTOLAKIS: Was it done in-
10 house, the review?

11 MR. HILSMEIER: Yes, by myself and
12 Brookhaven National Laboratory, Louis Chu.

13 CHAIRMAN APOSTOLAKIS: Okay.

14 MR. HAMZEHEE: I think just for clarity,
15 most of our work is in-house with some help from BNL,
16 in our area.

17 MR. HILSMEIER: And we reviewed the EPRI
18 report before we had the final version. In Task 2,
19 the purpose of Task 2 is review industry experience
20 per methods and databases, failure databases of
21 digital hardware/software use to model digital
22 systems. The basic approach was to establish contacts
23 with industry, such as NASA, Army, Navy, Air Force,
24 DOE, DoD, the Defense Nuclear Facility Safety Board,
25 FAA, automotive industry and then several contractors,

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 OMNICON, RAC and Idaho National Laboratory, that's to
2 name a few.

3 The second step in the approach is to
4 search and collect guidance on the reports and then
5 review the reports. And what we observed from
6 industry is that most of industry managed digital
7 system risk through a qualitative approach, which
8 involves software development process, management,
9 testing the software, documentation, QV&V of the
10 software. And we found very little of industry that
11 forms quantitative risk analyses.

12 I think there are some small isolated
13 cases of quantitative risk analyses and digital
14 systems, such as Idaho National Laboratory performed
15 some digital reliability work for the Army and it's
16 all classified and proprietary, so we weren't able to
17 analyze the results. Also, OMNICON did similar work
18 for the Navy.

19 I'll be talking about the Idaho National
20 Laboratory Failure Rate Database under Task 5.
21 However, we also observed that NASA is moving to a
22 quantitative risk evaluation approach using PRAs. We
23 looked at the NASA Fault Tree Handbook and the NASA
24 Peer Review Procedure Guide, that was developed by
25 experts with extensive nuclear power plant PRA

1 experience. Task 2 is currently being worked on and
2 the final report will be completed by August 30, 2005.
3 Any questions on Task 2?

4 Task 3, we don't have a slide for, it's
5 simply documentation of all the work that we do in
6 creating an outline. We document as we go and one
7 document at the end. We want to make sure we stay up,
8 make sure we document all our thoughts and not miss
9 any information.

10 Task 4 is developing supporting analysis
11 for the Digital System Reliability Project and
12 basically involves obtaining information about the
13 behavior of the digital system, such as developing
14 FMEA, failure modes and effects analysis and
15 dependency analysis for the system. And the FMEA
16 dependency analysis is a foundation of reliability
17 model. And we also want to develop guidance on how
18 communication and voting should be modeled.

19 These supporting analyses will support the
20 development of the Digital Systems Reliability Model.
21 We need to apply the supporting analyses to a case
22 example. And our case example will be the Digital
23 Reactor Protection System proposed for Oconee. For
24 reactor trip demand using the Teleperm platform, the
25 expected period of performance is expected to start in

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 July of 2005, next month, and we expect to complete it
2 in September 2006. Any questions?

3 CHAIRMAN APOSTOLAKIS: Don't worry, there
4 are -- there will be.

5 MR. HILSMEIER: Okay. No questions.
6 Hossein questions me all the time.

7 CHAIRMAN APOSTOLAKIS: Do you feel you
8 have been treated unfairly?

9 MR. HILSMEIER: No, no.

10 CHAIRMAN APOSTOLAKIS: Okay. I
11 understand. Maybe you are doing a better job.

12 MR. HILSMEIER: I love this job in
13 consulting and working at the power plants.

14 CHAIRMAN APOSTOLAKIS: Okay. How much are
15 you going to tell us about the data now?

16 MR. HILSMEIER: I was going to skip this
17 task. I know this is your favorite task. Task 5 is
18 development of the failure database for digital
19 hardware. And for the analysis, our approach for
20 developing the database was reviewing failure rate
21 databases.

22 These databases were Military Handbook
23 Telcordia and PRISM. And I'll talk about this
24 approach in the next slide. It also serves industry
25 for additional digital failure data. Industry such as

1 LERs and EPIX from nuclear power plants, also NASA,
2 the SPAR model and FAA. And then last, under approach
3 is development of a population variability
4 distribution using the proprietary PRISM failure
5 records.

6 CHAIRMAN APOSTOLAKIS: What's PRISM again?
7 What's PRISM?

8 MR. HILSMEIER: It's a software package
9 developed by Reliability Analysis Center used to
10 predict failure rates.

11 CHAIRMAN APOSTOLAKIS: Who is Reliability
12 Analysis Center, is that the NASA people?

13 MR. HILSMEIER: It's a consulting company.

14 CHAIRMAN APOSTOLAKIS: Huh?

15 MR. HILSMEIER: It's --

16 DR. CHU: They work with the defense
17 industry a lot. It's like consulting.

18 CHAIRMAN APOSTOLAKIS: It's consultants?

19 DR. CHU: Yes.

20 MR. HAMZEHEE: It's proprietary.

21 CHAIRMAN APOSTOLAKIS: Huh?

22 MR. HAMZEHEE: It's proprietary though,
23 it's not available.

24 CHAIRMAN APOSTOLAKIS: So prohibited. Do
25 you have access to it?

1 MR. HAMZEHEE: We have purchased it and
2 yes, we do have access to it.

3 CHAIRMAN APOSTOLAKIS: Oh, okay.

4 DR. CHU: Yes, we are not supposed to
5 tabulate all the failure rates found at database.

6 CHAIRMAN APOSTOLAKIS: Is it a failure
7 rate database or is it failure modes? Are you using
8 it in any other way?

9 DR. CHU: They have raw data in the form
10 of failures in this number of hours.

11 CHAIRMAN APOSTOLAKIS: For software?

12 DR. CHU: For hardware.

13 CHAIRMAN APOSTOLAKIS: Okay. Anybody can
14 do that.

15 DR. CHU: That actually is the only thing
16 that we were able to find that kind of data, raw data.

17 CHAIRMAN APOSTOLAKIS: For what?

18 DR. CHU: Digital hardware.

19 CHAIRMAN APOSTOLAKIS: Digital hardware?
20 Well, I mean, if you rely on this a lot, maybe we
21 ought to look at it. There are mechanisms still
22 handling proprietary information. Yes.

23 MR. KEMPER: Did -- you say we purchased
24 it, right? So we --

25 MR. HAMZEHEE: Yes, for our own use to

1 include in ACRS we can look at it.

2 CHAIRMAN APOSTOLAKIS: Yes.

3 MR. HAMZEHEE: Oh, yes.

4 CHAIRMAN APOSTOLAKIS: Definitely, we are
5 part of the Agency.

6 MR. HAMZEHEE: Sure. As long as you agree
7 with us.

8 CHAIRMAN APOSTOLAKIS: As long as what?

9 MR. HAMZEHEE: You agree with us.

10 MR. HILSMEIER: Task 5 continued. The
11 first bullet was reviewing the failure rates databases
12 and Military Handbook, Telcordia and PRISM, that's
13 what I'm going to discuss next. The analysis of these
14 three sources Military Handbook and Telcordia will be
15 documents and PRISM is the software program. They use
16 empirical formulas to predict failure rates.

17 CHAIRMAN APOSTOLAKIS: Can you tell us
18 what that means?

19 MR. HILSMEIER: Yes, basically, they take
20 a base failure rate and apply pi shaping factors.

21 CHAIRMAN APOSTOLAKIS: Oh.

22 MR. HILSMEIER: To adjust failure rates
23 for quality.

24 CHAIRMAN APOSTOLAKIS: The basic failure
25 rate comes from standard methods, though?

1 MR. HILSMEIER: Yes.

2 CHAIRMAN APOSTOLAKIS: Bayesian or what,
3 maximum likelihood?

4 DR. CHU: They didn't provide the detail
5 of how they estimate.

6 CHAIRMAN APOSTOLAKIS: You know why? They
7 don't have an advisory committee to review those. You
8 guys wouldn't do that.

9 MR. HILSMEIER: That's why we didn't use
10 the data. I mean, the empirical formulas.

11 CHAIRMAN APOSTOLAKIS: See, the problem
12 with these things is they do it and then, you know,
13 people say oh, gee, this is DoD or NASA or whatever.
14 They have been doing it, so it must be right. Well,
15 no, it's not right.

16 MR. HAMZEHEE: I think we came to this
17 same conclusion. And I think he is going to tell you
18 the problems that we have found.

19 CHAIRMAN APOSTOLAKIS: And I agree with
20 him, yes.

21 MR. HAMZEHEE: Okay.

22 MR. HILSMEIER: The empirical formulas
23 work well when, in limited cases, the data is
24 applicable and sufficient. But in that case, one can
25 just use the data explicitly calculated by 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 rates.

2 CHAIRMAN APOSTOLAKIS: So a broken clock
3 is right twice a day.

4 MR. HILSMEIER: Exactly.

5 CHAIRMAN APOSTOLAKIS: Yes.

6 MR. HILSMEIER: So the other concern we
7 had with these three sources was the lack of
8 uncertainty consideration. And is it correct they
9 didn't provide any uncertainty, the empirical formulas
10 don't provide uncertainty?

11 DR. CHU: Right. One situation I asked
12 why don't you consider uncertainty? And the answer I
13 got was there are so many sources of uncertainty, you
14 can't handle it.

15 CHAIRMAN APOSTOLAKIS: Well, that's a good
16 reason. And besides why get an uncertainty about the
17 wrong point estimate anyway.

18 MR. HILSMEIER: So we didn't use these
19 sources, the empirical formulas. We also reviewed
20 industry experience failure databases. The existing
21 PRA failure databases touch as far as NASA, PRA guide,
22 IEEE, did not contain digital component failure rates.
23 The advanced reactor PRAs may contain limited
24 additional failure rate data, which is proprietary.

25 CHAIRMAN APOSTOLAKIS: If you can get

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 those.

2 MR. HILSMEIER: Yes, and we plan to
3 evaluate this further under the second phase of data
4 analysis.

5 CHAIRMAN APOSTOLAKIS: Now, that was
6 another thought. Is that not what is this kind of
7 data? Is that true, Louis?

8 DR. CHU: I'm sorry?

9 CHAIRMAN APOSTOLAKIS: Nobody has that
10 kind of data. You are going through this, because you
11 have to. Do you really think there is somebody out
12 there that has a databank that has well-documented
13 failure rates for software components or hardware?

14 DR. CHU: I tend to think the
15 manufacturers do have.

16 CHAIRMAN APOSTOLAKIS: Yes, they will tell
17 you FFA has.

18 DR. CHU: Actually, some -- most of the
19 data in the PRISM software came from some
20 manufacturer. The name they don't tell us.

21 CHAIRMAN APOSTOLAKIS: Of course they
22 don't tell you, because if you go and look, you will
23 reject it like they rejected PRISM.

24 MR. HAMZEHEE: But I think, George, I
25 mean, we have to start from somewhere.

1 CHAIRMAN APOSTOLAKIS: No, I'm not saying
2 we shouldn't do it.

3 MR. HAMZEHEE: And this database --

4 CHAIRMAN APOSTOLAKIS: But I'm just
5 telling you that we know the answer.

6 MR. HAMZEHEE: Yes, but I think from
7 manufacturers you get some reasonable data, because
8 you have numerator and denominator, even though you
9 may not have high confidence, but it's a good start.
10 And as these systems are installed and we get more
11 operating experience, then we update the information.
12 That's really one way to go I think. The only way you
13 can really get some numbers and do some
14 quantification.

15 CHAIRMAN APOSTOLAKIS: Well, I repeat it's
16 not the numbers that worry me, it's the actual failure
17 modes. I don't think we really understand those.

18 MR. HILSMIEIER: All right. We also
19 evaluate industry operating experience, such as the
20 nuclear power plant LERs, double event reports and
21 EPIX data, FAA, Army, the Department of Energy, and
22 they contain digital failures, but the reports are not
23 detailed enough. They don't describe what digital
24 component failed. As Steve mentioned yesterday, the
25 reports don't say -- specify in the meantime between

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 failures and specify additional systems that are
2 deployed that have not failed.

3 So there is a lot of information just from
4 these databases to calculate, to estimate a failure
5 rate. But we will evaluate some of these databases
6 further in the second phase of data analysis. Because
7 there is a second phase I'm kind of hinting at our
8 conclusion.

9 MR. HAMZEHEE: And I also would like to
10 add, George, that we will welcome any insights you
11 have. If you have some information that we can use,
12 this is a good time. So we are also asking you to
13 help us if you have some additional information in
14 some of your other work or involvement.

15 CHAIRMAN APOSTOLAKIS: I mean, even in my
16 additional comments, didn't I have a citation, which
17 is admittedly old, but was -- somebody at NASA had
18 collected information, actual data. What does that
19 mean, Louis? You didn't read the comments or you
20 checked the reference and it's not useful?

21 DR. CHU: I think I didn't read the
22 comment carefully.

23 CHAIRMAN APOSTOLAKIS: Thank you very
24 much. You come here.

25 MR. HILSMETIER: I didn't hear the

1 question. I'm sorry.

2 CHAIRMAN APOSTOLAKIS: Well, there is --
3 all I know is in that paper by Garrett and me and also
4 in the added comments. I don't have any thing
5 additional. Do you have the paper by Garrett, Chris
6 Garrett and me? That's all I got.

7 MR. HILSMEIER: All right.

8 CHAIRMAN APOSTOLAKIS: But I'm surprised
9 I don't see any of that here, because they have
10 individuals, not organizations, individuals have
11 collected information occasionally.

12 MR. HILSMEIER: And we also reviewed a
13 NASA failure database. I mean we didn't review it.
14 We tried getting the NASA failure database and this is
15 through Dr. Dezfouli.

16 CHAIRMAN APOSTOLAKIS: Who would have it
17 at NASA?

18 MR. HAMZEHEE: Normally, that would be
19 read from ISO and Bill Vesely and those guys can help.

20 CHAIRMAN APOSTOLAKIS: All right. Keep
21 going.

22 MR. HILSMEIER: All right. Thank you.
23 Right. Dr. Dezfouli was saying that --

24 CHAIRMAN APOSTOLAKIS: They are looking
25 for it just as you are.

NEAL R. GROSS

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

1 MR. HILSMEIER: The data will be available
2 for publishing in 2006. However, there is a
3 Conference Spec 2000 between NRC and NASA to establish
4 a cooperative, I'm not sure of the correct words, but,
5 agreement to work on the Digital System Reliability
6 and for the second phase of data analysis, we're going
7 to try to get the proprietary data. If not, then use
8 the public available data. And another question is
9 will the data have sufficient detail.

10 CHAIRMAN APOSTOLAKIS: It is an IEEE or
11 some other publication on computers, which seems to
12 publish periodically an evaluation of major failures?
13 I don't remember what the title is. Are you familiar
14 with it, Steve? I'm not sure it's IEEE. It's some
15 other organization.

16 MR. ARNDT: It's not IEEE.

17 CHAIRMAN APOSTOLAKIS: Computers.

18 MR. ARNDT: It's one of the computer
19 societies.

20 CHAIRMAN APOSTOLAKIS: Yes, yes. And
21 again, they don't go out of their way to collect data.

22 MR. ARNDT: Yes, it's not --

23 CHAIRMAN APOSTOLAKIS: But they take a few
24 cases of created ways and they analyze it. So you may
25 have to do some of that. I mean, you're not going 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 find the database anywhere I don't think. But you may
2 create a database by picking some of these. And as I
3 say, that paper by Chris Garrett has some information.
4 But it's already a little old. But if you see the
5 name of the journal, then you go to more recent issues
6 and see whether they have more.

7 MR. ARNDT: Yes.

8 CHAIRMAN APOSTOLAKIS: Again, don't expect
9 them to solve your problems.

10 MR. HAMZEHEE: Again, we're trying to do
11 our best to see what is available, make sure we're not
12 missing anything. And then at the end we have to use
13 what is available with some uncertainty and, you know,
14 again, we got to start from somewhere in order to
15 quantify some reliability. So even if we don't have
16 the amount of data we need, we can still do some
17 quantification with some uncertainty there.

18 This is exactly the problem we had 30
19 years ago when we started doing PRAs. We didn't have
20 data for every single component for every equipment in
21 the plant, but then there was high uncertainty
22 associated with those. So I think it's a good start
23 and hopefully as utilities --

24 CHAIRMAN APOSTOLAKIS: I'm not questioning
25 why you're doing it. I'm just trying to help. I

1 think you have to do this as long as you have the
2 right amount of skepticism.

3 MR. HAMZEHEE: Yes.

4 MR. HILSMEIER: We also plan to look at
5 the COMPSIS data, which is international effort to
6 collect I&C operating experience. And it's still in
7 the early stage of data collection.

8 CHAIRMAN APOSTOLAKIS: They started in
9 1999.

10 DR. CHU: Yes, I read that.

11 CHAIRMAN APOSTOLAKIS: Huh? Have they
12 collected anything in the six years?

13 DR. CHU: That is a fairly -- they started
14 collecting.

15 CHAIRMAN APOSTOLAKIS: Yes, I mean, that--

16 DR. CHU: Steve Watson can tell you.

17 CHAIRMAN APOSTOLAKIS: Steve who?

18 DR. CHU: Steve.

19 CHAIRMAN APOSTOLAKIS: So what do you
20 have?

21 MR. HAMZEHEE: You need to speak in the
22 microphone and introduce yourself, otherwise that lady
23 is going to get mad.

24 CHAIRMAN APOSTOLAKIS: And we don't want
25 that to happen.

1 MR. HAMZEHEE: No.

2 MR. ARNDT: The COMPSIS database is an
3 international OECD effort along the same lines as the
4 IEPD and things like that to collect data from various
5 international or national databases and agencies that
6 get data as part of their regulatory responsibilities
7 like our LER database.

8 CHAIRMAN APOSTOLAKIS: But have you
9 connected them?

10 MR. ARNDT: What we did was we started a
11 trial project in '99 to try and figure out whether or
12 not this was practical. We collected a small sample
13 of data to help us write the Coding Guidelines and
14 what information you need and things like that. We
15 got about 100 data points. Not over the useful, but
16 interesting. As of this year, we are starting to
17 collect full scale with all the signature countries
18 required to submit all their latest data.

19 CHAIRMAN APOSTOLAKIS: That's all nuclear?

20 MR. ARNDT: This is all nuclear.

21 CHAIRMAN APOSTOLAKIS: If you have 100, I
22 mean, I was hoping to see one or two or three examples
23 and I don't see any. You know, you guys don't want to
24 educate us?

25 MR. HAMZEHEE: I'm sorry, I was asking a

1 question.

2 CHAIRMAN APOSTOLAKIS: I'm asking Steve.
3 Louis, do you have any examples you can give us?

4 DR. CHU: Well, we -- all we have done is
5 using the data from the PRISM software and we used the
6 hierarchial Bayesian analysis to come up with a
7 failure rate.

8 CHAIRMAN APOSTOLAKIS: Are you going to
9 talk about any of that?

10 DR. CHU: Yes, I will.

11 MR. HAMZEHEE: Yes.

12 CHAIRMAN APOSTOLAKIS: Oh, you mentioned
13 that you have done it, but you're not talking about
14 it.

15 MR. HAMZEHEE: Well, we did. If you would
16 like --

17 CHAIRMAN APOSTOLAKIS: You said we did.
18 But, you know, this is a subcommittee. Subcommittees,
19 we generally are going to do that.

20 DR. CHU: Page 14 and 15.

21 CHAIRMAN APOSTOLAKIS: Yes.

22 DR. CHU: Talks about that.

23 CHAIRMAN APOSTOLAKIS: It says we did it,
24 at least. It doesn't say how you did it. This is a
25 Subcommittee meeting. In Subcommittee meetings we

1 want to know the how. Okay. Todd, you want to tell
2 us, Todd?

3 MR. HILSMEIER: How we got the failure
4 rates?

5 CHAIRMAN APOSTOLAKIS: Well, I was hoping
6 to see, you know, several examples of say here is the
7 means and then here our role of 2001 and here is why
8 it's interesting. You know, that kind of thing.

9 MR. HILSMEIER: Right.

10 CHAIRMAN APOSTOLAKIS: Maybe in a future
11 meeting we can do this, huh?

12 MR. HILSMEIER: Yes.

13 MR. KEMPER: If I could offer just back on
14 Tom's question, if nothing else, if all else fails, we
15 intend to use COMPSIS precisely for that purpose.

16 CHAIRMAN APOSTOLAKIS: Absolutely.

17 MR. KEMPER: We are paying into it, you
18 know. There is a fee every year and there is about,
19 I forget, eight or 11 countries, I think, have --

20 CHAIRMAN APOSTOLAKIS: Well, he says you
21 have 100 points, I mean.

22 MR. KEMPER: In countries.

23 CHAIRMAN APOSTOLAKIS: That's great.

24 MR. KEMPER: And we'll start collecting
25 data pretty soon and George Tartal is 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 representative to that committee.

2 CHAIRMAN APOSTOLAKIS: Yes.

3 MR. KEMPER: And he'll go there twice a
4 year represent.

5 CHAIRMAN APOSTOLAKIS: Where are there,
6 Paris?

7 MR. KEMPER: Sometimes it will be, sure.

8 CHAIRMAN APOSTOLAKIS: At one time you go
9 to London, is that what you're saying?

10 MR. KEMPER: It could be.

11 CHAIRMAN APOSTOLAKIS: Marseilles.

12 MR. KEMPER: Right. But that's the idea.
13 We will each agree the incidents occurred in our
14 countries.

15 DR. BONACA: What about Huntsville?

16 CHAIRMAN APOSTOLAKIS: Huntsville,
17 Alabama?

18 MR. KEMPER: But at any rate --

19 CHAIRMAN APOSTOLAKIS: Anyway, as an
20 action item for the future, we need to spend some
21 serious time looking at what kind of data is available
22 to us, what we learn from it, how we learn, don't just
23 give me Latin names with a hierarchial base.

24 MR. HAMZEHEE: You know, George, for this
25 meeting we were planning mainly to spend no more than

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 an hour to go over our program plan and to some detail
2 of some of these tasks, but if you like, we can then
3 meet with you again to spend a few hours on each of
4 these tasks.

5 CHAIRMAN APOSTOLAKIS: I think we should
6 do that.

7 MR. HAMZEHEE: And get more technical.

8 CHAIRMAN APOSTOLAKIS: I think this is
9 going to be one of the major issues that the Agency
10 will be facing in the next several years.

11 MR. HAMZEHEE: Sure.

12 CHAIRMAN APOSTOLAKIS: And we ought to be
13 on top of it.

14 MR. ARNDT: We can, as part of our ongoing
15 interaction, highlight a couple of main particular
16 tasks in the various programs. This one for this
17 program and go into a much greater level of detail.
18 We will work through Eric and try and figure out the
19 level of detail you're interested in and work that
20 out.

21 CHAIRMAN APOSTOLAKIS: I'm a little
22 overwhelmed by this. I mean, are we going to review
23 the individual projects of some going on past
24 judgment? I mean, this is down the road. You or the
25 program with some detail here as well, but --

1 MR. HAMZEHEE: We were not planning to
2 have a detailed time review. But if you are
3 interested, we can send you some of our preliminary
4 documents, reports and get some feedback from you.

5 CHAIRMAN APOSTOLAKIS: In what form?

6 MR. HAMZEHEE: Some like internal
7 documents that are, you know, formal documents.

8 CHAIRMAN APOSTOLAKIS: Feedback though has
9 to be formal.

10 MR. HAMZEHEE: Right.

11 CHAIRMAN APOSTOLAKIS: The feedback has to
12 be a letter from the Committee.

13 MR. ARNDT: What is probably the easiest
14 way to do it is to schedule meetings at decision
15 points. We have looked at the data and we think we
16 can't do much or we need to do more or whatever and
17 then present those kind of things.

18 CHAIRMAN APOSTOLAKIS: Yes. Maybe that's
19 a good point.

20 MR. ARNDT: We did an evaluation of this
21 and we chose these two models to pursue or things like
22 that.

23 CHAIRMAN APOSTOLAKIS: No, I agree with
24 you, Steve. I think that makes perfect sense. But
25 let me bring another factor into this. This reminds

1 me of the days when we were struggling with how to
2 formulate the frame work for risk-informed regulatory
3 decision-making. That ended up being Regulatory Guide
4 1.174.

5 MR. ARNDT: Right.

6 CHAIRMAN APOSTOLAKIS: And in the sense
7 that here, just as then, the way to proceed forward is
8 not obvious. I mean, we are really looking for ways
9 of doing it and how to do it.

10 MR. ARNDT: Right.

11 CHAIRMAN APOSTOLAKIS: I mean, now
12 everybody says 1.174, you know, as if it's the most
13 natural thing in the world. But I know people have to
14 agonize over it, you know. And the ACRS got involved
15 early in the process and we had what some people call
16 participatory review, instead of waiting until the
17 end.

18 So the staff will come to us and say well,
19 gee, we're thinking of doing this or that. What do
20 you guys think? And we will, you know, say well, you
21 know, this makes sense, this doesn't make sense. If
22 you feel that that kind of participation will be
23 beneficial to you, I would rather go that way than
24 wait until you have a draft NUREG and then have the
25 Committee say we don't like it, so that doesn't come

1 as well.

2 MR. ARNDT: Yes. And I agree. I think
3 for some of these tasks, particularly this one and
4 some of the others, we will investigate something and
5 we'll think we have a direction and that's what I mean
6 by a decision.

7 CHAIRMAN APOSTOLAKIS: Okay. So I would
8 like to have this being one of the areas where we can
9 do that. After you guys have thought about it and say
10 well, we're going to follow this route, maybe we can
11 have a meeting and get whatever reason you can get
12 from us.

13 MR. ARNDT: Yes, okay.

14 CHAIRMAN APOSTOLAKIS: Do the Members
15 agree?

16 DR. KRESS: I think it's great.

17 CHAIRMAN APOSTOLAKIS: I'm not running
18 this, you know. Well, actually, if they disagree with
19 that, I would have heard it all, so, but it was just
20 a courtesy. No, but I really think this is the best
21 way to proceed, because this is a very difficult
22 subject.

23 DR. KRESS: Usually we do this with the
24 full Committee.

25 CHAIRMAN APOSTOLAKIS: Yes.

1 DR. KRESS: On 1.174 rather than just two
2 or three Members.

3 CHAIRMAN APOSTOLAKIS: Well, yes, yes. In
4 this case, probably the Subcommittee, I think.

5 DR. KRESS: We might want to combine some
6 Subcommittees.

7 CHAIRMAN APOSTOLAKIS: The Subcommittee
8 probably will have a meeting or two and then go to the
9 full Committee for a letter. I would rather
10 communicate with the staff than using letters.

11 DR. KRESS: Oh, yes.

12 CHAIRMAN APOSTOLAKIS: My understanding is
13 that the ACRS Staff doesn't like us to give you
14 informal comments. I mean, we give you comments here,
15 but not in writing.

16 MR. HAMZEHEE: We can give you status at--
17 more often, but for that, then it can't be as
18 frequent, because it takes a lot of your resources to
19 prepare letters.

20 CHAIRMAN APOSTOLAKIS: No, I'm not saying
21 every week.

22 MR. HAMZEHEE: No, no.

23 CHAIRMAN APOSTOLAKIS: I don't want to see
24 you every week.

25 MR. ARNDT: The feeling is mutual.

NEAL R. GROSS

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

1 CHAIRMAN APOSTOLAKIS: Louis, I would
2 really like to know a little more about it though.
3 Can you tell us anything? I mean, you know that, you
4 know, A, B, C, D means nothing. Is there any detail
5 you can give us now or is it pretty much over?

6 MR. HILSMEIER: I can give --

7 CHAIRMAN APOSTOLAKIS: Yes, go ahead,
8 Todd.

9 MR. HILSMEIER: I can give you some
10 numerical guidance.

11 CHAIRMAN APOSTOLAKIS: Yes, no, I don't
12 need all the numbers.

13 MR. HILSMEIER: Okay. Because this
14 process, this task is still ongoing, that's -- and
15 we're counting time.

16 CHAIRMAN APOSTOLAKIS: Do you remember of
17 a failure mode that was kind of unusual and is worth
18 mention?

19 DR. CHU: Right now, we are looking at the
20 hardware failure part.

21 CHAIRMAN APOSTOLAKIS: Yes.

22 DR. CHU: We don't have detailed
23 description of any failures. What we have is, as I
24 indicated earlier, we have from one source of data for
25 this particular component. We observe high failures

1 in hours, that's all.

2 CHAIRMAN APOSTOLAKIS: That's all?

3 DR. CHU: Failure may represent, you know,
4 products that get returned to the manufacturer and
5 manufacturer return to analyze yes, it fail or
6 identify specific cause of failures. But we don't
7 have that information. All we know is this failure --

8 CHAIRMAN APOSTOLAKIS: You mentioned two
9 events yesterday, one of Turkey Point and the other
10 Davis-Besse. So at least you have those and you may
11 have more than --

12 DR. CHU: Yes, Turkey Point. Okay. In
13 terms of nuclear experience, Turkey Point is one that
14 we have found, too, but that's a well-known one and
15 then there's --

16 CHAIRMAN APOSTOLAKIS: That doesn't count.

17 DR. CHU: It was an equipment failure.

18 CHAIRMAN APOSTOLAKIS: It was not an
19 equipment failure. It was a software failure.

20 DR. CHU: It was software. And then
21 another one that seemed interesting is one at Pilgrim.
22 There it's, I will call it, a real software common
23 cause failure.

24 CHAIRMAN APOSTOLAKIS: Okay. What
25 happened? Do you remember?

1 DR. CHU: It was during a storm and there
2 is this voltage regulator that controls the voltage
3 out of the transformer. The software was programmed
4 such that when you have certain under-voltage, it will
5 just trip the transformer. And of course, the same
6 software is used on different transformers. And
7 during this storm, the trip occurred. All the
8 transformers lost power and you lost vital AC buses,
9 so it is an interesting event at Pilgrim. This is
10 based on my understanding by reading the LER.

11 And then there is another incident. I
12 don't remember the specific controller. It's someone
13 like, you know, there are two controllers, the main
14 controller, a backup controller, but the main
15 controller failed in such a way it prevented the
16 backup controller from taking over. So it's some kind
17 of dependency that caused it. That's interesting,
18 too. You know, it is this kind of dependency we would
19 hope to capture.

20 CHAIRMAN APOSTOLAKIS: Yes, that's the
21 kind of insight we want to gain, yes. Yes,
22 absolutely, yes.

23 MR. SNODDERLY: Because mainly, I know
24 there are some folks here from Duke, but I would
25 imagine when they come in with their application for

1 Ocone, they are going to look at your database and
2 the first thing they are going to say is it's not
3 applicable to us because, you know, we -- you know, we
4 have this system and it's different than yours. Okay.
5 So your database doesn't apply.

6 But if you can say, you know, have you
7 considered this specific type of under-voltage or
8 common cause failure, they can say yes, we either have
9 that design flaw or we don't, we designed it out. So
10 I think it's something you have -- it goes back to, I
11 think, some of the concerns that maybe NRR has, is
12 that I'm going to be presented with plant-specific
13 applications of specific digital replacements, and I
14 think it's going to be much more valuable to
15 understand, as Dr. Apostolakis has said, the failure
16 modes and to identify all --

17 CHAIRMAN APOSTOLAKIS: Sure.

18 MR. SNODDERLY: -- the commonality as
19 opposed to we think digital systems of aux feed water
20 systems have this failure rate, because I'm going to
21 say my aux has that probability.

22 CHAIRMAN APOSTOLAKIS: This is the
23 cornerstone of everything we do because, for example,
24 yesterday we heard about fault injection techniques
25 and they said we start with a space and we select the

1 faults. The natural question is how do you select the
2 fault to test against what happened at Pilgrim, right?

3 This is operating experience. This is the
4 real thing. Okay? That would be a contributor. I
5 mean, it can't be their only thing, the only basis,
6 but it's certainly very important to know. So this
7 data collection thing is really, in my mind, one of
8 the most important tasks that we have in this program.
9 Now, can you speed it up, Todd, a little bit? Yes,
10 skip this and this.

11 MR. HAMZEHEE: You don't want to hear
12 conclusions?

13 CHAIRMAN APOSTOLAKIS: I don't know. What
14 is 16?

15 MR. HAMZEHEE: It would be probably
16 conclusion.

17 CHAIRMAN APOSTOLAKIS: 16, what is 16?

18 MR. HAMZEHEE: 16?

19 MR. HILSMEIER: Task 6, Development of
20 Reliability of Digital System Hardware Model.

21 CHAIRMAN APOSTOLAKIS: So you seem to have
22 decided that either a fault tree or a Markov Model
23 will be good enough. Is that what you're saying here?
24 How did you decide that? I thought you were reviewing
25 methods or you are not reviewing methods for hardware

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 then? You are reviewing methods only for software
2 failure, because the third bullet seems to say we know
3 which way to go.

4 UNIDENTIFIED SPEAKER: George, this --

5 CHAIRMAN APOSTOLAKIS: Louis has announced
6 it.

7 DR. CHU: We are really looking at kind of
8 modeling the hardware of the digital system.

9 CHAIRMAN APOSTOLAKIS: Yes. So you have
10 decided for hardware, this is the way to go?

11 DR. CHU: We feel that the Markov Model
12 captures a lot of the digital system features.

13 CHAIRMAN APOSTOLAKIS: Well, you may be
14 right, but you probably need to support that. Maybe
15 not now, but in the future.

16 MR. HAMZEHEE: I think once the work is
17 done, we're going to have some justification and
18 bases, definitely.

19 CHAIRMAN APOSTOLAKIS: What I'm saying is
20 that in the future meetings or, you know, when you
21 have to submit reports, these things have to be
22 supported. Don't just say, you know, we feel it's
23 good. The Agency does not feel, Louis. The Agency is
24 cold-blooded logic.

25 DR. CHU: We have tasks. We have tasks to

1 develop models. At that point we will evaluate it
2 more to see if it's a reasonable model.

3 CHAIRMAN APOSTOLAKIS: Anyway, what I'm
4 saying is that the message you are sending there is
5 something that may be premature.

6 MR. HAMZEHEE: We agree, but so far, based
7 on what we have seen, either fault tree or Markov
8 would be okay. I mean, not if there are some special
9 cases that may not be --

10 CHAIRMAN APOSTOLAKIS: I don't know why.
11 I mean, a fault tree I can understand, but the Markov,
12 I mean, we start playing with states and transition
13 rates when we just said that there is no date. It's
14 an interesting way of proceeding. Okay. 17?

15 MR. HILSMEIER: Task 7 involves
16 quantifying the Hardware Reliability Model. We'll
17 discuss the core contributors, the system failure
18 probability.

19 CHAIRMAN APOSTOLAKIS: Now, the hardware
20 failures, shouldn't you talk about the environment at
21 some point, I mean, what harsh environments you may
22 have and what these will do to the hardware?

23 MR. HILSMEIER: I believe that should be--
24 that would be in the failure rates, the environment
25 reflected in the failure rates. Is that correct?

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: I don't know.

2 DR. CHU: Yes, but we don't have data to
3 differentiate. If you look at what's in the Military
4 Handbook or PRISM, that kind of method, they do
5 explicitly try to account for it, but we don't know
6 what is the basis that they come up with a pi factor
7 of .35 or whatever. And then my suspicion is that
8 they may have, you know, as stated, a particular
9 component, a particular situation where they try to
10 extrapolate to other situations.

11 CHAIRMAN APOSTOLAKIS: Even without this
12 expert opinion, I mean, they feel that it was down by
13 whatever, 70 percent, but I thought that was the whole
14 point, that if you have an accident and you create
15 harsh conditions, there is concern about the hardware
16 of a machine, because under normal conditions, what,
17 you expect random failures?

18 MR. HAMZEHEE: I think qualitatively we
19 will include it, but how are we going to actually
20 quantify it and do we have data to support it. That's
21 the question.

22 CHAIRMAN APOSTOLAKIS: Oh, I don't now.

23 MR. HAMZEHEE: See, that is -- for
24 qualitatively, you are right.

25 CHAIRMAN APOSTOLAKIS: Didn't the report

1 from the National Research Council address this issue?
2 I think they did.

3 MR. HAMZEHEE: I'm not familiar with that.

4 CHAIRMAN APOSTOLAKIS: There was a report
5 on digital software in the nuclear industry. I mean,
6 it's a few years old now but, in fact, our consultant,
7 Mr. White, was a member of the group.

8 DR. KRESS: It wasn't the National
9 Research Council. Wasn't it the National Academy?

10 CHAIRMAN APOSTOLAKIS: It was the National
11 Research Council, yes. The academies issue their
12 reports through the National Research Council.

13 DR. KRESS: Oh, that's right. They do.

14 CHAIRMAN APOSTOLAKIS: It's the other NRC,
15 as they say.

16 DR. KRESS: Yes.

17 CHAIRMAN APOSTOLAKIS: So I think -- no,
18 they have a lot of good discussions there and probably
19 they are addressing this issue, too.

20 DR. CHU: George, our current task is kind
21 of limited. Look at what's available out there. You
22 know, somewhere someone has ASME database or has
23 collected some data.

24 CHAIRMAN APOSTOLAKIS: The Academy report
25 may also verify or may have information.

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 DR. CHU: In the case of software, I mean,
2 we are starting the task. We are starting the correct
3 software failure experience. It looks like they are--
4 a lot of it is interesting experience.

5 CHAIRMAN APOSTOLAKIS: These Academy
6 reports usually are reviewed by everyone and his
7 mother and it's a good idea to know what they say,
8 because there was no consensus about that. That's
9 why, in fact, it never came up with any complete
10 recommendations, because they couldn't agree. They
11 just couldn't agree, but the discussions they had
12 there might be very enlightening and they have a long
13 list of references.

14 MR. HAMZEHEE: We'll look into it.

15 MR. HILSMIEIER: Task 8 involves developing
16 an acceptable method for including software failures
17 in digital system PRAs, and the first task step in
18 Task 8 is to review software-induced failure events
19 from different industries to identify failure modes,
20 failure causes, current frequencies and to gain
21 insight into modeling software failures in the PRA.
22 This sub-task was included under recommendations from
23 ACRS. I don't recall what meeting that was, 2004.
24 And then the second --

25 CHAIRMAN APOSTOLAKIS: This is the

1 presentation that follows, right? Isn't that what
2 Steve Arndt and Tunc Aldemir is going to talk about?

3 MR. ARNDT: Pardon me? What was the
4 question?

5 CHAIRMAN APOSTOLAKIS: Development of NASA
6 modeling software failures. Isn't that what you're
7 talking about later?

8 MR. ARNDT: Not exactly. As I talked
9 about last night, we're intentionally going at this
10 from two different perspectives. This effort is
11 looking at it from more traditional efforts of looking
12 at hardware modeling and software modeling and fault
13 tree modeling and things like that. The other effort
14 is looking at it from an integrated digital systems
15 type analysis that looks at using the more
16 complicated, integrated methodologies. So it's the
17 same concept, but from a different perspective and
18 we'll take about that after this presentation.

19 CHAIRMAN APOSTOLAKIS: All right.

20 MR. HILSMIEIER: And next we'll review
21 additional literature on development of the Software
22 Reliability Model. We'll address issues such as
23 software failure rates, meaning full and consideration
24 of uncertainties and evaluate different reliability
25 methods such as fault trees, Markov, reliability

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 growth models and the other methods that we find from
2 the review.

3 Then we'll develop the Quantitative
4 Software Failure Model and evaluate existing software
5 reliability models and establish a linkage between
6 software and hardware models, and determine software
7 failure parameters that have to be quantified.
8 Different types of software have different effects on
9 digital systems and they may have to be modeled
10 differently. We'll apply the Software Reliability
11 Model again to the digital protection system for a
12 time, and the scheduled time frame for this task is
13 July 2005 to September 2008.

14 Task 9 involves quantifying the software
15 failure probabilities identified under Task 8. And
16 this task is estimated to be performed in October 2007
17 and completed by September of 2008. Task 10 involves
18 quantifying the Digital System Reliability Model
19 incorporating the hardware and software together and
20 performing --

21 CHAIRMAN APOSTOLAKIS: For all of the
22 system?

23 MR. HAMZEHEE: Yes. For instance, for RPS
24 systems.

25 CHAIRMAN APOSTOLAKIS: The digital RPS?

1 MR. HAMZEHEE: Yes, the digital RPS. The
2 analog we already have.

3 CHAIRMAN APOSTOLAKIS: No, but you would
4 not include the rods.

5 MR. HILSMEIER: That's right. And we'll
6 perform sensitivity calculations to evaluate --

7 CHAIRMAN APOSTOLAKIS: You know, there is
8 a very good discussion in that Academy report on these
9 things and for the RPS, it might work, but for other
10 systems probably not, because all it does is it gives
11 a command scram, collects data and gives a command.
12 In other situations, we're saying that the argument is
13 that you cannot just talk about the software in
14 isolation from the bigger system. If the software,
15 you know, controls parts of the hardware and receives
16 commands and all that, but in the RPS probably it's a
17 simpler system, because all it does is monitors
18 variables and says shut down.

19 MR. KEMPER: Well, if I could add. This
20 is Bill Kemper again. To a large extent that's true,
21 but it's also variable trip calculations that go
22 through the various RPSSs, so that is a bit of
23 sophistication maybe that we have to investigate.

24 CHAIRMAN APOSTOLAKIS: Right. Right.
25 True. But I mean, if there is a system where this

1 approach works, then probably this is the kind. Okay.
2 Task 10.

3 MR. HILSMEIER: Task 10 is scheduled to
4 start in October 2007 and be completed in 2008, in
5 December. Task 11 involves integrating the Digital
6 System Reliability Model into the PRA. And if we
7 choose to use Markov in that model, then we have got
8 to develop an integration method. We also need --

9 CHAIRMAN APOSTOLAKIS: Now, this work for
10 Oconee, because you mentioned Oconee several times,
11 this is not in support of the NRR activity. I mean,
12 this is just the method development within RES and the
13 reason why you're using Oconee is because you're going
14 to have information.

15 MR. HILSMEIER: That's correct.

16 MR. HAMZEHEE: Correct.

17 CHAIRMAN APOSTOLAKIS: Okay.

18 MR. HILSMEIER: And also under Task 11,
19 we'll develop guidance on when diverse systems can be
20 considered independent. And that's scheduled to start
21 in October 2007 and complete in March 2009. The last
22 task is developing, preparing a NUREG report that
23 documents all the tasks and, as you mentioned earlier,
24 we will have intermediate reports.

25 CHAIRMAN APOSTOLAKIS: Well, you gentlemen

1 may want to think about a schedule for interactions
2 with us. I mean, pass it by Eric. Not too frequent,
3 not too infrequent. Hossein, this is the report.
4 Steve doesn't want anybody else to see what the report
5 is. Okay. Any questions from the Members of the
6 Subcommittee? I guess not. Please. Please, identify
7 yourself and speak with sufficient clarity.

8 MR. WATERMAN: This is Mike Waterman with
9 Office of Research. And just going back to my
10 experience over at NRR, I would like to bring up a
11 point about using manufacturing data, is the
12 denominator in that data is going to be biased by the
13 warranty period of the equipment that's reported to
14 the vendor.

15 So if you just rely on that data, all
16 you're going to get really reported to the vendor is
17 equipment that failed during the warranty period where
18 the company using that equipment thinks they can get
19 a new piece of equipment for it. Now, if that company
20 instead has a piece of equipment fail beyond the
21 warranty period, it's more expensive for them to
22 report the data and still buy the equipment than it is
23 for them to simply buy a replacement part, stick it in
24 and get back to operation. So you're probably not
25 going to get a lot of out-of-warranty reports on 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 Let's see here. The other basis is is
2 that if you have got equipment out in the field, the
3 manufacturer says look how long my equipment has been
4 running. And then when you go out to the field, you
5 find out two years prior to that that equipment was
6 replaced by another vendor's equipment. And so you
7 can't just say well, it hasn't failed so look how long
8 it has run without failure. It might be sitting over,
9 you know, acting as a reef out in somebody's harbor by
10 then. So it's kind of hard to use manufacturing data.

11 As a matter of fact, in dedicating COTS
12 equipment, we have four processes that can be used to
13 dedicate COTS equipment for safety-related
14 applications. That's special tasks and inspections,
15 supplier surveys, source verification and use of
16 historical data. That fourth option always has to be
17 combined with one of the other three simply because,
18 you know, historical data is just not all that
19 reliable.

20 With regard to using nuclear power plant
21 LERs, keep in mind that LERs are submitted when safety
22 systems are challenged. So the only time you're going
23 to get an LER is if the reactor trips or something
24 like that happens or a piece of safety-related
25 equipment is inoperable. You may have lots of other

1 failures in a plant that have occurred. But you may
2 never hear about them, you know, it costs money to do
3 an LER if they didn't affect safety. So you have got
4 to kind of keep that factored in there also. So just
5 a couple of comments on using historical data.

6 CHAIRMAN APOSTOLAKIS: Thank you.

7 MR. HAMZEHEE: Thanks, Mike.

8 CHAIRMAN APOSTOLAKIS: Any other comments
9 from the audience?

10 MR. TOROK: Yes.

11 CHAIRMAN APOSTOLAKIS: Yes, come in, come
12 up.

13 MR. TOROK: I'm Ray Torok from EPRI and I
14 guess we have been looking at, I guess, things related
15 to this for a couple of years now and I have some
16 suggestions about, I mean, questions about what you
17 have been looking at and maybe things that would be
18 helpful.

19 One of them is have you guys looked at the
20 sensitivity of the core damage frequency to how the
21 I&C is modeled in the PRA, you know, and more
22 specifically, what is the target reliability that you
23 need from the I&C to make it a negligible contributor
24 to risk compared to everything else, because in the
25 grand scheme there are many components in each 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 you know, pumps and valves and so on, and there are
2 many systems in a plant.

3 And so it may be that the reliability you
4 need from the I&C is really pretty modest in the grand
5 scheme of things and it may not be or it may be that
6 you don't need a precise, you know, determination of
7 the reliability. At least that's the way it looks
8 from a lot of sensitivity studies that we have done.

9 Another question is in regard to the use
10 of data from other places like NASA for example. When
11 you look at NASA software, are you looking at serial
12 number one, a one of a kind of software, you know,
13 based system as opposed to a commercial device where
14 there are 40,000 or 50,000 of them in the field.

15 Now, what we found in talking with
16 commercial vendors and reviewing, doing design reviews
17 and so on on their equipment including their software,
18 is that by the time a commercial device has matured in
19 the field, the manufacturer's historical data shows a
20 trend where the software-based failures go to nothing
21 and then they stop changing the software. They stop
22 fixing it, because it's as fixed as it's going to get,
23 and the hardware failures continue, all right, which
24 is kind of what you expect, because once you have the
25 hardware right or the software right it stays stable.

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 hardware continues to degrade with time and so on.

2 We have also talked with vendors were they
3 meticulously kept records comparing their old analog
4 devices to their new digital counterparts, because
5 they wanted to prove to themselves that the digital
6 devices were at least as reliable as the old analog
7 devices, so that had data on that. Now, whether or
8 not they want to share it with you, I don't know. You
9 know, we signed non-disclosure agreements and whatnot.

10 But the manufacturers are really up to
11 speed on that and many of these cases, now, I'm
12 talking primarily about simpler components,
13 transmitters, you know, signal controllers, simple
14 devices compared to PLCs, but in those cases once the
15 software gets mature, it's mature, you know, and
16 that's the end of the changes for that.

17 So another question then that goes with
18 that is have you guys looked at the possibility of
19 comparing the analog to digital reliability to get a
20 handle on what these digital systems are, because the
21 analog systems are modeled in the PRAs right now.
22 That leaves us a black-box and, in many cases, I
23 suspect the black-box is more than adequate in the
24 context of the PRA because of all the other
25 contributors, right?

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 other thing I wonder about when you're
2 looking at the data, especially for software, is that
3 you look -- I suggest that you look at the root cause.
4 A lot of things that are determined to be or that are
5 called software failures turn out to be requirement
6 specification errors and, in fact, I know many stories
7 about digital failures at various times and every one
8 of them comes back to a requirement specification
9 error not a software error at all.

10 CHAIRMAN APOSTOLAKIS: So?

11 MR. TOROK: So then the question, of
12 course, is how do you roll that into what you do with,
13 you know, your -- with your model in PRA?

14 CHAIRMAN APOSTOLAKIS: Yes. And how is
15 that consistent with your earlier admonition to look
16 at what kind of reliability should the software have
17 compared to the hardware if the failure models are
18 different? You know, it seems to me it's not just a
19 matter of the number. It's a matter of us
20 understanding how they fail and digital software don't
21 fail in a continuous manner like analog or the non-
22 physical components.

23 MR. TOROK: No, I --

24 CHAIRMAN APOSTOLAKIS: It seems to me you
25 have to understand first the failure models.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. TOROK: I agree, and that's why in the
2 method that we're proposing, we would love to talk to
3 you more about it.

4 CHAIRMAN APOSTOLAKIS: Yes, sure.

5 MR. TOROK: And I think we should. I
6 think we should participate in some of these
7 discussions, because we have kicked these things
8 around quite a bit. And that's why we ended up
9 looking to what we call this defensive measures
10 approach where you're trying to understand and
11 evaluate the specific design features that are
12 implemented in these software-based systems to
13 preclude certain types of failures, because that has
14 a tremendous impact on the reliability and in some
15 cases, you get into very subtle things.

16 CHAIRMAN APOSTOLAKIS: Maybe what you are
17 proposing in your report, I don't know, is how to
18 manage the issue of adding software to plants, because
19 you're talking about, you know, I guess defense-in-
20 depth and diversity issues.

21 MR. TOROK: Well, yes, and what we're
22 looking at, of course, is defensive measures built
23 right into the software.

24 CHAIRMAN APOSTOLAKIS: Yes.

25 MR. TOROK: Either intentionally as a

1 defensive measure or because something inherent in the
2 design structure provides some defense against common
3 cause failure, you know, and simple --

4 CHAIRMAN APOSTOLAKIS: So your report
5 might be more useful to NRR, because these guys are
6 developing methods for assessment, the assessment of
7 this. And after that they will go to the management,
8 but you, of course, are interested in what do we do
9 now. I mean, the industry has to have something, some
10 guidance, so you're probably ahead of the curve, but
11 it doesn't hurt for them to know what is already done
12 on this.

13 MR. TOROK: You know, of course, the
14 problem we end up with is software failures aren't
15 random at all, right? So what it comes down to is
16 understanding what kinds of failures the software is--

17 CHAIRMAN APOSTOLAKIS: You see, that's why
18 I keep questioning the use of Markov Models. You
19 know, they are not random. We have to understand that
20 and appreciate that. Now, there may be some instances
21 where, you know, the models are fine but, you know,
22 you have to really conclude that after some argument.

23 MR. HAMZEHEE: Yes.

24 CHAIRMAN APOSTOLAKIS: Okay.

25 MR. HAMZEHEE: And I think there were some

1 good remarks and I would like to just make two points
2 that are related. One is right now, as we speak and
3 as you know, the reliability of, for instance, analog
4 RPS is like a $1E^{-6}$ failure probability. So if they
5 are so highly reliable, can you beat that with the
6 digital?

7 CHAIRMAN APOSTOLAKIS: Anyway, the --

8 MR. HAMZEHEE: So we have to make sure,
9 number one, how they compare.

10 MR. TOROK: Well, there is --

11 CHAIRMAN APOSTOLAKIS: No, he wants you to
12 compare it with the failure rates of pumps.

13 MR. HAMZEHEE: Well, but right now this is
14 with RPS?

15 CHAIRMAN APOSTOLAKIS: Then you are at
16 least more free.

17 MR. HAMZEHEE: Because they are highly
18 reliable with analog systems. We don't know how
19 reliable the digital is, number one. Number two,
20 you're right again with respect to the software, but
21 the problem that we may have, and we don't know
22 because of some of these unknowns, is the software is
23 highly reliable, but if there is a bug someplace, it
24 can bypass all the redundancies within your system.
25 So that could wipe out the whole system. That's why

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 you have got to be careful as to not allow any
2 failures in your software.

3 CHAIRMAN APOSTOLAKIS: If it fails, you
4 don't know how it's going to fail.

5 MR. HAMZEHEE: Exactly. You could wipe
6 out the whole system regardless of how many channels
7 you have, how many redundancies you have.

8 MR. TOROK: That's true and the thing that
9 typically gets software into trouble is when it
10 encounters conditions that were unanticipated by the
11 designer or untested, that sort of thing. Well, it
12 turns out there are many defensive measures that can
13 be incorporated into the design of the feature, I
14 mean, into the design of the software, I'm sorry, to
15 handle those things. So that's why in our method it's
16 very important to find those.

17 CHAIRMAN APOSTOLAKIS: Anyway, maybe the
18 message here is that -- oh, I'm sorry.

19 DR. BONACA: You made a statement
20 regarding, you know, the importance of using
21 commercial devices where the potential is that since
22 you have the software so, therefore, the software
23 folds back under from that.

24 CHAIRMAN APOSTOLAKIS: Yes.

25 DR. BONACA: But I always sense that for

1 power plants, I mean, the way I see it, if I think
2 about replacement RPS and ESF, it's going to be really
3 probably one or two applications at least in the
4 short-term. So how does that insight apply? I mean,
5 am I misunderstanding what you're communicating there?

6 MR. TOROK: Well, I'm not sure. Let me
7 try this in -- a number of the applications that are
8 being done right now, like at Oconee they are using a
9 Teleperm XS platform, right, a commercial device, a
10 commercial PLC.

11 DR. BONACA: Commercial? Let me
12 understand now, commercial?

13 MR. HAMZEHEE: He is saying you can't use
14 commercial, because these are safety-related systems.
15 How can you use commercial for RPS, for instance?

16 MR. TOROK: Well, there is commercial
17 grade dedication to get commercial grade equipment in
18 there. In the case of the Teleperm, it has been
19 reviewed by NRR and there is an SER out on it. So
20 those things have been done.

21 MR. HAMZEHEE: There's a quality
22 requirement even for commercial. You have some
23 quality requirement.

24 DR. BONACA: The software logic is going
25 to be one application, right? The software logic 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 you have put in on this platform is going to be one
2 application.

3 MR. TOROK: That's right. That's a good
4 point. So what you find in a platform like that where
5 it's a very flexible platform by design, right, the
6 weak link from a software standpoint isn't in the
7 invented software that's on the platform or the
8 operating system or any of that stuff. The weak link
9 is the application code. That's where you have got to
10 be very careful.

11 DR. BONACA: And that's what we're
12 concerned about.

13 MR. TOROK: That's right. So the object
14 in a case like RPS is to keep that as painfully simple
15 as you can, right, and then to go through the right QA
16 process and so on.

17 DR. BONACA: And that's what troubles me
18 somewhat. This goes back to the presentations we had
19 yesterday morning regarding the new approach. For
20 example, we go from Reg Guides who are very
21 prescriptive about what you're going to monitor and
22 what controls you have in the RPS to one for new
23 plants that is very generic, general, provides all
24 these error guidelines.

25 And you know, my concern is, you know,

1 maybe the proliferation of uses that you may have, so
2 you get the bigger software on a bigger platform as a
3 capacity, so that you can handle more things, and I
4 think that in general brings with itself a higher
5 fault probability, it seems to me.

6 MR. TOROK: I agree, so it's the weakest
7 link. Nothing is better than keeping it simple.

8 DR. BONACA: Yes. I'm trying to
9 understand how you go about 4b.

10 CHAIRMAN APOSTOLAKIS: But not simpler, as
11 Einstein said.

12 DR. BONACA: Yes. But even, you know, I
13 mean, after TMI, for example, one of the objectives
14 was the one of minimizing literally the functions that
15 you put in front of an operator, make them really
16 meaningful, so that you have a good picture but, you
17 know, the word at that time a lot of companies that
18 proposed very large systems with many more functions,
19 etcetera, and the objective was they want to say
20 forget about this stuff. You want to focus on really
21 critical pieces of communication to the operators.
22 Okay? And I am trying to understand how the digital
23 systems are going to go away from this philosophy,
24 maybe. I don't know.

25 MR. HILSMEIER: That's a good point.

1 MR. TOROK: It's certainly concerned with
2 the digital systems and a fair question to ask is what
3 have you done to make sure that you're not going to
4 overwhelm the operator or have made it too
5 complicated? Is this a fair question?

6 DR. BONACA: Or create again other failure
7 modes inside the software that were not foreseen.

8 MR. TOROK: That's right. And the other
9 thing, the same consideration, if you add a diverse
10 backup for a software-based system to deal with the
11 common mode failure, because you add complexity when
12 you do that, so you want to be careful about where you
13 do that.

14 CHAIRMAN APOSTOLAKIS: Thank you very
15 much. Anybody who wants to be hated? We will
16 reconvene at 3:15.

17 (Whereupon, at 3:00 p.m. a recess until
18 3:20 p.m.)

19 CHAIRMAN APOSTOLAKIS: Back in session.
20 The last presentation will be by Mr. Arndt and
21 Professor Aldemir of Ohio State. Is that the plan?
22 Yes.

23 PROF. ALDEMIR: Yes, sir.

24 CHAIRMAN APOSTOLAKIS: And you need, what,
25 an hour and 45 minutes or something like that?

1 MR. ARNDT: An hour and a half to two
2 hours depending upon how many questions we get.

3 CHAIRMAN APOSTOLAKIS: There are no
4 questions.

5 MR. ARNDT: Yes, right. I will be giving
6 the first part of this presentation and since you have
7 heard more than enough of me for the last two days,
8 Professor Aldemir will be giving the latter part of
9 the presentation. Why don't you go ahead?

10 CHAIRMAN APOSTOLAKIS: Now, there is also
11 a report, which is a NUREG draft report out of Tunc's
12 shop.

13 MR. ARNDT: That was provided for
14 background.

15 CHAIRMAN APOSTOLAKIS: Just background.

16 MR. ARNDT: Yes.

17 CHAIRMAN APOSTOLAKIS: You are not asking
18 us to comment on it.

19 MR. ARNDT: No, it's a draft, so just
20 background.

21 CHAIRMAN APOSTOLAKIS: But it will become
22 a NUREG report.

23 MR. ARNDT: If we decide that it's of
24 sufficient quality, etcetera, etcetera, then it is
25 anticipated it to become a NUREG report.

1 CHAIRMAN APOSTOLAKIS: But I'm just
2 wondering. I mean, there is some speculation here
3 that a rating of various methods against some
4 criteria, I don't know, I mean --

5 MR. ARNDT: We'll talk about that today.

6 CHAIRMAN APOSTOLAKIS: Ah, okay. Go
7 ahead.

8 MR. ARNDT: Just as some basic background,
9 we talked about this a lot last night. The NRC
10 encourages the use of PRA and associated analyses to
11 the extent possible. In the National Academy study,
12 as well as the ACRS letter associated with it, they
13 encouraged the development of risk-informed
14 application in this area.

15 Particularly, to go back to the National
16 Academy study, the specific recommendation was that
17 the NRC should strive to develop methods for
18 establishing the failure probabilities of digital
19 systems for use in probabilistic safety assessment.
20 These methods should include acceptance criteria
21 guidelines, limitations of use and for rationalization
22 and justification for the methods chosen.

23 So the idea behind this is to look at the
24 different kinds of methodologies. As has been
25 recommended by the ACRS, it would be preferable if we

1 could do this in an integrated fashion. Now, we may
2 not be able to do that, but what we want to do is look
3 at near term PRA applications, which means you have to
4 integrate the rest of the current PRA and develop them
5 in such a way that it makes the most sense.

6 So because of this, what we need to do is
7 look at the need to account for dynamic interactions
8 with the process, the interactions between the digital
9 system itself, the various components in the digital
10 system as well as the systems that they are
11 controlling and tripping.

12 So as I mentioned yesterday, what we're
13 trying to do is look at this from two different
14 aspects, one from the traditional fault tree/event
15 tree analysis, one from a dynamic modeling analysis.
16 So what we're trying to do is figure out whether or
17 not you can build models that can account for these
18 effects and then feed them into our current regulatory
19 structure.

20 As we talked about yesterday, we have an
21 overall program plan that looks like this. What I
22 have done is I have shaded in green the areas that
23 this presentation is referring to. In the previous
24 presentation that Hossein gave, they are looking at
25 some of the other parts of the program. So 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 example, the failure modes, the traditional methods,
2 hardware, software quantification and the evaluation,
3 that's a simplified version of their chart. On the
4 other side, the stuff we're going to talk about this
5 afternoon, is looking at the dynamic modeling
6 methodologies.

7 CHAIRMAN APOSTOLAKIS: But several of the
8 methods that you will talk about have not been
9 designed just for dynamic methods. I mean, I'm
10 surprised that the guys on the left have not looked at
11 that and they just talk about traditional fault trees
12 and Markov. I mean, we will see them later, but --

13 MR. ARNDT: Yes, you can --

14 CHAIRMAN APOSTOLAKIS: I mean, the two
15 groups don't seem to talk to each other, do they?

16 MR. ARNDT: We do talk to each other.

17 CHAIRMAN APOSTOLAKIS: Over the phone?

18 MR. ARNDT: Yes, but we're down the hall
19 from each other. It's a challenge.

20 CHAIRMAN APOSTOLAKIS: But, Todd, really,
21 I mean, in your presentation I would have expected to
22 have seen a longer list of potential methods from
23 which you will pick one after you decide what is
24 applicable to your methods like these guys have been
25 doing, and I know what methods Tunc is going to talk

NEAL R. GROSS

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

1 about. I mean, some of them are unique to dynamic
2 systems in the sense that Tunc is talking about, but
3 not all of them.

4 MR. ARNDT: No.

5 CHAIRMAN APOSTOLAKIS: Not all of them.

6 MR. ARNDT: And what I think Todd was
7 trying to say is this is an example of a methodology.
8 They haven't come up with their actual solution yet.

9 CHAIRMAN APOSTOLAKIS: No, but the way
10 they were presenting it, they said we'll go either
11 with fault trees or with Markov. That means that's
12 it, one of the two. And now, we're going to hear
13 about five or six methods and I think most of them
14 apply to them as well.

15 MR. ARNDT: They potentially apply.

16 CHAIRMAN APOSTOLAKIS: Yes, potentially,
17 potentially, maybe, perhaps.

18 PROF. ALDEMIR: May I make a comment here?
19 My name is Tunc Aldemir and I am a faculty with Ohio
20 State University. I have been working with
21 Probabilistic Risk Assessment for over 20 years and
22 specifically in dynamic methodologies.

23 What I think the issue here, which was
24 mentioned earlier, is that we are approaching it from
25 -- I mean, it's the diversity issue like we had

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 national, what is it, Los Alamos and Sandia and then
2 Lawrence Livermore, not really competitors, but doing
3 different methodologies. We are approaching the same
4 problem using different approaches. I think that's
5 the issue, right?

6 CHAIRMAN APOSTOLAKIS: I don't know why
7 you guys are commenting on what I said so much.

8 MR. ARNDT: Okay.

9 CHAIRMAN APOSTOLAKIS: All I said was that
10 they did not present a complete set of potential
11 methodologies and I keep hearing well, we're doing it
12 two different ways and perhaps and potential. I think
13 it's a true statement.

14 MR. ARNDT: It is.

15 CHAIRMAN APOSTOLAKIS: Yes.

16 MR. ARNDT: Onward. So the objective of
17 the study is, basically, to look at the different
18 kinds of methodologies that might be available, make
19 some conclusions and choose the kinds of methodologies
20 we can use, develop an understanding of the potential
21 advantages and disadvantages and do some pilot studies
22 on the proposed methodologies.

23 As you heard earlier, the other side of
24 the problem is also going to do some pilot studies and
25 what we're planning on doing is having at least two

1 different pilot studies, one that has the likelihood
2 to be more successful than traditional modeling like
3 RPS, and one that has more likely challenges
4 associated with dynamic modeling like the auxiliary
5 feed water system.

6 So we're going to look at the various
7 issues associated with the current PRA modeling
8 methodologies, fault trees/event trees, review the
9 advantages and limitations of dynamic methodologies,
10 review the industry practices, has anybody else used
11 dynamic methodologies effectively, look at the
12 existing regulatory framework and what does that drive
13 us toward?

14 What do we need to accomplish? What level
15 of detail do we need to do, so this might be
16 implementable from a regulatory standpoint. And then
17 look at the minimum requirements associated with doing
18 this. Is there something associated with the dynamics
19 of the failures or with the system itself that
20 requires us to do this? We don't want to do this
21 simply as an academic exercise if the particular
22 interactions in the system --

23 CHAIRMAN APOSTOLAKIS: So don't go to Ohio
24 State.

25 MR. ARNDT: Yes.

1 CHAIRMAN APOSTOLAKIS: Well, you have a
2 professor and you are asking him not to do an academic
3 exercise.

4 MR. ARNDT: Yes.

5 CHAIRMAN APOSTOLAKIS: All right.

6 MR. ARNDT: But the point that we're
7 trying to make is if we do this research and it turns
8 out that these are really neat methodologies, but they
9 are not necessary to get an accurate answer, we don't
10 want to require or encourage the industry to do
11 something more than is necessary. Now, there may be
12 situations where you do need it and that's what we're
13 trying to understand, and we believe that there is at
14 least a good possibility that that's the case or we
15 wouldn't be doing it. And then identify the
16 requirements associated with it.

17 CHAIRMAN APOSTOLAKIS: Okay.

18 MR. ARNDT: So at this point, I'm going to
19 let Tunc talk for awhile and you can give him a hard
20 time.

21 PROF. ALDEMIR: Okay. When we got the
22 task -- I went through the introduction, I guess.
23 When we got the task, we said what is it that makes
24 analog systems different from digital systems? So we
25 looked through the literature and we really didn'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 find a complete list. Actually, we didn't even find
2 a partial list. So we tried to characterize.

3 Incidentally, on this project, we have
4 three people who are professional computer science
5 people, two professors and one student, so the
6 computer expertise is not being provided by the
7 nuclear people.

8 CHAIRMAN APOSTOLAKIS: By the way, do you
9 have anybody at Ohio State in the Computer Science
10 Department who worries about software failures?

11 PROF. ALDEMIR: There is no such person.

12 CHAIRMAN APOSTOLAKIS: There is nobody
13 anywhere in the Computer Science Department.

14 PROF. ALDEMIR: No, you are right. You
15 are right. I checked for that, because I wanted to
16 establish a Reliability Engineering Program a long
17 time ago. There is no such person, but we will have
18 somebody who is as close to it as you can get. That's
19 Mike Stusky, who is working on our project. So what
20 we found are the following and, again, this is
21 probably not a complete list, but this is the best we
22 could come up with.

23 First of all, the firmware and software
24 components of the digital I&C systems do not
25 demonstrate any wear characteristics, so they 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 respond to accelerated testing, stress testing,
2 etcetera, so it's hard to test them the way you would
3 do hardware. Firmware, software reliability cannot be
4 accurately modeled using your bathtub curve approach.
5 What happens is that you have the infant mortality
6 come down and come to sort of a plateau and then
7 slightly increase, because every time you fix software
8 you may be messing it up more.

9 So then the third difference is that, and
10 this is a big one, there may be complex interactions
11 between the constituents of the digital I&C system and
12 between the digital I&C system and the process
13 physics, which may lead to potentially significant
14 dependencies between failure events, such as digital
15 I&C systems rely on sequential circuits that have
16 memory, and so the system response is not just
17 dependent on the existing system state, but also on
18 the system history as well as the rate of progress.

19 Tasks may compete for digital controllers
20 resources, which may lead to problems such as deadlock
21 and starvation. Choice of external/internal
22 communication mechanisms for the digital I&C system,
23 such as buses and networks, and the communication
24 protocol affects the rate of data transfer. The
25 ability to coordinate multiple digital controllers

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 directly and explicitly may necessitate a finer degree
2 of communication and coordination between controllers.
3 A digital --

4 CHAIRMAN APOSTOLAKIS: I don't know what
5 that means.

6 PROF. ALDEMIR: Right now, I will go
7 through an example. I will go through an example
8 later on to show process couples events.

9 CHAIRMAN APOSTOLAKIS: Okay. Okay. We
10 can do that later.

11 PROF. ALDEMIR: And all I'm saying here is
12 that it makes it tighter. A digital controller can
13 remain active and not only react to data, but
14 anticipate the state of the controlled monitoring
15 system and actually do prognosis rather than just
16 diagnosis.

17 CHAIRMAN APOSTOLAKIS: Now, this is, your
18 bullet here, your third bullet, not the second, but
19 the third one, really the major issue in the software
20 safety community and that's why I said earlier for the
21 reactor protection system, you may be able to model
22 the software sort of independently of the rest of the
23 system. But in general, the school of thought that
24 follows that says that the software is embedded in the
25 hardware system that it controls and you have to study

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 it as one system. Okay. And I still think that
2 applies to the other guys, too. It's not just you.

3 MR. ARNDT: Well, the issue is --

4 CHAIRMAN APOSTOLAKIS: And this is a major
5 issue that was discussed in the Academy.

6 MR. ARNDT: Yes. And the issue is where
7 do you draw that line until you go at it from both
8 sides?

9 CHAIRMAN APOSTOLAKIS: If you want to draw
10 a line.

11 MR. ARNDT: Yes, if you want to.

12 CHAIRMAN APOSTOLAKIS: I don't even know
13 why you draw it.

14 PROF. ALDEMIR: Another important
15 difference is that the failure modes of the digital
16 I&C system are not defined, well-defined. For
17 example, failure of one component, constituent of the
18 system can affect the rest or other parts of the
19 overall system. A system may not fail only on
20 specific input, but on other inputs that are
21 semantically similar or even equivalent or correlated.

22 Software may be able to mask intermittent
23 failures in hardware, so it may be failed, but you may
24 not be aware of it. And there is an example here.
25 Digital I&C systems share data transmissions,

NEAL R. GROSS

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

1 functions, process equipment, which makes them more
2 vulnerable to common cause failure. It is possible
3 for the I&C system to introduce new events, new
4 failure events and also, as part of this as well,
5 multi-testing may introduce new failure dependencies
6 between systems.

7 Software is not a physical entity and
8 testing alone is not sufficient to verify that
9 software is complete and correct and, in fact, there
10 is a fair amount of literature on this. And software
11 defects may remain hidden for long periods and
12 suddenly appear when a certain execution path is
13 exercised.

14 CHAIRMAN APOSTOLAKIS: Which is typical of
15 design error.

16 PROF. ALDEMIR: Right.

17 CHAIRMAN APOSTOLAKIS: If you have a
18 design error that will appear only if you have a
19 strong earthquake, you know, that's the problem.

20 PROF. ALDEMIR: In fact, this came up
21 before and I want to make a comment as to the use of
22 conventional reliability models or potential use of
23 the conventional reliability models to model software
24 failures. Solenoid wells have a failure PDF,
25 probability distribution function, for failure that is

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 almost like a delta function. So you know, there is
2 an analog in the hardware world and what we are
3 talking here, if nothing happens, unless something
4 happens and so it's like a delta function.

5 CHAIRMAN APOSTOLAKIS: For equipment that
6 are there to mitigate the consequences of severe
7 external events, this is a major issue. If I have a
8 major earthquake, if I have a major tornado and I have
9 built into my plan systems and components that will
10 protect me against those, it is a design error there
11 I have never known until I'm hit. So in the hardware
12 there is exactly the same problem.

13 PROF. ALDEMIR: There is a problem.

14 CHAIRMAN APOSTOLAKIS: And if they find in
15 one of the plants, they had problems, that they had
16 run out of oil or lubricant or something, I don't
17 remember now, it was in the old days. A previous
18 incarnation of the ACRS worried about design errors
19 every time they met, so this is very well-known.

20 PROF. ALDEMIR: Well, this has been
21 discussed already, so I'm not going to spend too much
22 time and the previous presentation covered much better
23 than I am covering.

24 CHAIRMAN APOSTOLAKIS: Well, let me ask
25 you this. We always keep saying about other

1 industries. Have we ever found anything in other
2 industries that was useful to us?

3 PROF. ALDEMIR: No.

4 CHAIRMAN APOSTOLAKIS: No.

5 PROF. ALDEMIR: The answer is no from my
6 side.

7 CHAIRMAN APOSTOLAKIS: The answer is no.

8 PROF. ALDEMIR: There is one exception and
9 then, this is the last bullet. NASA, of course, has
10 been using dynamic methodologies for awhile, so that
11 is an --

12 CHAIRMAN APOSTOLAKIS: A small group at
13 NASA, not NASA itself.

14 PROF. ALDEMIR: But they are very much
15 interested in doing right now.

16 CHAIRMAN APOSTOLAKIS: Yes.

17 PROF. ALDEMIR: Mike Stamatelatos wants to
18 actually join forces with NRC on this.

19 CHAIRMAN APOSTOLAKIS: A lot of people are
20 interested, but what are they doing?

21 PROF. ALDEMIR: Well, we'll try to
22 coordinate.

23 CHAIRMAN APOSTOLAKIS: Yes.

24 PROF. ALDEMIR: Okay. So the question is
25 -- and we kept mentioning dynamic methodologies, but

NEAL R. GROSS

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

1 we did not really justify it. The justification
2 changed through implicit statements. I mean, when I
3 was listening to differences between digital systems
4 and analog systems, the need was implicit, but I want
5 to make it a little bit clearer here.

6 What happens is that these dynamic
7 interactions between plant processes and triggered and
8 stochastic events, which may happen in reactor
9 protection and control systems, may lead to coupling
10 between failure events and I will illustrate that
11 later on by an example from feed/bleed cooling of a
12 PWR following a small break.

13 Cases reported in the literature, and
14 there aren't too many of them as far as I know, maybe
15 three or four, all on this process control system
16 interaction indicate that the event tree/fault tree
17 approach may yield conservative, but this may be an
18 important point, but may be overly conservative
19 results. This may be a point for the industry maybe.

20 Omission of failure scenarios is possible
21 if dynamic interactions between plant physical
22 processes and triggered or stochastic logical events
23 are not accounted for. The first study, as far as I
24 know and it may be the only study as far as I know, is
25 by Cacciabue and Amendola and Cojazzi. It's about,

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, 15, almost 20 years old. They discovered that
2 you may be missing important scenarios if you don't
3 use -- if you use static methods in conventional event
4 tree/fault tree.

5 And dynamic methodologies, I will define
6 formally in a little while, will be needed only for
7 systems in which significant interactions are
8 possible. If they are not and RPS system is a good
9 candidate, but as was mentioned earlier, there may be
10 also complex interactions within that system through
11 the software, so we are not too clear if it's really
12 going to be applicable. But if there is any system,
13 reactor-related system, that is probably a good
14 candidate.

15 We need to worry about two types of
16 interactions. The first one is the interaction
17 between the I&C system and, in our case, the reactor
18 protection and control system and controlled and
19 monitored plant physical processes, such as heatup and
20 pressurization of the reactor and level control, which
21 I will call Type I interactions. This is not standard
22 from literature. We are just inventing the
23 terminology, Type I interactions.

24 And I call them Type I, because
25 historically they were the first ones 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 discovered. Interactions between the constituents of
2 the reactor protection and control system itself, such
3 as communication between different components, multi-
4 tasking, multiplexing, and there are lots more. So we
5 call them Type II interactions.

6 From a reliability modeling viewpoint,
7 Type I and Type II interactions are separable only for
8 single-input, single-output I&C systems.

9 CHAIRMAN APOSTOLAKIS: Like a scram
10 system.

11 PROF. ALDEMIR: Even then, again, it
12 depends how many single-input, single-output. Yes,
13 multiple-input, single-output I am not too sure. This
14 assessment you validated but, again, you know, it's
15 kind of speculative at least, but sounds reasonable,
16 I guess.

17 Generally, it is difficult to integrate a
18 dynamic model into existing plant PRAs, almost all of
19 which are based on the ET/FT approach. Now, this is
20 a critically important point, because there are
21 dynamic methodologies available and I believe you can
22 use them for all sorts of fancy modeling, however
23 fancy your system may be. But then what do you do
24 with the results is a big issue, because it has to go
25 into a complete plant PRA and that is based on codes

NEAL R. GROSS

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

1 like SAPHIRE and CAFTA.

2 So you have to come up with cut sets. You
3 have to come up with the dependencies between. You
4 have to figure out the boundaries of the system within
5 the existing PRA, take it out, put the new one in.
6 That's a major task and I don't think that anybody
7 knows how to do that yet.

8 So what are dynamic methodologies, and I
9 will look at first for Type I interactions. There are
10 three types, three major types, continuous time
11 methods, discrete time methods and what I call visual
12 methods. I first called it graphic methods. My
13 colleagues did not like it, so I called it visual
14 methods and most of which are semi-dynamic and I will
15 define that in a little while.

16 So continuous time methods. The first one
17 is the continuous, not the first one historically, but
18 the one that is most comprehensive and then includes
19 almost everything else, is called the continuous event
20 tree approach, which was proposed by the late Jacques
21 Devooght from the Free University of Belgium, a very
22 elegant theory. It consists of a set of linear
23 integral differential equations. It includes
24 everything about the system. You can model almost
25 anything that you want, but it's very complicated,

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 too.

2 Then there is the discreet space, but
3 continuous time analog of this. The one problem with
4 CET or the continuous event tree is that it is hard to
5 model transitions on demand or failures on demand. So
6 we came up with a discreet space version of it. This
7 one, the continuous cell-to-cell mapping technique,
8 which allows failures or modeling failures on demand.

9 When you go to discreet time methods, of
10 course, the first one is Monte Carlo. I mean, if you
11 could --

12 CHAIRMAN APOSTOLAKIS: What do you mean?
13 Monte Carlo is a method of propagating uncertainties.
14 Why is that a discreet time method?

15 PROF. ALDEMIR: You can do the same thing
16 to failures.

17 CHAIRMAN APOSTOLAKIS: But Monte Carlo you
18 can use everywhere.

19 PROF. ALDEMIR: Right, right, right.

20 CHAIRMAN APOSTOLAKIS: I mean, it's a
21 method for solving a problem. It's not a model or a
22 methodology.

23 PROF. ALDEMIR: But it is a methodology to
24 approach the problem. If you really can afford the
25 computational time, in fact, that's the best thing 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 do.

2 CHAIRMAN APOSTOLAKIS: But you will still
3 need a model and you may still need the CET.

4 PROF. ALDEMIR: You will need a failure
5 model, sorry, a probability distribution function to
6 describe your failure. You are right in that. But
7 when I say --

8 CHAIRMAN APOSTOLAKIS: Not only that, but
9 I mean how the components interact, how they interact
10 with the process system. I mean, this is just a
11 method for --

12 PROF. ALDEMIR: If you have a system
13 simulator and you use a model --

14 CHAIRMAN APOSTOLAKIS: So I will need a
15 model.

16 PROF. ALDEMIR: Yes, you are right.

17 CHAIRMAN APOSTOLAKIS: I need a model.

18 PROF. ALDEMIR: Right.

19 CHAIRMAN APOSTOLAKIS: This is not a
20 methodology like DYLAM, for example, DYLAM is a
21 methodology.

22 PROF. ALDEMIR: You are right.

23 CHAIRMAN APOSTOLAKIS: And Monte Carlo is
24 not.

25 PROF. ALDEMIR: When I said methodology,

NEAL R. GROSS

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

1 I implicitly was thinking of stochastic methodologies.

2 CHAIRMAN APOSTOLAKIS: I would delete it
3 from here. I mean, it's just a tool for --

4 PROF. ALDEMIR: Okay.

5 CHAIRMAN APOSTOLAKIS: -- working with any
6 of those.

7 PROF. ALDEMIR: Okay. Then there is a
8 dynamic event tree generation approach and there is a
9 slew of methodologies. DYLAN is the first one as far
10 as I know, developed by Ispra Mendelo and I think
11 Mendelo was the main contributor. Then there is the
12 one that Nathan Siu developed at MIT while he was at
13 MIT. They are similar in principle, but they differ
14 in branching rules. Then there is the Accident
15 Dynamic Simulator by Ali Mosleh at the University of
16 Maryland. There is the Integrated Safety Assessment
17 methodology developed by --

18 CHAIRMAN APOSTOLAKIS: This is what the
19 chemical guys use?

20 PROF. ALDEMIR: No, no, this is by Jose
21 Izquierdo from Spain.

22 CHAIRMAN APOSTOLAKIS: Because there is an
23 ISA that is being used by the MOX people. Is that
24 what they call it, Integrated Safety Analysis?

25 MR. SNODDERLY: Right.

NEAL R. GROSS

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

1 CHAIRMAN APOSTOLAKIS: This is not it?

2 MR. SNODDERLY: Right. No, it's something
3 else.

4 PROF. ALDEMIR: No, this is not it. This
5 is by Jose-Maria Izquierdo from Spain and the Spanish
6 NRC, by the way, or their equivalent of it is using it
7 to assure that the scenarios are complete for the
8 licensee reports. And there is the cell-to-cell
9 mapping technique, which was developed at Ohio State
10 and it's a discreet time, discreet space version of --

11 CHAIRMAN APOSTOLAKIS: So there is one
12 less C.

13 PROF. ALDEMIR: One less C, yes.

14 CHAIRMAN APOSTOLAKIS: Which C did you
15 drop?

16 PROF. ALDEMIR: Actually, historically,
17 this came first. This came later and this came last.

18 CHAIRMAN APOSTOLAKIS: Yes, but, I mean,
19 what is the extra C? It stands for what?

20 PROF. ALDEMIR: Continuous cell-to-cell
21 mapping technique.

22 CHAIRMAN APOSTOLAKIS: Oh.

23 PROF. ALDEMIR: Cell-to-cell.

24 CHAIRMAN APOSTOLAKIS: There should have
25 been a D there. Where is the D?

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 PROF. ALDEMIR: Discreet.

2 CHAIRMAN APOSTOLAKIS: Discreet.

3 PROF. ALDEMIR: Okay. Professor
4 Apostolakis is going to argue with that probably, but
5 there is also a DDET/MC. DDET/MC is a dynamic event
6 tree generator developed by --

7 CHAIRMAN APOSTOLAKIS: That's okay. We
8 don't need it.

9 PROF. ALDEMIR: -- a Belgian chap, Pierre-
10 Etienne Labeau, Pierre-Etienne Labeau, but what
11 happens with the MC part is it is used to quantify
12 uncertainties associated with the inputs to dynamic
13 event tree. See, there are two types of uncertainties
14 and I'm talking about aleatory and epistemic, but
15 there are two types of uncertainties that you need to
16 analyze when you look at the event tree.

17 Firstly, the branching probabilities and
18 the numbers you use are just numbers and you don't
19 know if you are right or not. So there is one
20 approach which likes to sample over a given
21 distribution rather than using discreet numbers.
22 There is another approach, which uses the Latin
23 Hypercube, that means that you generate more than one
24 branch, and then you say, but you started an
25 initiating event. How do you know your initiating

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 event was right in the first place? So you have to
2 sample over the uncertainties in the initiating event
3 and that's where the MC part is coming from.

4 I'm sorry. I'm sorry. I get in a
5 lecturing mode. Visual methods. You know, the common
6 denominator for these methods is that they have all
7 graphical interfaces. You can look at them and you
8 see system topology.

9 CHAIRMAN APOSTOLAKIS: But again, I don't
10 know. I mean, isn't the Petri net a discreet time,
11 discreet space and state?

12 PROF. ALDEMIR: You can look at it
13 different ways, true.

14 CHAIRMAN APOSTOLAKIS: But is it true?

15 PROF. ALDEMIR: Yes, sure. But as I said,
16 the common point is that --

17 CHAIRMAN APOSTOLAKIS: You have --

18 PROF. ALDEMIR: -- of these methods is
19 that the commonality is going to be the visual aspect
20 of it.

21 CHAIRMAN APOSTOLAKIS: No. I mean, you
22 really have to make that very clear, I mean, in your
23 report or whatever. I understand the difference
24 between continuous time and discreet time. They are
25 different things. What you call visual, I mean, they

NEAL R. GROSS

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

1 fall into one of the previous two categories. The
2 additional thing they have is that, as you say, you
3 know, they pictorially represent what is going on.
4 This is definitely a discreet time, discreet state,
5 isn't it?

6 PROF. ALDEMIR: Sure.

7 CHAIRMAN APOSTOLAKIS: And the same
8 applies to DFM?

9 PROF. ALDEMIR: Oh, yes, yes. I mean,
10 dynamic flowgraphs.

11 CHAIRMAN APOSTOLAKIS: Yes, right.

12 PROF. ALDEMIR: GO-FLOW.

13 CHAIRMAN APOSTOLAKIS: Yes. I mean, all
14 of these are one of the previous two groups.

15 PROF. ALDEMIR: Yes. The reason I grouped
16 them differently, and -- well, dynamic flowgraph, GO-
17 FLOW, Dynamic Fault Tree, Event Sequence Diagrams.
18 Oh, sorry. We'll come to that.

19 CHAIRMAN APOSTOLAKIS: Oh.

20 PROF. ALDEMIR: The reason --

21 CHAIRMAN APOSTOLAKIS: But DYLAM is
22 pictorial, too, is it not?

23 PROF. ALDEMIR: Not really, no. You don't
24 have to come up with a visual outlay of system
25 topology before you can start your model. These you

NEAL R. GROSS

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

1 have to.

2 CHAIRMAN APOSTOLAKIS: So what I would
3 suggest is that you place them in the previous two
4 categories as appropriate, and then you put an
5 asterisk or something next to them and say these are
6 also visual.

7 PROF. ALDEMIR: Okay.

8 CHAIRMAN APOSTOLAKIS: They have a visual
9 component.

10 PROF. ALDEMIR: That's a good suggestion.

11 CHAIRMAN APOSTOLAKIS: Because it took me
12 awhile to figure that out. I say why is he doing it
13 that way?

14 PROF. ALDEMIR: Well, you know, if you
15 really look --

16 CHAIRMAN APOSTOLAKIS: No, look, I
17 understand.

18 PROF. ALDEMIR: But --

19 CHAIRMAN APOSTOLAKIS: Let's go on,
20 because it's kind of late.

21 PROF. ALDEMIR: All right. Fine. Well,
22 I put the disclaimer that this is only my brainchild.
23 Nobody else is to blame and I take all the blame.

24 CHAIRMAN APOSTOLAKIS: Yes. The problem
25 with these categorizations, Tunc, is that when you say

NEAL R. GROSS

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

1 "accuracy," when you say "ease," when you say
2 "desirability," you have to have some quantitative
3 measure because, you know, otherwise I don't know why
4 you gave a 10 to ESD. I mean, what is that, you know,
5 Event Sequence Diagram.

6 PROF. ALDEMIR: Well, I can explain that.

7 CHAIRMAN APOSTOLAKIS: But I don't even
8 think it's a methodology. It's just a reliability
9 block diagram.

10 PROF. ALDEMIR: No, no, not really.

11 CHAIRMAN APOSTOLAKIS: Oh, come on.

12 PROF. ALDEMIR: Not really. Not really.

13 CHAIRMAN APOSTOLAKIS: And where is the
14 event tree approach? Do you have the event tree
15 there?

16 PROF. ALDEMIR: The event tree is -- these
17 are dynamic, these are dynamic. You have -- of
18 course, the dynamic event tree is a whole bunch of
19 them, DYLAN, DETAM, DDET, ADS and so forth, but event
20 tree is not here.

21 CHAIRMAN APOSTOLAKIS: Why? I mean, I
22 don't want to get in details over this. DFM gets a 3?

23 PROF. ALDEMIR: DFM gets a 3.

24 CHAIRMAN APOSTOLAKIS: Why?

25 PROF. ALDEMIR: I will explain. I will

NEAL R. GROSS

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

1 explain that. I was going to pick a few and explain
2 why I am giving these numbers and, as I said --

3 CHAIRMAN APOSTOLAKIS: But do you
4 understand my problem with all this?

5 PROF. ALDEMIR: Not --

6 CHAIRMAN APOSTOLAKIS: You are not really
7 giving us some objective criteria for the
8 classification and I don't know why this is useful.

9 PROF. ALDEMIR: Okay. I cannot give you
10 quantitative criteria.

11 CHAIRMAN APOSTOLAKIS: So why do you give
12 me the data?

13 PROF. ALDEMIR: If somebody wants to have
14 some idea of how difficult they are to use, how
15 accurately they can represent system dynamics --

16 CHAIRMAN APOSTOLAKIS: What do you mean
17 difficult? You don't have any difficulty there.

18 PROF. ALDEMIR: Ease of probabilistic
19 model construction.

20 UNIDENTIFIED SPEAKER: The second column.

21 CHAIRMAN APOSTOLAKIS: But you know, this
22 is meaningless, because maybe a methodology that is
23 more involved and it's a bit more difficult has bigger
24 benefits, too.

25 PROF. ALDEMIR: True. True. I mean, I'm

NEAL R. GROSS

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

1 not --

2 CHAIRMAN APOSTOLAKIS: Where are the
3 benefits?

4 PROF. ALDEMIR: Here, I mean, the benefits
5 accuracy is the system representation of system
6 dynamics.

7 CHAIRMAN APOSTOLAKIS: Oh, I'm sure Dr.
8 Guarro will disagree on the 3 you gave DFM.

9 PROF. ALDEMIR: Yes. As I said, I will
10 take the blame.

11 CHAIRMAN APOSTOLAKIS: He already, in
12 fact, disagreed with it. He talked to me about it.

13 PROF. ALDEMIR: Well, these numbers are
14 just --

15 CHAIRMAN APOSTOLAKIS: We're getting into
16 terrible territory here but, you know, what can you
17 do?

18 PROF. ALDEMIR: No, no.

19 CHAIRMAN APOSTOLAKIS: I mean, I'm
20 familiar with the method.

21 PROF. ALDEMIR: No, the --

22 CHAIRMAN APOSTOLAKIS: I don't know why
23 you gave it a 3.

24 PROF. ALDEMIR: I was --

25 CHAIRMAN APOSTOLAKIS: It seems to me it

1 is as accurate as anything else.

2 PROF. ALDEMIR: I don't know if we should
3 get too technical here, but, you know, the process
4 modeling is you go by large increments in changes in
5 the process variables. So I am not sure how
6 accurately you are modeling this process dynamic.

7 CHAIRMAN APOSTOLAKIS: Listen, Tunc. If
8 I have a method that is very high level, okay, it will
9 be accurate, because at a very high level it tells me
10 that if this happens and the operators do this, you
11 know, then that, it's very accurate, but it's almost
12 useless, because it's very high level. Okay?

13 PROF. ALDEMIR: True.

14 CHAIRMAN APOSTOLAKIS: If I have a small
15 LOCA and I don't have a high pressure injection and I
16 don't have this and that, I'm in trouble. It's
17 extremely accurate, but it's not useful. You have to
18 go further down and say ah, what does it mean not to
19 have high pressure injection? And you do fault trees,
20 you do this and this and that.

21 Now, according to this classification, as
22 I understand it, this second way of doing business
23 would not be too accurate, whereas the first one is
24 accurate, because it's a very high level.

25 PROF. ALDEMIR: No, no, no, not high

1 level, detail, system detail. How much --

2 CHAIRMAN APOSTOLAKIS: ESDs are high
3 level.

4 PROF. ALDEMIR: ESDs.

5 CHAIRMAN APOSTOLAKIS: ESDs. Don't go
6 into the puzzle.

7 PROF. ALDEMIR: Okay. I mean, I guess you
8 may be right, but my understanding of it is that the
9 transitions are from continuous event trees.

10 CHAIRMAN APOSTOLAKIS: But the ESD, the
11 Event Sequence Diagram, is the way NASA is using them
12 and the way they have been used in the nuclear
13 industry. They just say you lost the system. Then
14 you have the standby system. If it fails, you go over
15 there. If it works, you go here. Then you have that.
16 I mean, that's a high level sequence.

17 PROF. ALDEMIR: As you will see at the
18 end, that's why we are not using it for benchmarking.

19 CHAIRMAN APOSTOLAKIS: But what --

20 PROF. ALDEMIR: There is no nuclear
21 application.

22 CHAIRMAN APOSTOLAKIS: All I'm saying,
23 Tunc, is --

24 PROF. ALDEMIR: We can change this.

25 CHAIRMAN APOSTOLAKIS: -- you are asking

NEAL R. GROSS

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

1 for trouble with this table.

2 PROF. ALDEMIR: I agree.

3 CHAIRMAN APOSTOLAKIS: And I don't know
4 how useful it is.

5 PROF. ALDEMIR: Okay. No problem. We'll
6 get rid of the table.

7 CHAIRMAN APOSTOLAKIS: You understand?

8 PROF. ALDEMIR: Yes.

9 CHAIRMAN APOSTOLAKIS: Okay.

10 PROF. ALDEMIR: No problem, no problem.

11 CHAIRMAN APOSTOLAKIS: It's not that I
12 disagree with everything you have there, but it's --

13 PROF. ALDEMIR: I understand.

14 CHAIRMAN APOSTOLAKIS: Anytime you do
15 anything --

16 PROF. ALDEMIR: No sense in creating
17 controversy. No, I understand.

18 MR. ARNDT: No, let me do it. The point
19 was we're trying to go through all the different
20 methodologies that are available or have been
21 discussed in the literature and come up with some way
22 of working through the ones that might be possible.

23 CHAIRMAN APOSTOLAKIS: I understand the
24 intent.

25 MR. ARNDT: Okay.

1 PROF. ALDEMIR: I am using it as --

2 CHAIRMAN APOSTOLAKIS: I understand the
3 intent.

4 PROF. ALDEMIR: I am using it as a
5 rationale to chose methodologies.

6 CHAIRMAN APOSTOLAKIS: But you went too
7 far.

8 PROF. ALDEMIR: Okay. Fine.

9 CHAIRMAN APOSTOLAKIS: You went too far.

10 PROF. ALDEMIR: Okay.

11 MR. KEMPER: If I could offer this. If
12 there is any help that you can give us --

13 PROF. ALDEMIR: Yes.

14 MR. KEMPER: Because what he is trying to
15 do here is to construct a screening criteria, right,
16 to determine which are the one or two methodologies
17 that we should pursue. So if there is anything that
18 you can help us with on this, we would be more than
19 happy.

20 CHAIRMAN APOSTOLAKIS: Okay. So this
21 table I suggest deletion.

22 MR. KEMPER: Well, we need some screening
23 criteria. I mean, without some objective --

24 CHAIRMAN APOSTOLAKIS: Well, it's not this
25 or nothing. I mean, come on. He has looked at all

NEAL R. GROSS

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

1 these other things. He has arguments. He knows how
2 they work.

3 PROF. ALDEMIR: But see, we have a little
4 problem here, because we cannot communicate
5 informally, right? That's one thing.

6 CHAIRMAN APOSTOLAKIS: Well, one way of
7 doing this, if you really want to, is to poll people.
8 I mean, you don't just give your view. You could have
9 approached the actual developments of these and asked
10 them to rank either their own method or the other
11 guy's method.

12 PROF. ALDEMIR: That is a very good
13 suggestion.

14 CHAIRMAN APOSTOLAKIS: Yes. That might
15 have been more reasonable.

16 PROF. ALDEMIR: That's a very good
17 suggestion.

18 CHAIRMAN APOSTOLAKIS: And you should have
19 a range of things.

20 PROF. ALDEMIR: But do you agree with the
21 metrics?

22 CHAIRMAN APOSTOLAKIS: Oh, I don't know.
23 No, the benefit, where is the benefit? I said there
24 has to be some benefit.

25 PROF. ALDEMIR: Oh, this is a benefit.

1 CHAIRMAN APOSTOLAKIS: I mean, certain
2 methods are more complicated.

3 PROF. ALDEMIR: Accuracy is the system
4 representation of system dynamics.

5 CHAIRMAN APOSTOLAKIS: I mean, I don't
6 know. Is the theory of relativity complex? Yes, yes,
7 but that's the only way of understanding a few things.

8 PROF. ALDEMIR: This is the benefit part.
9 If you don't like the --

10 CHAIRMAN APOSTOLAKIS: Where is the
11 benefit, the accuracy?

12 PROF. ALDEMIR: Accuracy, accuracy is the
13 benefit.

14 CHAIRMAN APOSTOLAKIS: You would have to
15 explain to me more or what do you mean by accuracy?
16 Again, I tell you, if I stay at a high level I'm more
17 accurate, but I'm not very useful. Benefit means, you
18 know, somebody like NRR or whoever who wants to use it
19 in doing something with it, is he going to find it
20 useful? If you give him a very high level description
21 of the system, that's not useful. It's a good
22 starting point like, you know, small LOCA, high
23 pressure injection. Yes, thank you very much. But
24 there are many ways of achieving high pressure
25 injection.

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 PROF. ALDEMIR: Well, you know, if there
2 is any procedure where we can get comments from you,
3 you know, without --

4 CHAIRMAN APOSTOLAKIS: This is the
5 procedure.

6 PROF. ALDEMIR: Okay. Then can you give
7 us metrics that I can use?

8 CHAIRMAN APOSTOLAKIS: Why do you want --
9 I don't understand, I mean.

10 PROF. ALDEMIR: As Bill said, we need
11 screening criteria to justify the kind of
12 methodologies we are going to use for benchmarking,
13 which will come on later on.

14 CHAIRMAN APOSTOLAKIS: What are the
15 objectives of your answers? Where do you want to go
16 with this and then to evaluate these according to your
17 objectives.

18 PROF. ALDEMIR: This is actually what we
19 tried to do, because we actually want to go to the
20 fault. We want to have accurate system and we want to
21 have an accurate model. We want to have an easily
22 constructed model. We want that model to integrate
23 well with an existing PRA.

24 CHAIRMAN APOSTOLAKIS: Well, you already--
25 well, first of all, I mean, I am not supposed to solve

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 your problem here, but you listed a number of possible
2 problems very early on. Okay. Maybe you can start
3 with those and ask yourself whether some of these
4 methodologies could be helpful in addressing these
5 unique issues that you raise.

6 PROF. ALDEMIR: That's in the second
7 table, which you argued with again.

8 CHAIRMAN APOSTOLAKIS: And ask, you know,
9 what are the needs of the Agency, right? Ask the NRR
10 guy what does he want to know?

11 PROF. ALDEMIR: Okay. Yes.

12 CHAIRMAN APOSTOLAKIS: Okay. Right?

13 PROF. ALDEMIR: Okay.

14 CHAIRMAN APOSTOLAKIS: Like we know with
15 standard PRAs we want to understand not only what the
16 level of risk is, but also what are the dominant
17 contributors. Okay. So a methodology that gives us
18 a dominant contributor, is good enough. Right? So
19 you know, think about it that way. I'm not saying
20 it's a straightforward, simple problem, but this
21 certainly invites --

22 PROF. ALDEMIR: No, you are right. But I
23 mean, as I said, you know, this is what we could come
24 up. Any suggestions are --

25 CHAIRMAN APOSTOLAKIS: Because if I look

NEAL R. GROSS

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

1 at this now, I know, for example, that later on,
2 because I listened to you at the ANS meeting, you are
3 proposing to compare DFM with something else. If I
4 look at this table, I wouldn't chose DFM.

5 PROF. ALDEMIR: But this is not the
6 complete picture, because --

7 CHAIRMAN APOSTOLAKIS: It gets a 3, a 5,
8 a 7 and a 7.

9 PROF. ALDEMIR: Wait until -- oh, sorry,
10 I don't have it here. But this is conditional. This
11 is only for the process side.

12 CHAIRMAN APOSTOLAKIS: Yes.

13 PROF. ALDEMIR: It does not include the
14 digital aspects. There is another table there, which
15 tries to combine both.

16 CHAIRMAN APOSTOLAKIS: I see.

17 PROF. ALDEMIR: So this --

18 CHAIRMAN APOSTOLAKIS: But why is ease of
19 modeling a factor?

20 PROF. ALDEMIR: Well, because --

21 CHAIRMAN APOSTOLAKIS: I mean, if it's a
22 complex problem --

23 PROF. ALDEMIR: True.

24 CHAIRMAN APOSTOLAKIS: -- even the
25 methodology would be false.

1 PROF. ALDEMIR: True. But if it is so
2 complex that you need a four year degree, I mean, a
3 four year program to learn it, then it's not going to
4 be very useful to a lot of people.

5 CHAIRMAN APOSTOLAKIS: But it shouldn't be
6 up there at the same level as the accuracy.

7 PROF. ALDEMIR: Fine.

8 CHAIRMAN APOSTOLAKIS: What we defined as
9 accuracy.

10 PROF. ALDEMIR: I mean, as I said, any
11 suggestions are welcome.

12 CHAIRMAN APOSTOLAKIS: And if I have two
13 methodologies and one is very accurate and the other
14 is not so accurate, but it's easier to use, then I can
15 see how you can go with that one. But to say accuracy
16 and ease of use are the same benefit, I mean --

17 PROF. ALDEMIR: Fine. We can change the
18 metrics in any way that --

19 CHAIRMAN APOSTOLAKIS: Anyway, I think you
20 get the message.

21 UNIDENTIFIED SPEAKER: Yes, I think so.

22 PROF. ALDEMIR: Yes. Okay. Now, the Type
23 II interactions. Again, these --

24 CHAIRMAN APOSTOLAKIS: Type II now is
25 within the --

NEAL R. GROSS

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

1 PROF. ALDEMIR: Within the system. Markov
2 Models, and when I say Markov Models, you know, I'm
3 not going to spend too much time on these, because we
4 I think discussed this at some length yesterday, and
5 when I refer to Markov Model, I only refer to Barry
6 Johnson's model, because there are others.

7 There are basic methodologies. The Markov
8 Models, and again this has been discussed, so I'm not
9 going to talk about it, Bayesian methodologies. The
10 one that we looked at in detail is by my colleague
11 from MIT.

12 CHAIRMAN APOSTOLAKIS: Again, why is that
13 a dynamic methodology? I mean, poor Bayes is not
14 dynamic.

15 PROF. ALDEMIR: It is dynamic in the sense
16 that your model is being updated as you get new
17 information.

18 CHAIRMAN APOSTOLAKIS: But that's not what
19 you meant by dynamic earlier. Dynamic, you said
20 interactions with a physical process, I mean.

21 PROF. ALDEMIR: It is taking into -- well,
22 this is Type II within the system not physical
23 process. This is Type II. So, Barry Johnson, sorry.
24 My colleague's methodologies are Golay's Bayesian
25 update method and it has got a lot of assumptions and

1 part of which is that software is being developed.
2 It's not really applicable to -- let me get their
3 information on this. It's not really applicable to
4 existing software. The number of paths, possible
5 paths within the system, has to be estimated. You are
6 assuming a lot of -- making a lot of assumptions.

7 CHAIRMAN APOSTOLAKIS: The University of
8 Maryland --

9 PROF. ALDEMIR: Pardon me?

10 CHAIRMAN APOSTOLAKIS: The University of
11 Maryland yesterday told us that they also want to know
12 that, the number of paths.

13 PROF. ALDEMIR: Yes, yes, yes, right. You
14 are making assumptions on the choice of the priors.
15 You are rejecting some execution paths, but you don't
16 really know whether you should have looked at them or
17 not.

18 CHAIRMAN APOSTOLAKIS: That's fine, that's
19 fine.

20 PROF. ALDEMIR: Okay. So dynamic
21 flowgraph methodology is, as you will see later on,
22 the best one, in fact, compared with earlier what I
23 said, everything combined. It turns out to be the
24 best one. The only restriction we could find out, and
25 that comes to what Professor Apostolakis was referring

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 earlier, why we ranked it low, is because it is
2 making certain assumptions on how to model the
3 process.

4 And, for example, level change, high level
5 change, low level change, medium level change and kind
6 of qualitative descriptions. It's based on digraphs,
7 which are qualitative in nature, and that is where 3
8 is coming from actually. So you don't know.

9 Now, if you talk to the method developers,
10 then they tell you that sure, I can take 10, 15
11 levels, 100 levels, but the model becomes very
12 complicated.

13 CHAIRMAN APOSTOLAKIS: True.

14 PROF. ALDEMIR: True. There is a self-
15 check mechanism. But the thing that we were looking
16 at, at this point, is how they have been used in the
17 literature, not speculate on how they could have been
18 used. So if you look at what has been out there,
19 which is a NUREG on a feed water control system, the
20 system dynamics are qualitative.

21 CHAIRMAN APOSTOLAKIS: That's not on the
22 table.

23 PROF. ALDEMIR: Right, right. But the
24 reason I mention NUREG, because this is an NRC-related
25 meeting. That's why. So I mean, there is a NUREG.

NEAL R. GROSS

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

1 That's the point. But you know, that is the reason
2 why 3, not necessarily because of the inherent
3 limitations of the methodology. Petri nets.

4 CHAIRMAN APOSTOLAKIS: The analysis of the
5 reactor at Sandia, I thought, was pretty interesting
6 that Chris Garrett did. You have that paper.

7 PROF. ALDEMIR: I don't have it.

8 CHAIRMAN APOSTOLAKIS: Where he found, in
9 fact, a fault in the software.

10 PROF. ALDEMIR: I don't have that. Which
11 one are you talking about, this one that was more
12 recently published?

13 CHAIRMAN APOSTOLAKIS: Yes.

14 PROF. ALDEMIR: Oh, the reliability and
15 system safety?

16 CHAIRMAN APOSTOLAKIS: I believe so, yes,
17 where he found that there was a denominator, k minus
18 1.

19 PROF. ALDEMIR: Right.

20 CHAIRMAN APOSTOLAKIS: In the program.

21 PROF. ALDEMIR: Right, but that was -- oh,
22 okay.

23 CHAIRMAN APOSTOLAKIS: Yes, he found it.

24 PROF. ALDEMIR: No, no, I don't mean that.

25 I mean --

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: He went to the
2 developer and the developer, first of all, was shocked
3 that he was there and, second, he said, which is
4 related to what you guys were saying yesterday --

5 PROF. ALDEMIR: Right.

6 CHAIRMAN APOSTOLAKIS: He said but there
7 will never be a situation where k is 1. But the
8 interesting thing is -- do you have that paper?

9 PROF. ALDEMIR: Yes, yes, I have that
10 paper. I have the paper. Let's see, Petri nets.

11 CHAIRMAN APOSTOLAKIS: In fact, that could
12 be one of your criteria. Has the method under
13 scrutiny ever been used in a case study and has it
14 identified anything?

15 PROF. ALDEMIR: Well, we tried. We did
16 actually try to do that. That's the only reason why,
17 as I said, we are using -- you will see. We will zero
18 in on two methodologies and that's the only reason why
19 we're doing that, because it has been implemented.

20 CHAIRMAN APOSTOLAKIS: I'm trying to help.

21 PROF. ALDEMIR: No, I understand, I
22 understand. Okay. Petri nets.

23 CHAIRMAN APOSTOLAKIS: It may not go, but
24 the motivation is there.

25 PROF. ALDEMIR: That's all right. Petri

NEAL R. GROSS

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

1 nets. Again, you know, they seem to do a very good
2 job within Type II interactions, but I am not too sure
3 how well they model Type I interactions, and then I
4 will have a complete table later on with a different
5 ranking.

6 Test-based approaches, as the name
7 implies, is just test-based, so then there are all
8 sorts of issue, you know, how do you select your test
9 cases and the system must be mostly complete. Testing
10 is a value-added activity. It shows presence, but not
11 the absence of error. Test cases may not be rigorous
12 enough to exercise the system to predict accurately
13 its reliability and, of course, they don't model Type
14 I interactions, which is interactions with the
15 process. Black-box models are the type of models --

16 CHAIRMAN APOSTOLAKIS: I don't see the
17 word black-box. Oh, down there. So you skipped the
18 software metric?

19 PROF. ALDEMIR: We discussed this
20 yesterday at great length.

21 CHAIRMAN APOSTOLAKIS: But what do you
22 think?

23 PROF. ALDEMIR: I mean --

24 CHAIRMAN APOSTOLAKIS: Black-box.

25 PROF. ALDEMIR: Because it's going to

NEAL R. GROSS

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

1 start anew.

2 CHAIRMAN APOSTOLAKIS: Well, let me ask
3 you this. I see these others without necessarily
4 agreeing with them, but I see them as, you know,
5 taking a piece of software and doing something to it.
6 Is the software metric approach doing the same thing
7 or is it more generic?

8 PROF. ALDEMIR: My opinion is that it is
9 generic but, you know, the rankings and so forth, the
10 choices are by our computer science people, who felt
11 more qualified. Their impression of metric-based
12 approaches is that -- I mean, if you want me to
13 mention the kind of things that they had problems
14 with, measured the software development process, but
15 not the end result of the process.

16 It has yet to be shown that this method
17 can scale to high reliability requirements with a
18 large system, which they claimed yesterday it does.
19 The metrics chosen are based on expert opinion and may
20 change as new metrics are discovered and, of course,
21 does not model Type I interactions.

22 CHAIRMAN APOSTOLAKIS: So what is this
23 Schneidewind?

24 PROF. ALDEMIR: Schneidewind Model. Well,
25 it's a black-box model and the name implies they treat

NEAL R. GROSS

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

1 it as a black-box. They chose -- NASA used it for
2 modeling one of the missions. And it has got -- it
3 uses a non-homogenous Poisson process as the basis to
4 predict the reliability of software components,
5 assumes that the software system is changed only when
6 there is an observable failure, failure data needed
7 for quantification, but may not be available, because
8 they have the data on the shuttle system, needs
9 mechanism to select cases, test times and reword
10 criteria. In other words, there is no justification
11 of what's being done, and it has been only implemented
12 on software. So again, you know, it does not model
13 the complete system.

14 CHAIRMAN APOSTOLAKIS: Okay.

15 PROF. ALDEMIR: So we tried to come up
16 with --

17 CHAIRMAN APOSTOLAKIS: So you do have.
18 Why are you asking me then? You do have your criteria
19 here.

20 PROF. ALDEMIR: These are requirements.
21 Okay. We tried to go through a screening process to
22 gradually reduce, so we went through a screening of
23 Type I interactions. We went through a screening of
24 Type II interactions. And then we did a screening of
25 both. And then we tried to come up with requirements.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 So if you want me to use them as metrics, that's fine.

2 CHAIRMAN APOSTOLAKIS: I think this is
3 the ones --

4 PROF. ALDEMIR: Great.

5 CHAIRMAN APOSTOLAKIS: -- that you should
6 be using and No. 3 is the most important of them all.

7 PROF. ALDEMIR: Yes, no problem.

8 CHAIRMAN APOSTOLAKIS: No problem.

9 PROF. ALDEMIR: So I don't know. Well,
10 I'll just go through them fast. The model must be
11 able to predict future failures well. The reason I
12 mention it is because there are models based on
13 existing performance and they are not necessarily all
14 that great, because you don't know if you have covered
15 everything. And there are models that people have
16 based on neural nets, for example, which are based on
17 totally the operation of data, which is not very
18 practical to predict future events.

19 The model must account for the relevant
20 features of the system under consideration. You must
21 be able to model all types of complex interactions
22 that are taking within the system. Also, you need to
23 worry about if you are omitting things by using
24 assumptions. So you have to make sure that your
25 assumptions are reflecting the true operation of the

1 system, which ties up with 3.

2 This we discussed in great length. The
3 model must be able to represent dependencies. No. 5,
4 desirable feature. It must not be hard to learn. No.
5 6, data used in the quantification process must be
6 credible to a significant --

7 CHAIRMAN APOSTOLAKIS: Oh, you have more?

8 PROF. ALDEMIR: I have 11. You must be
9 able to differentiate between a state that fails one
10 safety check and that those that fail multiple ones,
11 must be able to differentiate between faults that
12 cause function failures and intermittent failures,
13 must have the ability to provide relevant information
14 to the users and that has to do with the -- one of our
15 internal reviewers argued with that, for example, that
16 Monte Carlo methodology does precisely the same, but
17 the intention here is that it provides you information
18 that you can use to integrate the results into a full
19 PRA like cut sets and so forth.

20 And talking about integration, when you
21 integrate this system, this model into the full PRA,
22 it must be able to match with the rest. For example,
23 like a Markov Model, you need a lot of detailed system
24 information, which the fault tree is not going to give
25 you. By the same token, you have to extract 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 information out of the Markov Model to put into the
2 PRA. But you can do that even qualitatively using
3 graph theoretical methods, so you can get qualitative
4 information out of Markov Models.

5 This kind of goes with 10. Models should
6 not require highly time-dependent or continuous plant
7 state information. So if you think that these are
8 good metrics, we can use them.

9 CHAIRMAN APOSTOLAKIS: I think they are
10 pretty good, but I'm wondering why the previous
11 speaker didn't use something like this. Todd? I
12 mean, shouldn't you have some list of requirements, as
13 well, in the development of your models?

14 These are not unique to time-dependent, I
15 mean, dynamic methodologies that Professor Aldemir is
16 talking about. They are general requirements, except
17 the last one, for any model, so it seems to me since
18 both of you are part of the NRC, you should have a
19 common set of requirements, should you not? Maybe you
20 should increase the number of telephone calls.

21 MR. HILSMEIER: That's a very good idea.

22 CHAIRMAN APOSTOLAKIS: Now, honestly,
23 Todd, is this the first time you've seen this?

24 MR. ARNDT: We have shared our graphs with
25 Todd.

1 CHAIRMAN APOSTOLAKIS: Just about. No,
2 but, I mean, I would expect, I mean, you know, you
3 have the two approaches that Steve has talked about,
4 but a lot of the elements are common. And one is the
5 requirements for what you are trying to develop, and
6 all the methodologies that Tunc mentioned, he just
7 about exhausted everything. I mean, so I don't see
8 why they don't apply to you.

9 Now, you can reject some of these for
10 obvious reasons like the continuous event tree and say
11 my God, this is too much for me, because I'm dealing
12 with this problem, which is perfectly all right. This
13 is good. So I would expect to see a little closer
14 collaboration.

15 PROF. ALDEMIR: Another table.

16 CHAIRMAN APOSTOLAKIS: Now, wait, wait,
17 wait.

18 PROF. ALDEMIR: Okay.

19 CHAIRMAN APOSTOLAKIS: Where are you
20 setting as a requirement that the model should be
21 capable or at least have a promise of handling certain
22 things that we have observed, such as the sequencer
23 issues that Mr. Waterman mentioned yesterday?

24 PROF. ALDEMIR: Well, that is implicit in
25 4, of course.

1 CHAIRMAN APOSTOLAKIS: In where?

2 PROF. ALDEMIR: In 4. Model must be able
3 to represent dependencies between failure events
4 accurately and quantitatively.

5 CHAIRMAN APOSTOLAKIS: I don't know.
6 Classify what you told us yesterday, Mike, as a
7 failure, I mean, as being one of dependencies. I
8 don't think so.

9 MR. ARNDT: Yes. It's basically, the way
10 Tunc defined it is, a Type II dependency. The issue
11 is, and we could probably define it better, but it's
12 a design fault associated with the interaction between
13 two parts of the software.

14 MR. WATERMAN: No, I think that's a Type
15 I failure. You don't know the failure exists until
16 you get some kind of Type I demand that it performed.
17 That's why they ran on and on and on and didn't
18 realize they didn't have HPI about 30 percent of the
19 time, because they didn't have any external event that
20 said hey, work for me and then the software said I'm
21 not going to do that. So I think that's kind of a
22 Type I event. You don't know the failure exists.

23 CHAIRMAN APOSTOLAKIS: Yes. In any case,
24 I think it's this kind of experience.

25 MR. WATERMAN: Yes.

1 CHAIRMAN APOSTOLAKIS: I mean, the
2 impression I get from you guys, both teams, is that
3 there is precious little out there regarding nuclear
4 experience. At least, you know, if you can say okay,
5 I know these four incidents.

6 MR. ARNDT: Yes.

7 CHAIRMAN APOSTOLAKIS: Does this
8 methodology have any chance of modeling?

9 MR. ARNDT: That coupled both in with, as
10 Tunc mentioned, the ability to represent dependencies,
11 what we probably should do, and when tested gets
12 accurate results on the examples that we actually
13 have.

14 PROF. ALDEMIR: Oh, oh, we should put that
15 as the 12th requirement that compare actually.

16 CHAIRMAN APOSTOLAKIS: Does it have any
17 chance of modeling the existing operating experience?

18 PROF. ALDEMIR: You know, it is implicit
19 in here, but --

20 CHAIRMAN APOSTOLAKIS: A catchall.

21 PROF. ALDEMIR: In other words, what I
22 meant, implicitly meant with 1, also includes that
23 future failure, as well, because if something comes
24 up, we should be able and once something comes up,
25 literally happens, we should be able to model it. So

NEAL R. GROSS

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

1 it is implicit in there, but maybe we should make it
2 more explicit.

3 CHAIRMAN APOSTOLAKIS: I would rather do
4 what you just said, make it 12.

5 PROF. ALDEMIR: Okay. Make it 12.

6 CHAIRMAN APOSTOLAKIS: And use explicitly
7 the words operating experience.

8 PROF. ALDEMIR: Fine.

9 MR. ARNDT: Right.

10 CHAIRMAN APOSTOLAKIS: To show that you
11 are fully aware of it.

12 PROF. ALDEMIR: Well, I'll take notes.

13 MR. ARNDT: We'll get it from the
14 transcript.

15 PROF. ALDEMIR: The transcript. Okay.
16 Good.

17 MR. ARNDT: Something on the order of
18 ability to integrate operational experience.

19 PROF. ALDEMIR: Okay. That's good. Can
20 I go on?

21 CHAIRMAN APOSTOLAKIS: Yes, please.

22 PROF. ALDEMIR: Another table. Now, here,
23 why I'm doing what you just said I should do in the
24 first place, but I am doing it myself and not giving
25 numbers in this situation.

NEAL R. GROSS

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

1 CHAIRMAN APOSTOLAKIS: This is progress,
2 saying X and O is really progress versus --

3 PROF. ALDEMIR: And lots of question
4 marks, as you see.

5 CHAIRMAN APOSTOLAKIS: -- 1, 2, 3, 4, 5.

6 PROF. ALDEMIR: No, you are right. I
7 mean, this was done for our internal screening
8 purposes. We put it there and we were invited to
9 come.

10 CHAIRMAN APOSTOLAKIS: Also, these are the
11 11 requirements?

12 MR. ARNDT: Yes.

13 PROF. ALDEMIR: Yes.

14 CHAIRMAN APOSTOLAKIS: Oh, well, that's
15 much better, Tunc.

16 PROF. ALDEMIR: As I said, we have done
17 it, but again this is my personal opinion. Again, I
18 don't want anybody to jump on anybody else, because
19 this is what I thought is the case.

20 CHAIRMAN APOSTOLAKIS: We will only jump
21 on you.

22 PROF. ALDEMIR: But you are right in the
23 sense that we should test this and that's, I guess,
24 one of the reasons why we have this meeting in the
25 first place, to have input. We should test it. We

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 should send it out as a survey to the developers, to
2 all the stakeholders, so to speak.

3 CHAIRMAN APOSTOLAKIS: This one.

4 PROF. ALDEMIR: This one, right. And we
5 have comments from some of the reviewers, internal
6 reviewers, on this, for example, and it got revised
7 actually. Now, I don't want to go through this again.

8 CHAIRMAN APOSTOLAKIS: That's okay.

9 PROF. ALDEMIR: But if you want, I can
10 give you some justification. For example, let's take
11 DFM. DFM, you see no zeros here.

12 CHAIRMAN APOSTOLAKIS: What is 4? What is
13 4?

14 PROF. ALDEMIR: 4 is capable to what I
15 just said earlier and then we have this.

16 CHAIRMAN APOSTOLAKIS: So it is not " It
17 is not hard for an analyst to learn."

18 PROF. ALDEMIR: No, no, it is the --

19 CHAIRMAN APOSTOLAKIS: "Must be able to
20 represent dependencies."

21 PROF. ALDEMIR: Dependencies.

22 CHAIRMAN APOSTOLAKIS: Yes, I think
23 there's a question mark there. You are right.

24 PROF. ALDEMIR: I mean, right, you will
25 see that that's one where we are going. I mean,

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's what we are aiming at. We're going to test it.

2 CHAIRMAN APOSTOLAKIS: And then 6, "The
3 data used must be credible."

4 PROF. ALDEMIR: None of them has that.
5 None of them has credible data.

6 CHAIRMAN APOSTOLAKIS: Yes, everybody has
7 a question.

8 PROF. ALDEMIR: Right, right, nobody.

9 CHAIRMAN APOSTOLAKIS: And then what else
10 do you have? 8. What is 8? "The model must be able
11 to differentiate between faults that cause function
12 failures and intermittent failures." I don't know
13 what that means, but I guess you are right.

14 PROF. ALDEMIR: Well, I can go into that.

15 MR. ARNDT: Take yes for an answer.

16 CHAIRMAN APOSTOLAKIS: No, that's fine.
17 Move on.

18 PROF. ALDEMIR: Okay. But you see, what
19 I'm trying to get at is that whenever there is an
20 internal, initial, not internal, initial screening
21 first and then try to combine both, there is an
22 implicit screening for the others, but I didn't show
23 that. And then I didn't make a table.

24 CHAIRMAN APOSTOLAKIS: Tunc, as you know,
25 even if you send this out, it's like any new field.

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 Most of the developers of these methodologies have not
2 used somebody else's methodology, so they really
3 cannot pass judgment. They have some idea.

4 PROF. ALDEMIR: That is a good point.

5 CHAIRMAN APOSTOLAKIS: They have some idea
6 like you organized this workshop in Turkey years ago.
7 Okay. People listen to other people and so on, but
8 they haven't really tried it. They haven't really.
9 You know, so they are very familiar with their own
10 methodology, but not with other people's approach.

11 PROF. ALDEMIR: I doubt that this is the
12 proper forum, but as you well know, Ohio State is part
13 of the University Consortium to help Idaho National
14 Lab to conduct research towards future reactors, and
15 our task is as instrumentation control and PRA. So as
16 the first task of this academic center of -- and there
17 are academic centers of excellence established at each
18 five universities.

19 CHAIRMAN APOSTOLAKIS: Yes.

20 PROF. ALDEMIR: Our first task, we were
21 planning to organize a workshop on dynamic
22 methodologies in PRA.

23 CHAIRMAN APOSTOLAKIS: That's not what --

24 PROF. ALDEMIR: No. The reason I mention
25 that, do you think it's a good idea to use this as a

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 forum to get opinions?

2 CHAIRMAN APOSTOLAKIS: I think the best
3 way to do what I said is through benchmark exercises
4 where people are forced to use somebody else's model
5 to actually do real work, but these tend to be
6 expensive.

7 PROF. ALDEMIR: That's exactly right.

8 CHAIRMAN APOSTOLAKIS: And you have a
9 large number of methods here.

10 PROF. ALDEMIR: That's right. So we have
11 to screen. That's the whole problem.

12 CHAIRMAN APOSTOLAKIS: Yes.

13 PROF. ALDEMIR: We have to screen.

14 CHAIRMAN APOSTOLAKIS: But you see, the
15 biggest problem with workshops or anything else is
16 people just don't listen to others.

17 PROF. ALDEMIR: Well, we saw that in
18 Turkey.

19 CHAIRMAN APOSTOLAKIS: You don't have to
20 go so far to see it.

21 PROF. ALDEMIR: No, I don't mean that. I
22 mean the workshop. I am trying to explain.

23 MR. ARNDT: You can go to an ACRS meeting,
24 people not listening to you.

25 PROF. ALDEMIR: Excluding present company.

NEAL R. GROSS

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

1 CHAIRMAN APOSTOLAKIS: No, I'm serious,
2 and this is true everywhere. I mean, that's why in
3 the beginning there is chaos. Take PRA, you know, in
4 the '70s and '80s. There is no classical statistics.
5 There is classical-based. Classical now in the year
6 of 2005, you realize that there hasn't been a single
7 PRA done in a classical way. So at this point you say
8 well, maybe then they are right, okay, but that's the
9 way it is.

10 PROF. ALDEMIR: Well, we tried to then do
11 the screening, because it's expensive to benchmark
12 everything.

13 CHAIRMAN APOSTOLAKIS: I don't see
14 anywhere though you saying I'm going to look at the
15 basic assumptions behind these things and make a
16 judgment myself whether these assumptions are sound.
17 I think you should do that.

18 PROF. ALDEMIR: Well, it is, of course,
19 implicit in those tables. I mean, what I say are you
20 modeling the process, it's implicit in that. If the
21 assumptions are too restrictive, you are not modeling
22 it correctly.

23 CHAIRMAN APOSTOLAKIS: But I would also
24 come to my favorite theme of the last two days.
25 Markov approach, fundamental assumption, cost 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 transition rate from this state to that state. It's
2 not justified.

3 PROF. ALDEMIR: Let me say a few words on
4 that. Okay. Let me go through this and then I'll
5 come back to Markov and then say a few things.

6 CHAIRMAN APOSTOLAKIS: And I think GO-FLOW
7 is --

8 PROF. ALDEMIR: Actually as good as Petri
9 nets, actually as good as --

10 CHAIRMAN APOSTOLAKIS: Which tells me a
11 lot.

12 PROF. ALDEMIR: As good as -- you know,
13 the reason -- what?

14 MR. ARNDT: Just to go to that slide.

15 PROF. ALDEMIR: Well, okay. When we
16 ranked these things, we found out that, again, purely
17 subjective basis, because there is no real
18 benchmarking, but dynamic flowgraph methodology,
19 that's the one that we found, let's put it this way,
20 least objectionable with the least restrictions, least
21 number of assumptions.

22 CHAIRMAN APOSTOLAKIS: But let me also add
23 something here, because other people may not remember.
24 All these approaches, not all but certainly the DFM,
25 it doesn't give you any probabilities. It just gives

NEAL R. GROSS

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

1 you failure modes, sequences that lead to failure.
2 This is very important, because Steve also yesterday,
3 every time I pushed him hard, he said oh, but there's
4 always benefit here because we understand the
5 structure of the model. I think most of these models
6 help you do that.

7 MR. ARNDT: Yes, they do.

8 PROF. ALDEMIR: All of them.

9 CHAIRMAN APOSTOLAKIS: But some of them do
10 not claim that they produce probabilities. There is
11 a good reason for that. The developers were modest
12 people.

13 PROF. ALDEMIR: Well, okay. Let me go
14 through this and I will come back to Markov and say a
15 few words.

16 CHAIRMAN APOSTOLAKIS: Okay.

17 PROF. ALDEMIR: Because to respond to some
18 of the comments that were made yesterday. Dynamic
19 flowgraph methodology we found has the least. The
20 only thing that we could see in the dynamic flowgraph
21 is this potentially not describing the system process
22 or the process dynamics correctly and if you don't do
23 it correctly, as I will show you in a little while,
24 you may be missing sequences. Also, you may be coming
25 up with the wrong numbers if you are going to quantify

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 it.

2 Now, the second choice, although Professor
3 Apostolakis may not agree, is the Markov approach.
4 Maybe this is the time. The Markov approach. Again,
5 one of the important reasons why we zeroed in on these
6 two is because there are applications in the
7 literature on systems that pertain to nuclear systems.
8 Markov has that. Dynamic flowgraph methodology has
9 that.

10 Now, Markov, as was mentioned yesterday,
11 maybe it's the right time, has to work with numbers,
12 but not necessarily so. If you want to extract
13 qualitative information out of the system, you can
14 look at the -- you can regard the lambdas as
15 placeholders. You can use a search, graph theoretic
16 search scheme through the matrix, transition matrix,
17 and you can come up with very a well-defined, very
18 detailed scenario as to how the accident progresses.

19 Now, there is no machinery to do that
20 automatically, I agree, but it can be done. So you
21 can get qualitative information. That's one. The
22 other thing is that even if the numbers are wrong, you
23 can do, of course, sensitivity analysis.

24 CHAIRMAN APOSTOLAKIS: But the question is
25 how do you transition from one state to the other?

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 assumption there is independently of the number is
2 that there is a constant rate of --

3 PROF. ALDEMIR: No, no, no.

4 CHAIRMAN APOSTOLAKIS: But I'm saying that
5 there is.

6 PROF. ALDEMIR: No constant, no assumption
7 on constant rate.

8 CHAIRMAN APOSTOLAKIS: I mean, if there is
9 a design error, I don't know why I would transition
10 from one state to the other. There is a design error,
11 for heaven's sakes. If the conditions are there, it
12 will never work, because it's wrong. That's where I
13 have a problem. With the Markov I go there, I come
14 back, I go there, I come back.

15 PROF. ALDEMIR: What you are saying is
16 that the transition is dependent upon the initial
17 conditions.

18 CHAIRMAN APOSTOLAKIS: Yes.

19 PROF. ALDEMIR: Right.

20 CHAIRMAN APOSTOLAKIS: I mean, the
21 fundamental assumption is that I can go from one state
22 to another. And what I keep hearing from the experts,
23 who have experience with these things, is that the
24 specification error is a requirement there. So if the
25 damn thing doesn't work under these conditions in one

NEAL R. GROSS

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

1 case, it will never work, because it's wrong and
2 Markov doesn't allow that. Now, don't tell me about
3 semi-Markov, I mean, come on.

4 PROF. ALDEMIR: Well, no, but I will come
5 to something else, you know.

6 CHAIRMAN APOSTOLAKIS: This is my problem.

7 PROF. ALDEMIR: No, that is a valid
8 assumption, I mean, not assumption, valid statement,
9 but let me say something about the failure rate.
10 Constant failure rate or non-constant failure rate is
11 no problem, because if there is --

12 CHAIRMAN APOSTOLAKIS: Well, yes, but
13 there are still transitions though.

14 PROF. ALDEMIR: Well, I mean, if you
15 assume that the concept of a transition, constancy or
16 non-constancy is no problem, it can be taken care of.

17 CHAIRMAN APOSTOLAKIS: Absolutely.

18 PROF. ALDEMIR: The other thing, and it is
19 not by the way, it is not a bad assumption. If you
20 are basing your failure data on the field data and on
21 a maintained system, it is not a bad idea to use
22 constant failure rates.

23 CHAIRMAN APOSTOLAKIS: I can't think of a
24 single incident from the ones that Mike described
25 yesterday, others that I have seen, this Canadian

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 reactor, the Bruce reactor where they had a problem a
2 number of years ago, where it was a matter of
3 transition. It was wrong and the right conditions
4 were created and the error came to the surface. It
5 was a design error or specification, if you wish, or
6 whatever that was dormant until the right conditions
7 were created.

8 Now, I can't see for the life of me any
9 Markov approach dealing with that. We need something
10 new, something fresh and I don't know what that is.
11 If you ask me, I don't know. I'm sorry, I don't know,
12 but I'm not going to go with the wrong approach just
13 because I don't know.

14 PROF. ALDEMIR: I mean, what I am trying
15 to say is that if there is a transition possible,
16 whether it is due to the software failure, so to
17 speak, or whether because the software was designed
18 wrong and the initial conditions prompted that
19 transition, as long as there is a transition, that's
20 okay.

21 CHAIRMAN APOSTOLAKIS: I understand that,
22 yes.

23 PROF. ALDEMIR: That's fine.

24 CHAIRMAN APOSTOLAKIS: Yes, if it's a
25 transition.

1 PROF. ALDEMIR: I mean, that is my system
2 topology. That is my system topology.

3 CHAIRMAN APOSTOLAKIS: My problem is that
4 I don't see very many cases where there is a
5 transition, so you and I and others have to eventually
6 convince ourselves that, you know, under certain
7 conditions perhaps it's okay, under others it's not.
8 But the big issue now in front of us, and I don't
9 think you should feel responsible that you can solve
10 it.

11 PROF. ALDEMIR: No, no.

12 CHAIRMAN APOSTOLAKIS: This is a real
13 issue.

14 PROF. ALDEMIR: Yes.

15 CHAIRMAN APOSTOLAKIS: I mean, this is a
16 new issue.

17 PROF. ALDEMIR: No, all I am trying to see
18 is, first of all, you know, you need a couple of
19 methodologies, as you said, to kind of look at what is
20 available, what are their weak points and their strong
21 points.

22 CHAIRMAN APOSTOLAKIS: Yes.

23 PROF. ALDEMIR: And when looking at
24 available methodologies, what we are seeing is that
25 these are the two most promising. The others don't

1 rank as high. That's why we are using them.

2 CHAIRMAN APOSTOLAKIS: You know, I
3 explained to somebody, but maybe I should say it
4 again, just a little lecture here.

5 One of the labors of Hercules was to
6 capture and kill a bandit who was between Athens and
7 Corinth. His name was Procrustes. I will tell you
8 how you spell that later. What he did, he would grab
9 travelers, at that time, you know, by walking or
10 whatever, rob them and then he had a bed. He would
11 stretch them out on the bed.

12 If they were shorter than the bed, he
13 would stretch them to fit the bed and, of course, they
14 died. If they were taller than the bed, he would cut
15 off pieces of them until they fit the bed. And from
16 that a saying came about, which is much better known
17 in Greek, but in English, too, I just seen it, the
18 Procrustean bed.

19 All these people who are taking existing
20 methods from reliability and put them on software are
21 using the Procrustean bed. They are taking something
22 that doesn't fit the bed and either they stretch it or
23 they cut it off until it fits the bed, and that is not
24 an approach, an acceptable approach anyway and as
25 Hercules demonstrated.

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 PROF. ALDEMIR: Well, I mean, I agree with
2 you, of course. There is nothing to disagree but, you
3 know, we have to do -- either we do nothing or we do
4 something.

5 CHAIRMAN APOSTOLAKIS: Correct, something,
6 correct.

7 PROF. ALDEMIR: If we are -- and if we
8 have to have time constraints, we have to do something
9 fast. We have to use available stuff.

10 CHAIRMAN APOSTOLAKIS: Listen. It cannot
11 be a Procrustean bed. You have to do something. I
12 agree. But remember Procrustes and what happened to
13 him. So let's go. Don't feel that you have to do
14 something --

15 PROF. ALDEMIR: No.

16 CHAIRMAN APOSTOLAKIS: -- even if it's
17 wrong.

18 PROF. ALDEMIR: But I can make the same
19 arguments about all the other, for example, common
20 cause failure models.

21 CHAIRMAN APOSTOLAKIS: No, they are not
22 like that. Come on. They are not. They are crude,
23 but they are not wrong. There is a big difference, a
24 big difference.

25 PROF. ALDEMIR: Okay. So --

1 CHAIRMAN APOSTOLAKIS: So where are you
2 now, Slide 19?

3 PROF. ALDEMIR: Slide 19 and, basically,
4 the model story of this Slide 19 is that the top two
5 ranking ones are dynamic flow methodologies.

6 CHAIRMAN APOSTOLAKIS: I see you have an
7 example later.

8 PROF. ALDEMIR: I will come to that.

9 CHAIRMAN APOSTOLAKIS: Maybe the
10 Subcommittee is interested more in that. We keep
11 seeing acceptance criteria and they more or less
12 repeat themselves, don't they?

13 PROF. ALDEMIR: Acceptance criteria. By
14 the way, we are defining it in a slightly different
15 way.

16 CHAIRMAN APOSTOLAKIS: I understand that,
17 but, I mean, you have already stated your position.

18 PROF. ALDEMIR: Yes, right. Okay.

19 CHAIRMAN APOSTOLAKIS: So I'm asking you
20 whether it would be worthwhile going to Slide 22.

21 PROF. ALDEMIR: Okay.

22 CHAIRMAN APOSTOLAKIS: Do you think you
23 are skipping something that's very important? It's
24 late in the day.

25 PROF. ALDEMIR: Not really, because I

NEAL R. GROSS

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

1 stated, like you said, I stated most of them. I am
2 trying to condense them, basically, from 11 to 7.
3 That's all there is to it.

4 CHAIRMAN APOSTOLAKIS: 22.

5 PROF. ALDEMIR: Now, what I am trying to
6 show you here is how the process couples failure
7 events or, actually, stochastic and it demands events
8 that may take place on demand. So what we have here
9 is, I guess, a real system from a BWR/6 and this is
10 supposed to provide core cooling in case the RCIS, the
11 reactor core insolation cooling system, becomes
12 incapacitated.

13 And I'm not going to go through the system
14 description in detail, because I'm sure everybody is
15 more familiar with it than I am. But the key point is
16 that there is a high pressure core spray system
17 consisting of many components, and there are three
18 sets of safety relief valves. What we will try to do
19 is to just concentrate on one of them.

20 So the incident that we have in mind is
21 the following. There is a small break which
22 incapacitates the RCIC system. In this situation it
23 so happens that the enthalpy lost through the break is
24 larger than the enthalpy addition due to decay heat.
25 So the level goes down, pressure goes up. So you can

NEAL R. GROSS

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

1 get the HPCS pump started through two signals, either
2 the first low level signal or the high radiation
3 signal in the containment.

4 The HPS pump starts, but nothing happens,
5 at this point, until the level hits the low, low mark,
6 I think it's the second low mark, in which case the
7 injection valve opens and water is sprayed, so the
8 level starts. In the meantime, of course, it reduces
9 the pressure a little bit, but not sufficiently, so
10 you may need to -- the SRV, which is pressure-
11 activated, SRV 1, safety relief valve 1, opens and it
12 relieves pressure, so the level comes -- it starts
13 spraying water, the level starts going up.

14 When you hit the high pressure mark, this
15 valve closes, pump doesn't stop, keeps circulating
16 water heat through the jockey pump. And when the
17 pressure comes down, the set point and the safety
18 valve closes, so you feed, you try to cool the core
19 through a feed/bleed cooling mode.

20 Now, it is desirable, I have been told, to
21 operate like this with using one SRV, because it takes
22 less time to start up the reactor again in the future.
23 So the top events that we defined -- oh, before I go
24 into that. The system, as you see, is very complex.

25 CHAIRMAN APOSTOLAKIS: This is not

1 software.

2 PROF. ALDEMIR: No.

3 CHAIRMAN APOSTOLAKIS: This is just Type
4 I dynamic.

5 PROF. ALDEMIR: No, Type I, Type I
6 interaction. There is no example of Type II
7 interactions, none in the literature that we have
8 seen.

9 CHAIRMAN APOSTOLAKIS: So you will
10 consider software here in Type I interactions?

11 MR. ARNDT: This is just an illustration.
12 Go ahead.

13 PROF. ALDEMIR: An illustration of how
14 Type I interactions tie up, coupled failure events.
15 Type II, there are two effects of the digital aspects.
16 One of them is the closer communication between the
17 devices, which makes the Type I coupling much worse
18 than this one and two on top of that, you have Type II
19 coupling or Type II there. There is no model. There
20 is no application of Type II interactions, so that's
21 why I'm showing this one.

22 So you try to control the water, I mean,
23 cool the reactor through feed/bleed cooling mode and
24 although this is a complex system, as you see, for
25 modeling purposes we can make it simpler. This comes

1 to the one-input, one-output model that I was talking
2 about, even if it's a digital controller inside. As
3 long as they are within the shaded area, I can regard
4 it as a single controlled, single structural unit or
5 micro component, which is what I'm doing in the next
6 picture.

7 And since I am using one safety relief
8 valve, I am regarding it as a single component, in
9 spite of its intricate construction. Either I have
10 data or I'm modeling it through conventional
11 techniques to get failure data. So this is how it
12 looks for modeling purposes. Then these are the set
13 points and we are talking about -- okay, sorry. Let
14 me go back here.

15 We are talking about four set points.
16 Either I go below a certain level or go above a
17 certain level, sorry, high level, low level possible
18 failure mechanisms and the high pressure/low pressure.
19 Now, these don't have safety implications obviously.
20 What the low level signal will do is it initiates the
21 RPCS system, but the point is that it will affect the
22 demand frequency of the RPCS.

23 So although this is not a safety-related
24 issue, it has safety implications from a PRA
25 viewpoint, because if you do a PRA, you are going 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 change the demand frequency on the RPCS. And again,
2 the pressure, of course, you know, if SRV 1 does not
3 respond, then you have the other SRVs and you can go
4 for manual operation and so forth.

5 So the incident that we had here, I looked
6 at, is a 1 percent double-ended guillotine break.
7 Pressure reaches whatever in two minutes following the
8 loss of --

9 CHAIRMAN APOSTOLAKIS: What do you mean by
10 1 percent?

11 PROF. ALDEMIR: Of area.

12 CHAIRMAN APOSTOLAKIS: So double-ended at
13 the largest pipe and you are considering 1 percent of
14 that?

15 PROF. ALDEMIR: No, no, we are talking
16 about a small, small break here, small instrumentation
17 break.

18 CHAIRMAN APOSTOLAKIS: I don't know. What
19 does --

20 DR. BONACA: You mean 1 percent of the
21 double-ended --

22 CHAIRMAN APOSTOLAKIS: If the largest pipe
23 has an area A, you are considering a pipe that has
24 area 1 percent of that?

25 PROF. ALDEMIR: Yes.

1 CHAIRMAN APOSTOLAKIS: And that breaks?

2 PROF. ALDEMIR: That's right.

3 CHAIRMAN APOSTOLAKIS: Okay.

4 PROF. ALDEMIR: Level reaches whatever in
5 two minutes following the LOCA, so these are your
6 initial conditions and we're assuming that the major
7 contributor to the HPCS failure is the failure of the
8 injection valve.

9 Now, this is the results of the analysis
10 using the cell-to-cell mapping technique. I don't
11 know if I should read this through, but the point is
12 that the failure mode of the system depends very much
13 on the exact timing of the failures and exact location
14 of the system variables at the time of the failure.
15 That's what comes out of this picture.

16 CHAIRMAN APOSTOLAKIS: Give us an example
17 of the exact time.

18 PROF. ALDEMIR: Examples. Low level,
19 which is minus 148 inches, occurs. If only HPCS fails
20 or only SU2, which is the SRV, fails to open. High
21 level occurs if SU2 fails closed after SU1 fails
22 after.

23 CHAIRMAN APOSTOLAKIS: After?

24 PROF. ALDEMIR: After. So high pressure
25 occurs if the level at the time of the SRV failure is

NEAL R. GROSS

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

1 such that it takes longer for the level to reach the
2 low level point, 100 minus 148 inches, than the time
3 it takes for the pressure to reach 1110 psi. And
4 there are two other examples how this exact timing is
5 important at the time of failure. This was a study we
6 did a long time ago. It has been now, what, 15 years.

7 CHAIRMAN APOSTOLAKIS: But you know how
8 the event tree guys would model this if they realized
9 it. They would have SU1 fails. Well, that's easy.
10 Yes, SU1 fails and then ask does SU2 fail afterwards?
11 Put it on the right of the event tree and then you
12 would have a number of consequences. If they put it
13 on the left, you have another kind.

14 I mean, there are good ways of doing these
15 things and, as you know, that's why the people have
16 not embraced the dynamic methodologies, you know,
17 since you guys started screening because, you know,
18 the same thing with electric power. You remember how
19 they model. Even in the Reactor Safety Study they say
20 what is the probability that off-site power will be
21 recovered before the diesels fail, and they have a
22 crude equation with an integral there and it's not
23 very accurate, but it's good enough.

24 PROF. ALDEMIR: But remember here, you
25 know, there are two types of situations. I mean, if

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 it were just sequence dependence, I would agree with
2 you, but it not just sequence dependence.

3 CHAIRMAN APOSTOLAKIS: Okay. What else is
4 there?

5 PROF. ALDEMIR: This bullet here. It's
6 the exact timing.

7 CHAIRMAN APOSTOLAKIS: Okay.

8 PROF. ALDEMIR: This one. This one. All
9 three exact timing, not sequenced. These are
10 sequenced.

11 CHAIRMAN APOSTOLAKIS: So why aren't they
12 listening to you?

13 PROF. ALDEMIR: Because two reasons.

14 CHAIRMAN APOSTOLAKIS: This is not just
15 software.

16 PROF. ALDEMIR: I will give you two
17 reasons.

18 CHAIRMAN APOSTOLAKIS: Okay.

19 PROF. ALDEMIR: The first reason is that
20 it is hard to follow this methodology. The second
21 reason is that they say, you know, from the workshop,
22 that's what Stefan Hirshberg said, so what? So if you
23 are right, what do I care if it is not very
24 significant? In fact, the same comment was made
25 earlier. You know, if the digital I&C system failure

NEAL R. GROSS

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

1 is not significant to core malfrequency, what do I
2 care?

3 Now, nothing has been done so far for a
4 full PRA to show that and I think this is an excellent
5 opportunity to do it, which we are proposing to do, by
6 the way. So that is why we haven't been listening and
7 I'm very happy that, you know, we have such an
8 occasion to look at it and see if it is really
9 significant or not.

10 Okay. I just summarized it, but I want to
11 mention these two here, which are going to be
12 important. You see, we are overestimating the low
13 pressure probability by a factor of 3 and
14 overestimating low level probability by a factor of 2.
15 Now, if we had digital controllers in place, because
16 of tighter coupling I would have expected much larger
17 differences.

18 And you see the other interesting result,
19 and that is part of the controversy. High level/high
20 pressure results are very close to conventional
21 methodology results. So sometimes it's okay,
22 sometimes it isn't okay, and that is the other
23 argument that people have raised. So as a regulator,
24 for example, in the old days, NRC would say what do I
25 care? You know, it's safe, no problem, 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 think in today's risk-based environment.

2 So anyway, conclusions. No single
3 methodology satisfies all requirements, namely for
4 DFM, for example. The only thing that is really
5 missing is the data business, but of course that is
6 true for everything. Data, even if we had data, it's
7 not going to be convincing. It's not going to be
8 credible to a significant portion of the technical
9 community. We need to show that DFM is capable of
10 describing the system dynamics properly and the
11 alternative is Markov approach.

12 Oh, I have two more. And what happens
13 when you don't use dynamic event trees? Well, we
14 don't have any evidence on digital Type II
15 interactions. What we have is only evidence on Type
16 I interactions, which says that, which implies, not
17 says, but implies, part of it is a little bit
18 conjecture, that if the system is a single failure
19 mode, if it doesn't have logic loops, if it doesn't
20 have substantial time delay with respect to the system
21 time constants between the initiation of the fault and
22 system failure, then the likelihood is high that the
23 event tree/fault tree approach is going to give good
24 results.

25 Now, if we extrapolate this evidence to

1 the digital I&C systems, what we can say is the
2 following. The ET/FT approach may yield satisfactory
3 results as the conventional one when a digital system
4 does not interact with a process that has multiple top
5 events, logic loops and so forth is basically a
6 repetition of these three, rely on sequential
7 circuits, which have memory, have tasks which compete
8 for the I&C system resources and anticipate future
9 states of the controlled/monitored process.

10 That's why I said RPS system is the most
11 likely one that can be modeled using the static event
12 tree/fault tree approach, but I don't know exactly how
13 this system works. If there is extensive
14 communication within the system, you know, some of
15 these, and I think Bill mentioned earlier or somebody
16 mentioned earlier, that there is a computer in there
17 and you are looking at future states, so I'm not sure
18 in that respect. So what we were proposing to do is
19 first --

20 CHAIRMAN APOSTOLAKIS: Now, before you go
21 to that, you are focusing here on dynamic stuff, which
22 is important and so on, but another dimension, and I'm
23 not sure it's a truly different dimension, but in the
24 spirit of helping, you are aware of this thing that
25 we're talking about that a failure of a software

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 should be looked at in the context in which the
2 software is used.

3 PROF. ALDEMIR: Yes, right.

4 CHAIRMAN APOSTOLAKIS: That there is a
5 classic example with the landing gear of an airplane
6 that Chris used as an example.

7 PROF. ALDEMIR: Yes, I read the paper.

8 CHAIRMAN APOSTOLAKIS: Where the airplane
9 was on the ground and the pilot ordered the system to
10 raise the landing gear and the system obeyed. There
11 should have been something there forbidding it to do
12 that if the plane is on the ground. So the question
13 that was raised is is that software now faulty? I
14 mean, can you say that the software -- no. One school
15 of thought says the software did what it was supposed
16 to do. It's the designer who screwed up.

17 PROF. ALDEMIR: Yes, specification error,
18 specification error.

19 CHAIRMAN APOSTOLAKIS: With the
20 requirements, requirements actually, not the
21 specifications. So what is the failure of the
22 software sometimes is not obvious, because the
23 software did it.

24 PROF. ALDEMIR: Yes, that's why --

25 CHAIRMAN APOSTOLAKIS: He wanted me to

1 raise the landing gear. I am going to do it. You
2 know, so the context is very important. I mean, if
3 it's flying, it's good. If it's on the ground, it's
4 not good and that's a trivial example, of course, but
5 it happened actually. It happened. So I don't know.

6 And then, of course, the example we have
7 been using here is the abnormal events, external
8 events that require the software to do something
9 extraordinary, and that's when you see that there is
10 a problem. So should you make context as another
11 dimension of all this and how does that fit into what
12 you are describing?

13 PROF. ALDEMIR: I'll let Steve comment and
14 then I will comment.

15 CHAIRMAN APOSTOLAKIS: Okay.

16 MR. ARNDT: Yes. The concept that you are
17 putting forth is a very important issue and how
18 context-specific, if you will, are certain situations
19 is also a big issue.

20 CHAIRMAN APOSTOLAKIS: Yes.

21 MR. ARNDT: And that drives us to the
22 kinds of questions we were asking last night. What
23 kind of modeling is necessary? What level of detail
24 of modeling not only in terms of how many circuits and
25 things like that, but how much of the process, how

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 of the specification, what kinds of issues do you
2 have to deal with?

3 As I go back to what I talked about
4 yesterday, one of the big issues in developing both
5 guidance for what is acceptable from a licensee PRA,
6 as well as what we want in our own PRA, and asking
7 these kind of questions and that's part of both
8 developing the methodologies, as well as understanding
9 what the requirements need to be, what level of
10 information do you have to embed in the process model.
11 And one of the toughest ones, as you have pointed out,
12 is how do you deal with specification issues.

13 CHAIRMAN APOSTOLAKIS: Yes, and
14 requirements.

15 MR. ARNDT: And requirements.

16 MR. KEMPER: The integration, what you are
17 trying to do is model what you don't know. Right?

18 CHAIRMAN APOSTOLAKIS: We are very good at
19 that.

20 MR. KEMPER: There may or may not be.

21 CHAIRMAN APOSTOLAKIS: We are very good at
22 that.

23 PROF. ALDEMIR: This is what we are
24 planning to do. You know, as has been clear so far,
25 not only we are taking software and hardware jointly,

1 but we are also taking the process as part of it. So
2 what you are --

3 CHAIRMAN APOSTOLAKIS: And the process may
4 create contexts.

5 PROF. ALDEMIR: Right.

6 CHAIRMAN APOSTOLAKIS: But we didn't say
7 anything about --

8 PROF. ALDEMIR: But you know, what we are
9 going to do is when we come to -- okay, maybe not I
10 think enough time here, but what we are going to do is
11 basically take this. If we can get a good description
12 of the feed water control system, which we are sure to
13 get --

14 CHAIRMAN APOSTOLAKIS: Yes.

15 PROF. ALDEMIR: -- then we are going to
16 couple it to a system simulator.

17 CHAIRMAN APOSTOLAKIS: No, no, no, but you
18 are now going into the details of how to do it.

19 PROF. ALDEMIR: But that's what will
20 happen.

21 CHAIRMAN APOSTOLAKIS: But you gave us a
22 presentation where you said, you know, there are
23 certain needs. I have to recognize a few things and
24 so on. And what I'm saying is shouldn't you also
25 recognize somewhat there that the context is

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 important?

2 PROF. ALDEMIR: Oh, you mean the
3 conclusions?

4 CHAIRMAN APOSTOLAKIS: And even before.

5 MR. ARNDT: Yes.

6 PROF. ALDEMIR: Okay, okay.

7 CHAIRMAN APOSTOLAKIS: When you have your
8 requirements and all that.

9 PROF. ALDEMIR: I see, I see. Okay.
10 Sure, sure.

11 CHAIRMAN APOSTOLAKIS: It seems to me --

12 PROF. ALDEMIR: Yes, yes, yes.

13 CHAIRMAN APOSTOLAKIS: Do you mention it
14 in the NUREG, draft NUREG?

15 PROF. ALDEMIR: No, no, good point, good
16 point.

17 CHAIRMAN APOSTOLAKIS: And what I'm saying
18 is that maybe it's something.

19 PROF. ALDEMIR: Good point.

20 CHAIRMAN APOSTOLAKIS: I thought that
21 example by Chris was very, very illuminating.

22 PROF. ALDEMIR: No, no, that's a valid
23 point.

24 CHAIRMAN APOSTOLAKIS: Yes. All this
25 applies to your work, too.

1 MR. ARNDT: Right. And where this is
2 going to be particularly important, and why we're
3 looking at particular kinds of methods, is how do you
4 develop a state-based model or whatever model you use
5 to feed the particular reliability models.

6 PROF. ALDEMIR: But in the report we --
7 what I think Professor Apostolakis is saying, that we
8 should make it a separate point.

9 MR. ARNDT: As explicit.

10 CHAIRMAN APOSTOLAKIS: Discuss it.

11 PROF. ALDEMIR: Good point, good point.

12 CHAIRMAN APOSTOLAKIS: I know you know
13 about it.

14 PROF. ALDEMIR: Yes.

15 CHAIRMAN APOSTOLAKIS: But good point,
16 good point. And we see all this stuff.

17 PROF. ALDEMIR: Right, good point.

18 CHAIRMAN APOSTOLAKIS: Because you see,
19 when you talk about state space, a new context may
20 create new states.

21 PROF. ALDEMIR: Right.

22 CHAIRMAN APOSTOLAKIS: There is a defined
23 support. Can you hear him?

24 MR. CHIRAMAL: The example, there is
25 something missing in the examples. My name is Matt

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 Chiramal, NRR. It starts off with a loss of off-site
2 power and the feed water pumps have tripped,
3 everything is tripped and it initiated with a large
4 break or a small break?

5 PROF. ALDEMIR: Small break.

6 CHAIRMAN APOSTOLAKIS: Small break.

7 MR. CHIRAMAL: So you mentioned the loss
8 of off-site power.

9 PROF. ALDEMIR: No, no loss of off-site
10 power.

11 MR. CHIRAMAL: Then the feed water system
12 would be working.

13 PROF. ALDEMIR: The break is such that it
14 incapacitates the reactor core isolation cooling
15 system.

16 MR. CHIRAMAL: Yes, but the thing is if
17 the feed water is running already, it supplies water
18 already.

19 PROF. ALDEMIR: Oh, you mean the -- oh,
20 yes, off-site power.

21 MR. CHIRAMAL: So you are missing a lot of
22 initials.

23 PROF. ALDEMIR: Okay.

24 MR. CHIRAMAL: Plus when it happened, the
25 second HPC pump also, high pressure injection pump,

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 tripped. There should be two, at least two or three
2 sometimes. You are looking at a system a lot more
3 better than when you read an example like that.

4 PROF. ALDEMIR: But the point is that the
5 paper is not here, so I'm not sure if I am capturing
6 all the assumptions that we had in the paper here in
7 this transparency. And you may be right. We might
8 have missed them in the original paper. But the point
9 is that the dynamics is not going to change very much.

10 CHAIRMAN APOSTOLAKIS: No, because the
11 feed water is an entirely different situation.

12 MR. ARNDT: Yes, we'll clean it up. The
13 point is that there are certain scenarios that when
14 you have competing events, the dynamics drive you to
15 the different conclusions.

16 CHAIRMAN APOSTOLAKIS: And I think another
17 thing you should do, Tunc, is nobody disputes what you
18 say, but what you really ought to do, as well, and
19 maybe you plan on some of it, is look at those crude
20 models that people use to handle these situations and
21 then draw some conclusions that the crude model is way
22 off or something like that.

23 PROF. ALDEMIR: We tried to do that.

24 CHAIRMAN APOSTOLAKIS: Because people are
25 aware of these things. I mean, even in the Reactor

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 Safety Study, as I said, they do. They do it.

2 PROF. ALDEMIR: And this came up again in
3 the --

4 CHAIRMAN APOSTOLAKIS: Not happily perhaps
5 or satisfactorily, but they do it.

6 PROF. ALDEMIR: In the workshop it came
7 again. You know, if we try to do that analysis, the
8 conventional analysis, people become skeptical. They
9 say well, of course, you know, how do you know, we
10 could have done -- Stefan Hirshberg was saying that
11 oh, I could do anything you can do with event
12 trees/fault trees.

13 CHAIRMAN APOSTOLAKIS: That's a song from
14 something.

15 PROF. ALDEMIR: But what he ends up doing
16 is exactly what we are doing, except not so
17 methodical. He uses a simulator. He generates
18 multiple event trees, multiple fault trees.

19 CHAIRMAN APOSTOLAKIS: I don't know what
20 you are trying to say now, but the truth of the matter
21 is that you are not identifying a situation that
22 people are completely unaware of. They are aware of
23 the fact that sequencing sometimes is important and
24 they have proposed very crude methods for handling
25 that and the classic case is loss of off-site power

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 when it is restored. Okay?

2 So if it is restored after the batteries
3 are exhausted, then I'm in trouble, right? So people
4 say well, gee, you know, I had to do that. Okay. How
5 long are the batteries going to last? 11 hours. What
6 is the probability that we will restore off-site power
7 in 11 hours? So they break it up into pieces that
8 they can handle.

9 Now, of course, you might say but how do
10 you know it's 11 hours? It might be something else.
11 And they will reply well, I don't need that kind of
12 detail, because I have already gotten my order of
13 magnitude number and that is good enough.

14 PROF. ALDEMIR: But there are two
15 different issues here. One of them is the sequencing
16 timing and subjectives, the phasing of mission, so to
17 speak, as you describe it. The other one is
18 interaction. They are different issues.

19 CHAIRMAN APOSTOLAKIS: No, I'm with you.
20 All I'm saying is that your arguments will carry more
21 weight if you acknowledge that other people are doing
22 something about some of these.

23 PROF. ALDEMIR: We did that in the NUREG.

24 CHAIRMAN APOSTOLAKIS: Okay.

25 PROF. ALDEMIR: It is in the NUREG. We

NEAL R. GROSS

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

1 did talk about phase missions and how people address
2 that issue. You are right. I mean, we did that.
3 That was Curtis Smith's --

4 CHAIRMAN APOSTOLAKIS: So what you are
5 telling me is I should read the NUREG?

6 PROF. ALDEMIR: No, no, there was no
7 implication, no.

8 CHAIRMAN APOSTOLAKIS: I started, by the
9 way. So can we go on now to the happy end, next
10 steps?

11 UNIDENTIFIED SPEAKER: Backwards.

12 PROF. ALDEMIR: Oh, backwards, okay.
13 Sorry. We are proposing to develop two benchmark
14 problems that will capture important features of the
15 existing I&C systems, and they have digital
16 counterparts. We want to do an analog. This was also
17 mentioned yesterday, that we should do that or
18 somebody should do that. We are planning to take an
19 analog system as is and if we can find -- the ideal
20 situation is to find something that was there earlier
21 and then that is there now and then compare the exact
22 systems as they are and if we can get access to the
23 data. I'm not sure if we can.

24 But anyway, we're going to come up with
25 two systems that will try to capture all 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 features that I mentioned, and we will use dynamic
2 flowgraph methodology and the Markov approach with a
3 common set of failure data to compare just the
4 capabilities, not necessarily data sensitivities or --

5 CHAIRMAN APOSTOLAKIS: What do you mean
6 "common set of failure data?" I mean, their needs may
7 be very different. I mean, if you give them the
8 failure data, you are forcing them to use it.

9 PROF. ALDEMIR: No, no, no.

10 CHAIRMAN APOSTOLAKIS: I mean, the failure
11 models that they are considering may be different.
12 Why don't you do it in pieces? First, ask the Markov
13 guys to come up with a state space and ask the DFM
14 guys to come up with the equivalent.

15 PROF. ALDEMIR: That's what --

16 CHAIRMAN APOSTOLAKIS: And then compare.

17 PROF. ALDEMIR: That's what we --

18 CHAIRMAN APOSTOLAKIS: Forget about
19 failure rates. When you say failure data, I don't
20 know what you mean.

21 PROF. ALDEMIR: Well, it could be --

22 CHAIRMAN APOSTOLAKIS: Don't give it to
23 them.

24 PROF. ALDEMIR: No, no, no. I'm sorry.
25 This is the situation. When I say "common set of

NEAL R. GROSS

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

1 failure data," the current plan is that the University
2 of Virginia is going to come up with the failure modes
3 of the system. Then we are going to use the same
4 failures. We're going to take those failure modes and
5 then try to see if the dynamic flowgraph methodology,
6 given the system description, how it operates, is
7 going to come up with the same failure modes, because
8 there may be a discrepancy. It's not clear at this
9 point.

10 CHAIRMAN APOSTOLAKIS: Yes, but that
11 doesn't mean that Virginia is right.

12 PROF. ALDEMIR: No, no, but we're going to
13 do comparison.

14 CHAIRMAN APOSTOLAKIS: So you're just
15 making part of it.

16 PROF. ALDEMIR: We are looking at both
17 failure modes. But what I'm trying to say here in
18 this bullet is we need to quantify.

19 CHAIRMAN APOSTOLAKIS: Yes.

20 PROF. ALDEMIR: So if we need
21 quantification, we'll try to make sure that both sets
22 are using the same data.

23 CHAIRMAN APOSTOLAKIS: Yes. I disagree
24 with your statement. We need to quantify no matter
25 what.

1 MR. ARNDT: We need to try to quantify.

2 PROF. ALDEMIR: It has to go into a full
3 PRA. I have to have numbers.

4 CHAIRMAN APOSTOLAKIS: Yes. Okay. Are we
5 going to have another chance to look at the benchmark
6 exercise?

7 MR. ARNDT: Yes.

8 CHAIRMAN APOSTOLAKIS: After the fact or
9 during the fact or before the fact?

10 MR. ARNDT: It's entirely up to you.

11 CHAIRMAN APOSTOLAKIS: Well, if I were
12 you, I would ask for it as early as possible, because
13 clearly there are some disagreements here.

14 MR. ARNDT: Okay.

15 CHAIRMAN APOSTOLAKIS: And I think it's
16 too late to resolve them today.

17 MR. ARNDT: Okay.

18 PROF. ALDEMIR: Okay. But anyway, the
19 intention is that if DFM and if we have agreement, and
20 I'm not sure if it's going to be that easy to resolve
21 at this point, I mean, from what Professor Apostolakis
22 said. And then we are going to take the results and
23 try to see how we can incorporate them into a full
24 PRA. And with dynamic flowgraph methodology, it's
25 fairly clear, because it gives prime implicates which

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 can replace the minimal cut sets within the PRA, so it
2 should integrate fairly easily.

3 If it turns out that we need more detail
4 for more physical process detail, then we'll also try
5 to see how we can get the Markov Model out, but then
6 try to put it in a mechanical fashion into an existing
7 PRA such as SAPHIRE. And also, we are doing it kind
8 of independently of this project, but we are also
9 looking at the feasibility of developing a dynamic
10 methodology on the SAPHIRE platform, but this is
11 another project.

12 (Whereupon, at 5:00 p.m. the meeting
13 continued into the evening session.)
14
15
16
17
18
19
20
21
22
23
24

E-V-E-N-I-N-G S-E-S-S-I-O-N

5:00 p.m.

CHAIRMAN APOSTOLAKIS: Thank you very much. Do you have anything else to say?

PROF. ALDEMIR: Oh, any questions?

CHAIRMAN APOSTOLAKIS: Steve, do you have anything to say that you really think is important?

MR. ARNDT: I guess not.

CHAIRMAN APOSTOLAKIS: Okay. Maybe we should go around. I don't know. Are there any questions?

MR. THORNSBURY: We have representatives from NSIR here in case they wanted to comment on the research process.

CHAIRMAN APOSTOLAKIS: Anybody who wants to speak? No. Okay.

MR. MORRIS: On this topic, no, or on any topic?

CHAIRMAN APOSTOLAKIS: We have one topic. Okay. Thank you very much. This was very, very helpful both yesterday and today and yesterday's speakers. I believe the Subcommittee has a much better idea now what's going on. The plan is to have another Subcommittee meeting to cover the rest of the plan, right? Then in October maybe, September,

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 October, sometime --

2 MR. SNODDERLY: October.

3 CHAIRMAN APOSTOLAKIS: October. You will
4 come and brief the full Committee, at which time we
5 will write a letter on the plan. Now, today maybe if
6 the Members are willing, they can give us preliminary
7 thoughts. If you are unwilling, that's fine, too.
8 What?

9 MR. ARNDT: The NSIR staff wanted to be
10 available to make comments on the overall plan.

11 CHAIRMAN APOSTOLAKIS: Yes.

12 MR. ARNDT: Not this particular
13 presentation.

14 CHAIRMAN APOSTOLAKIS: Okay.

15 MR. ARNDT: Do you want to hear from them
16 for a minute or two?

17 CHAIRMAN APOSTOLAKIS: Okay. Go ahead.

18 MR. MORRIS: I mean, I wasn't available
19 yesterday. I'm Scott Morris.

20 CHAIRMAN APOSTOLAKIS: Can you go there,
21 please?

22 MR. MORRIS: Yes.

23 CHAIRMAN APOSTOLAKIS: We have a
24 microphone.

25 MR. MORRIS: I'm Scott Morris from NSIR.

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'm one of the Section Chiefs in the Division of
2 Nuclear Security. I couldn't be here yesterday,
3 unfortunately. It's my understanding that the NRR
4 folks had an opportunity to comment as well. We only
5 looked at the cyber security portion of it, which I
6 think is Section 3.4. The research folks, Bill Kemper
7 and his staff, asked us to take a look at it and see
8 whether or not we had any heartburn with it or thought
9 we could make it do more.

10 CHAIRMAN APOSTOLAKIS: And you wrote a
11 memo, right?

12 MR. MORRIS: And we wrote a memo and I
13 think it summarizes it fairly well, but I guess the
14 point that I wanted to raise in this discussion is
15 that we -- you know, from a security standpoint, I
16 mean, you look at everything differently when you do
17 it from a safety standpoint, because it's not random
18 failures. I mean, it's bad people trying to do bad
19 things and take advantage of vulnerability, etcetera.

20 And so from our standpoint, we're
21 interested in any research that would help promote an
22 understanding of the vulnerabilities that exist and
23 how they could be exploited. Now, we are fairly far
24 down a path of devising a process, an approach. We
25 have issued a couple of NUREGs already you may or may

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 not be aware of that define a mechanism by which
2 licensees at reactor facilities or any facility, for
3 that matter, can employ this process and help
4 determine where their vulnerabilities exist.

5 It's a very well-articulated process and
6 it doesn't really -- from a big picture standpoint, we
7 really don't care what happens inside of the box. We
8 just want to know of a box that may control a safety
9 system. We don't really care.

10 CHAIRMAN APOSTOLAKIS: Are these Official
11 Use Only?

12 MR. MORRIS: Yes. They haven't been
13 widely disseminated.

14 CHAIRMAN APOSTOLAKIS: But we can have it?

15 MR. MORRIS: Absolutely.

16 CHAIRMAN APOSTOLAKIS: Yes.

17 MR. MORRIS: I'll make those available to
18 you. But the point is it's not so important to us to
19 know how all the inner workings of the -- we just want
20 to know, number one, look out, look at your site.
21 Figure out what systems are important to you from a
22 safety standpoint, then figure out how those systems
23 are controlled, operated, monitored, whatever and how
24 they can be exploited from an external adversary or
25 even an internal.

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 figure out if this is the box, how is
2 it connected to the outside world, and to take a look
3 at all those connections and make sure that you're
4 satisfied that they are either secure through a system
5 of barriers or protocol, whatever. And if they are,
6 fine, but to figure out what they all are and then use
7 a risk-based approach to determine which ones you need
8 to do something with or not.

9 And we have, as I said, been -- we have
10 prepared these detailed methodologies. We were aided
11 by the industry, because we have piloted it at four
12 different sites. We had PNNL help. Pacific Northwest
13 National Lab helped us devise this with their
14 expertise. And now, we're working with the industry
15 themselves, Nuclear Energy Institute, and their own
16 Cyber Security Task Force to develop a program
17 management document.

18 They currently have it published, it's NEI
19 04-04, that they use, but it's to take what we have
20 developed as a staff, to use this cyber security self-
21 assessment methodology and then put a programmatic
22 overlay over the whole thing to help individual
23 licensees identify it and manage the risks of cyber
24 security at their facilities.

25 And we're working very closely with them,

NEAL R. GROSS

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

1 commenting on that whole thing. So with all of that
2 as a background as to what NSIR is doing, a very non-
3 detailed description, we looked at the research plan,
4 from what they wanted to do or what they had proposed
5 to do, and of course our overriding comment was hey,
6 anything you can do to help us implement this process,
7 that's our top priority.

8 But we understand there is benefit to
9 doing some degree of anticipatory research to look
10 inside the box, you know, to enhance our understanding
11 of what's actually out there and to do some research
12 to look at validating what we think we know, but do we
13 really know it, you know, and how some of the software
14 works.

15 All that is legitimate, but it doesn't
16 directly help me necessarily. It may add credibility
17 to the overall, what we're doing, but it doesn't -- so
18 our comments were all based on we're doing this.
19 Anything you can do to help us implement this is
20 great. We understand there's a need to do these other
21 things at some good level. You know, NRR can weigh in
22 on that and I think they have.

23 CHAIRMAN APOSTOLAKIS: But you said you
24 went to PNNL for help.

25 MR. MORRIS: Yes.

1 CHAIRMAN APOSTOLAKIS: Why shouldn't that
2 activity be part of the plan or maybe there is no
3 reason for it to be part of the plan. But I mean,
4 does PNNL know -- would PNNL benefit from interactions
5 with Steve and Mike and their contractors, because
6 that's really the question. I mean, if it's an
7 isolated activity that is really very different from
8 what the rest of the guys are doing --

9 MR. MORRIS: I'm not sure. I think Eric
10 can tell you better.

11 CHAIRMAN APOSTOLAKIS: I mean, you create
12 a plan usually because there are activities that have
13 a common goal and there may be synergies. You know
14 how it is.

15 MR. MORRIS: Yes, I understand.

16 CHAIRMAN APOSTOLAKIS: But if your needs
17 are so different that really you are not going to
18 benefit from anything that these guys are doing, then
19 maybe what you did is good enough. Otherwise, the
20 question is why weren't PNNL part of this?

21 MR. KEMPER: Well, let me try to address
22 that. Our approach in the cyber area is to take an
23 inside and outside approach. We're looking at what's
24 the vulnerability of safety-related digital control
25 systems and other things are connected to from 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 inside threat as well as an outside threat. So that's
2 why we started from the inside. It's important to
3 understand the protocol and communication lessons
4 between one process over another to get a better
5 appreciation for what the vulnerability is.

6 As Todd said, we're trying to assess the
7 vulnerability, not the threat, that's up to -- the
8 threat. So until we actually start taking these
9 systems apart and looking at their susceptibility to
10 cyber attacks --

11 CHAIRMAN APOSTOLAKIS: But you are not
12 looking for those, are you?

13 MR. KEMPER: Oh, yes. We haven't
14 explained it to you yet.

15 CHAIRMAN APOSTOLAKIS: Oh, okay. This is
16 one of the next meetings.

17 MR. KEMPER: This is the next meeting,
18 right.

19 CHAIRMAN APOSTOLAKIS: Okay. Okay. Maybe
20 you should come to the next meeting.

21 MR. MORRIS: We'll be there.

22 MR. KEMPER: Okay. So that's the inside
23 part. And then, of course, there's the another --

24 CHAIRMAN APOSTOLAKIS: I understand that.

25 MR. KEMPER: -- which is the outside.

NEAL R. GROSS

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

1 We're going to look at a typical, you know,
2 configuration of connectivity of power plants and try
3 to see what's the vulnerability of that.

4 CHAIRMAN APOSTOLAKIS: Even with that
5 though, NSIR says that you are not really helping.

6 MR. WATERMAN: Well, to interject, when we
7 received NSIR's comments and follow-up comments --

8 CHAIRMAN APOSTOLAKIS: Okay.

9 MR. WATERMAN: -- into the research plant,
10 additionally, the NUREG 6047, as I've read it --

11 COURT REPORTER: Sorry, when you speak,
12 move the microphone over.

13 MR. WATERMAN: Oh, okay.

14 CHAIRMAN APOSTOLAKIS: We were whispering,
15 but --

16 MR. WATERMAN: Mike Waterman in research.
17 As I understand 6047, it is designed to look at
18 installations in nuclear power plants, right now look
19 for vulnerabilities in installed systems. It's our
20 research plan to address more of that. However, the
21 other area that we're looking at is guidance for
22 developers of new networks that haven't been installed
23 in plants yet to tell if these are the things you
24 ought to be considering when you are thinking about
25 designing a secure network to put into a plant, so we

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 can sort of head off some of the issues that Scott is
2 trying to deal with right now.

3 Instead of having bad networks installed
4 in the plants and then having 6047 and tools deal with
5 those issues once they are in, we're also trying to
6 provide guidance that have --

7 CHAIRMAN APOSTOLAKIS: It seems to me that
8 all this really should be discussed at the next cyber
9 meeting.

10 MR. MORRIS: Well, I just wanted to say
11 that this is premature.

12 CHAIRMAN APOSTOLAKIS: It's a little
13 premature, yes, but especially --

14 MR. MORRIS: Yesterday you guys talked
15 about some of this stuff.

16 CHAIRMAN APOSTOLAKIS: Yes.

17 MR. MORRIS: It happened then.

18 CHAIRMAN APOSTOLAKIS: Okay.

19 MR. MORRIS: But I think you do need to be
20 aware of --

21 CHAIRMAN APOSTOLAKIS: Yes.

22 MR. MORRIS: -- that there is a fairly
23 significant level of activity going on.

24 CHAIRMAN APOSTOLAKIS: Yes, the next
25 meeting will be probably some time in August perhaps.

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. THORNSBURY: Or September.

2 CHAIRMAN APOSTOLAKIS: September is hard
3 for some of us.

4 MR. THORNSBURY: It will be in one of
5 those two.

6 CHAIRMAN APOSTOLAKIS: Is that okay with
7 you guys?

8 UNIDENTIFIED SPEAKER: It would be okay
9 with us. August would be --

10 MR. KEMPER: I won't be able to
11 participate.

12 CHAIRMAN APOSTOLAKIS: August is --

13 MR. KEMPER: Because I mean, in August I'm
14 away on vacation.

15 UNIDENTIFIED SPEAKER: In July?

16 CHAIRMAN APOSTOLAKIS: After the middle?

17 MR. KEMPER: Oh, after the middle.

18 DR. BONACA: After the middle we're going
19 to transfer me, right? So then we have a couple of
20 good preparation for the full meeting. We have --

21 MR. SNODDERLY: Mario, was there a
22 subcommittee scheduled yesterday for September for
23 Browns Ferry? I think there was.

24 CHAIRMAN APOSTOLAKIS: Probably was.
25 Actually, we scheduled something.

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. SNODDERLY: So you may want to tag it
2 on to that.

3 CHAIRMAN APOSTOLAKIS: Yes.

4 MR. SNODDERLY: Because you never know
5 when the time --

6 DR. BONACA: And that's going to be
7 probably involving most members.

8 MR. SNODDERLY: Right.

9 DR. BONACA: Because of all the mix.

10 CHAIRMAN APOSTOLAKIS: Visit where?

11 DR. BONACA: It's going to be here, but we
12 return subcommittee on Browns Ferry.

13 MR. THORNSBURY: Okay. We'll work that
14 out.

15 DR. BONACA: We talked to the staff.

16 MR. SNODDERLY: So Eric will work with
17 Steve --

18 CHAIRMAN APOSTOLAKIS: Well, remember that
19 the --

20 MR. SNODDERLY: -- to come up with an
21 agenda.

22 CHAIRMAN APOSTOLAKIS: Right. I mean,
23 it's hard for me to -- Monday, Wednesday is going to
24 be very hard to get it.

25 DR. BONACA: The trouble now, you know,

NEAL R. GROSS

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

1 with meeting July 20th and then the summer is getting
2 all scheduled with meetings.

3 CHAIRMAN APOSTOLAKIS: Anyway, Tom, you
4 want to say a few words?

5 DR. KRESS: Yes, I can give some
6 impressions.

7 CHAIRMAN APOSTOLAKIS: Yes.

8 DR. KRESS: First of all is I'm awfully
9 glad to see research doing this. I think it's stuff
10 that we have called for in the past and it's going to
11 be badly needed and it's going to be, I think, very
12 helpful. I like the idea of up front looking for
13 modes of failure first, types of failures you have by
14 searching out. I'm afraid you won't find very many
15 out there though.

16 I like the thought that the EPRI guy, he's
17 not here now, suggested that have you thought about
18 looking at whether or not you can declare all digital
19 systems, I&C systems better than analog and therefore
20 you could either say that the risk is not that
21 significant or you could just use the analog value and
22 say you've bound it. I like that thought.

23 One thing that struck me is that basically
24 everything we are doing in terms of looking at digital
25 software failure rates, failure probabilities seems 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 imply that the failure is a random event and we know
2 they are not. And I think the one unique failure
3 probability, I think it will be sequence dependent,
4 and maybe even time dependence within the sequence.
5 I think you have a problem looking for a failure
6 probability.

7 I think you need -- that's why you need
8 these failure modes and how they fail and how they
9 interact first, because I am very doubtful you will
10 get a unique failure probability. Other than that,
11 I'm sure glad that you guys are doing this, because
12 it's something that, I think, will bear fruit and be
13 very useful.

14 CHAIRMAN APOSTOLAKIS: Thank you, Tom.
15 Mario?

16 DR. BONACA: Yes, I'm commenting also on
17 some presentation we had yesterday morning. I felt
18 that Reg Guide 1.97 endorsing actually policy
19 standard, I think, is good. It is going in the right
20 direction. I don't know, however, about the
21 possibility of backfitting that Reg Guide to older
22 plants. That's an issue that is not submitting to us
23 it seems to me, at this stage.

24 We heard about the preliminary validation
25 of the methodology for assessing software quality. We

1 had a presentation yesterday morning. I was, I guess,
2 confused about what is in that report that was
3 presented, so --

4 CHAIRMAN APOSTOLAKIS: Which one is that
5 one?

6 DR. BONACA: It's the --

7 MR. SNODDERLY: Maryland.

8 CHAIRMAN APOSTOLAKIS: Maryland?

9 DR. BONACA: Yes. Maybe it was my problem
10 in digesting all the information in that document.
11 But I wasn't too convinced about that work. In so far
12 as the plan, the role plan, I think I totally agree
13 with you, Tom, that, you know, I really had an
14 appreciation developed yesterday and today for the
15 need for this work. I mean, clearly, I came out of
16 this meeting with increased concern with the use of
17 digital systems, although we know that they will be
18 here. And they will be used.

19 So, you know, one thought, we certainly
20 would like to get involved with the Ocone upgrade.

21 CHAIRMAN APOSTOLAKIS: Oh, yes.

22 DR. BONACA: As a means of learning more
23 about those issues you are bringing up, which is time
24 dependency, for example, that may mask certain faults
25 at first view. And, you know, my thought is that you

1 wanted to couple the design from the platform. But in
2 this case, it may be very well that the platform
3 itself or the process that you are using for the
4 digital design it seems to create the opportunity for
5 mistakes on the part of the design. There is that
6 kind of feedback there.

7 I thought that the plan was quite
8 significant and I hope that they can resolve their
9 differences with NRR. Clearly, I think that NRR is
10 writing and being involved in the finding of need, but
11 I think that we have to look forward and far on this
12 issue, because there are significant implications for
13 safety.

14 DR. KRESS: I hope that the apparent
15 negative reaction of NRR doesn't put a damper on this,
16 because, you know, I think this is anticipatory
17 research and might not even need a user need.

18 DR. BONACA: Yes, I mean, I don't see, you
19 know, given all we have heard, you have to get to it
20 and study and try to understand it and these are
21 pressing issues.

22 DR. KRESS: I mean, I thought NRR had the
23 feeling that they know how to do these reviews already
24 and they don't need this. But I think that's very
25 short sided.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: But it's also --

2 DR. BONACA: I think --

3 CHAIRMAN APOSTOLAKIS: -- important to
4 know that the attitude of the NRR people this time
5 around was very different than the first time we met.

6 DR. KRESS: Yes, there is change.

7 DR. BONACA: Yes, there is better
8 communication.

9 DR. KRESS: Somebody must have jumped on
10 them.

11 MR. SNODDERLY: Well, I think, Mario makes
12 a good point that we need to be very involved in the
13 Ocone review, because that will demonstrate NRR's
14 concern.

15 DR. KRESS: On how they --

16 MR. SNODDERLY: Right. Do they have the
17 tools, do they have the capability to do that?

18 CHAIRMAN APOSTOLAKIS: And we can --

19 MR. SNODDERLY: So we will have to --

20 DR. BONACA: Yes, I think that's great.

21 MR. SNODDERLY: -- have follow-up and find
22 out when that schedule is and where and make sure we
23 schedule that.

24 DR. BONACA: Remember, designing this
25 upgrade for Ocone.

1 CHAIRMAN APOSTOLAKIS: Framatome.

2 DR. BONACA: Okay. But, you know, I mean,
3 I think we will learn a lot from them.

4 CHAIRMAN APOSTOLAKIS: Oh, yes. Anything
5 else?

6 DR. BONACA: No, nothing.

7 CHAIRMAN APOSTOLAKIS: Good. Well, I
8 think my views were made clear more or less, but I
9 want to say that yes, I'm very pleased myself that the
10 staff is doing this. By and large, it is a very good
11 program, plan and I'm looking forward to seeing the
12 revised schedule that you gentlemen are working on
13 now. I also have serious doubts about the usefulness
14 of all this metric thing that was presented. It was
15 yesterday. Actually, I have more than doubts, but I
16 just want to say doubts. I don't think it's useful at
17 all.

18 DR. KRESS: The fault density?

19 CHAIRMAN APOSTOLAKIS: What?

20 DR. KRESS: The fault density, you meant?

21 CHAIRMAN APOSTOLAKIS: No, the other one
22 with -- I don't know, the Maryland one.

23 DR. BONACA: Yes.

24 CHAIRMAN APOSTOLAKIS: The metrics. I
25 don't see how that can help a decision-maker. Well,

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 I have problems with the fault injection when they
2 start developing failure rates, but I think a good
3 thing about this meeting and the last meeting we had,
4 but especially this one, is I think we are beginning
5 to understand each other much better. But there are
6 some fundamental issues that bother me. And, you
7 know, you gentlemen showed some appreciation for some
8 of them anyway.

9 DR. KRESS: I thought they needed a better
10 definition of fault and a specific comment.

11 CHAIRMAN APOSTOLAKIS: Yesterday?

12 DR. KRESS: Yes. You know, you're trying
13 to determine the number of remaining faults by some
14 process, which I thought might be reasonable. But
15 it's the denominator that goes into that that bothers
16 me. And I think you need to think about that
17 denominator.

18 CHAIRMAN APOSTOLAKIS: Any time anybody
19 does a historical to determine the number of remaining
20 faults, you should be awfully skeptical.

21 DR. KRESS: Yes, but it's -- you know, the
22 numbers --

23 CHAIRMAN APOSTOLAKIS: But it is a
24 difficult issue.

25 DR. KRESS: The denominator worried me

1 more than that.

2 CHAIRMAN APOSTOLAKIS: So I think today's
3 presentations were -- not presentations, the substance
4 of it was much better. Some of the stuff was
5 presented yesterday, not all of it. A lot of it was
6 good, too. So I think we are on our way and we're
7 going to review the rest of the plan and then write a
8 letter on the plan itself. But also, what is not
9 clear in my mind is how we're going to comment on the
10 individual projects now.

11 So, at some point, I mean, you know, this
12 is research. Do they have to come to us? They don't
13 have to, do they? Professor Aldemir finished at
14 present three new reports to issue. I don't think the
15 staff is -- there is a mandatory for them to come to
16 us, unless we request it.

17 MR. SNODDERLY: For review, right, unless
18 we request to review the new reg reports.

19 CHAIRMAN APOSTOLAKIS: Steve?

20 MR. ARNDT: You're right. It's a decision
21 of the staff whether to issue publications or not.
22 Now, not necessarily Professor Aldemir's work, but any
23 of our work. If it goes into regulatory
24 implementation, a Reg Guide or a revision of the SRP,
25 then you need to come to. The point, however, is, 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 we mentioned earlier in the day, there are certainly
2 times where we would want your input on decision
3 points and directions and things like that.

4 CHAIRMAN APOSTOLAKIS: Okay.

5 MR. ARNDT: Either in this forum or in
6 another forum and we'll work with Eric to try and do
7 that.

8 CHAIRMAN APOSTOLAKIS: So it would be sort
9 of a participatory review.

10 MR. ARNDT: Right.

11 CHAIRMAN APOSTOLAKIS: Which I think is
12 fine with the Committee.

13 MR. KEMPER: Can I ask a specific -- Bill
14 Kemper here. Yes, what I would like to do is we're
15 going to get together and kind of discuss our projects
16 and maybe identify those milestones where another
17 engagement with you all would be appropriate. Okay?

18 CHAIRMAN APOSTOLAKIS: Sure.

19 MR. KEMPER: So we're going to have to
20 take this to heart.

21 CHAIRMAN APOSTOLAKIS: Very good.

22 MR. KEMPER: And really value the
23 interaction here. You have given us some real good
24 things to think about. And, obviously, it makes us
25 feel a lot more comfortable knowing that we're on 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 path that you all are comfortable with.

2 CHAIRMAN APOSTOLAKIS: Yes.

3 MR. KEMPER: As opposed to violently
4 opposed to, you know, before we go public with that.

5 CHAIRMAN APOSTOLAKIS: Wonderful.
6 Anything else? Well, thank you gentlemen again. This
7 has been very useful and this meeting of the
8 Subcommittee is adjourned.

9 (Whereupon, the meeting was concluded at
10 5:23 p.m.)

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

CERTIFICATE

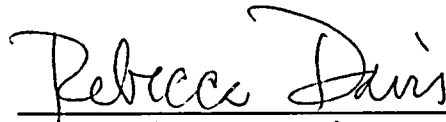
This is to certify that the attached proceedings
before the United States Nuclear Regulatory Commission
in the matter of:

Name of Proceeding: Advisory Committee on
Reactor Safeguards
Digital Instrumentation and
Control Systems Subcommittee
Meeting

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.



Rebecca Davis
Official Reporter
Neal R. Gross & Co., Inc.

Overview and Status of “Digital Systems PRA” Project



Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 15, 2005

Hossein Hamzehee

Probabilistic Risk Assessment Branch
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
(301-415-6228, hgh@nrc.gov)

Todd Hilsmeier

Probabilistic Risk Assessment Branch
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
(301-415-6788, tah1@nrc.gov)

Tsong-Lun Chu

Brookhaven National Laboratory
(631-344-2389, chu@bnl.gov)

Overview and Status of “Digital Systems PRA” Project

Purpose:

- **The purpose of this presentation is to:**
 - **Describe the “Digital Systems PRA” project plan.**
 - **Provide status of project.**
 - **Discuss tasks that are completed or in progress.**

Overview and Status of “Digital Systems PRA” Project

Presentation Outline:

- **Background**
- **Objectives of Digital Systems PRA**
- **Integrated Project Plan and Technical Tasks**
- **Discussion and Status of Tasks in Project Plan**
- **Schedule**

Background

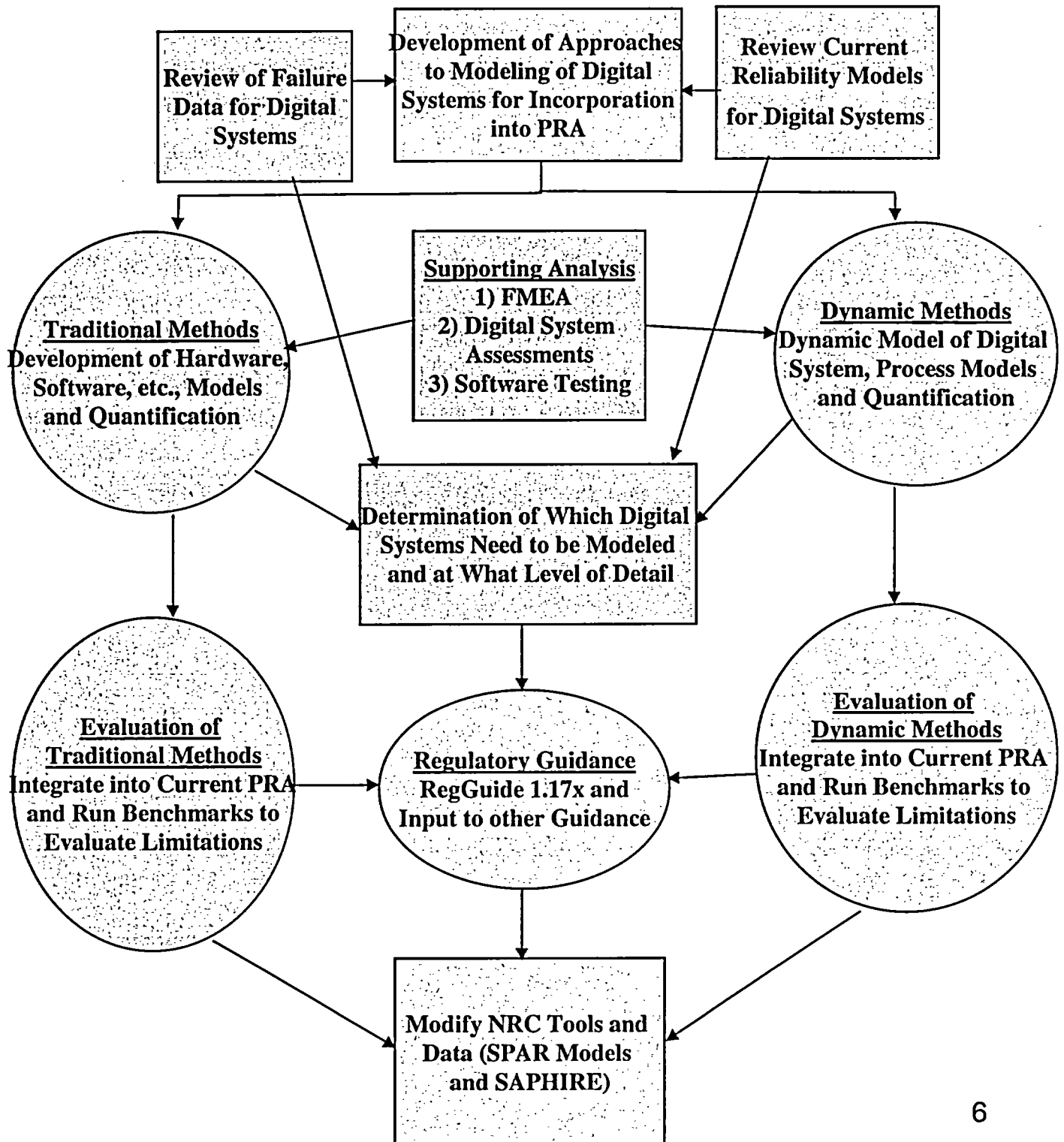
- **Nuclear power plants are replacing obsolete analog I&C systems with digital ones. Advanced reactors will use integrated digital I&C systems.**
 - **The following plants express interest in upgrading their analog RPS system to a digital platform: Oconee, Callaway, Wolf Creek, and Comanche Peak.**
- **NRR will be reviewing submittals on analog to digital system upgrades at nuclear power plants, which will require RES support. The PRA modeling of digital systems is important to support a risk-informed approach to evaluation and selection of digital systems (NRC's PRA Policy Statement, Regulatory Guide 1.174).**
- **Status of EPRI TR 1002835 Review:**
 - **EPRI TR 1002835: "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades".**
 - **NRR/RES currently performing an "acceptance review" to determine if NRC will review EPRI TR 1002835 in its current form.**
 - **After the acceptance review, NRR will develop a review schedule.**

Objectives of Digital Systems PRA

- **The objective of the project is to develop a probabilistic method for modeling failures of digital I&C systems that can be integrated with a PRA using traditional PRA methods (fault trees, event trees).**

- **Digital systems are not currently being treated adequately and uniformly in PRAs.**
 - **Lack of an acceptable approach for modeling digital systems in PRA (e.g. black box approach).**
 - **Current methods and data on modeling digital systems are not adequate.**

NRC Digital System Risk Program



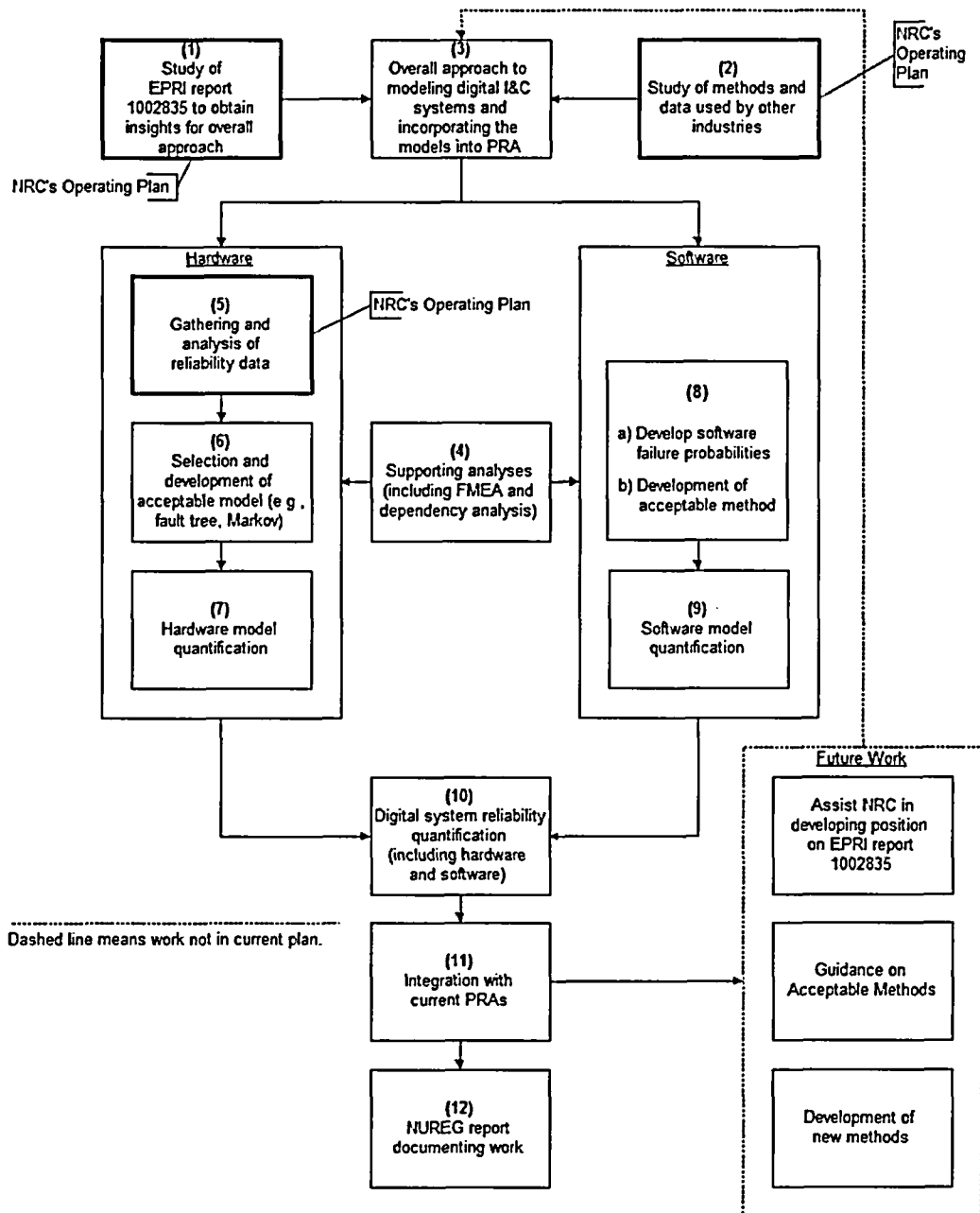


Figure 1
Technical Tasks/Activities Associated with Digital Systems PRA Project

Task 1

Insights from EPRI TR-1002835

Objective:

Review EPRI TR-1002835 (“Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades”) to obtain insights on reliability modeling of digital systems.

Observations:

- EPRI TR advocates the risk-informing of digital I&C systems.
- EPRI TR proposed to use simplified and standard risk-informed methods as alternatives to current deterministic method.
- The “Simplified Risk-Informed” method should be clarified and demonstrated with examples (may not provide conservative risk values).
- EPRI TR does not provide information on how to develop models needed in the “Standard Risk-Informed” method.
- EPRI TR does provide some characteristics to consider in model development.

Schedule:

Incorporating Research review comments into draft report.
Final report on Task 1 will be completed by June 30, 2005.

Task 2

Study Methods and Data Used by Other Industries

Objective:

Review industry experience for methods and databases used to model digital systems (including ways quantitative reliability analyses are used).

Observations:

- Approach:
 - Establish contacts (e.g., NASA, Army, Navy, Air force, DOE, DOD, DNFSB, FAA, Automotive, OMNICON, RAC, INL).
 - Search and collect guidance and reports.
 - Review reports.
- Most industries manage digital system risk through software development process, management, and testing.
- NASA appears to be moving to a quantitative risk evaluation approach using PRAs.
 - NASA Fault Tree Handbook and NASA PRA Procedures Guide were developed by experts with extensive nuclear plant PRA experience.
 - NASA Fault Tree Handbook contains standard fault tree methods with introduction of fault coverage of digital components.
 - NASA PRA Procedures Guide contains standard PRA methods tailored for NASA applications, and has a section on software risk assessment, which presented a frame work for considering software failures and proposed an approach for quantifying software failures.

Schedule:

Final Report to be completed by August 30, 2005.

Task 4

Supporting Analyses of Digital Features

Objective:

Obtain information about the behavior of a digital system.

- Develop a FMEA and a dependency analysis of the system (foundation of reliability modeling).
- Develop guidance on how communication and voting should be modeled.
- Analyses will support development of the digital system's reliability model.
- Applied to digital RPS system proposed for Ocone.

Estimated Period of Performance:

This task is expected to start in July 2005 and will be completed by September 2006.

Task 5

Collection of Failure Data and Development of Database for Probabilistic Modeling of Digital Hardware

Objective:

Develop failure database for digital hardware, based on currently available data, for quantifying digital system reliability models.

Analysis:

- **Database Development Approach:**

- Review failure rate databases - Military Handbook 217F, Telcordia, PRISM.
- Search industries for additional digital failure data (e.g., LERs, EPIX, NASA, SPAR, FAA).
- Development of population variability distributions using proprietary PRISM failure records.

Task 5 - Hardware Analysis (continued)

- **Military Handbook 217F, Telcordia, PRISM Failure Rate Prediction Methods:**
 - Use of empirical formula (not laws of physics) in predicting failure rates has been found to be inaccurate.
 - Applicability of empirical formula is limited to cases where applicable and adequate failure data is available. Extrapolation could lead to significant errors.
 - Lack of uncertainty consideration.

Task 5 - Hardware Analysis (continued)

● Review of Industry Experience:

- Existing PRA failure databases (SPAR database, NASA PRA guide, IEEE Std 500) do not include digital component failure rates.
- Advanced reactor PRAs (e.g. AP600 PRA -Westinghouse 1996) may contain limited digital failure rate data that are proprietary.
Will evaluate further in second phase of data analysis.
- Industry operating experience (e.g., nuclear plant - LER/EPIX, FAA, Army, DOE) contain digital failures, but do not contain information on: subcomponents that failed, how many of the same components/systems are in operation, and how long they have been in operation, which are needed to derive failure rate estimates.
Will evaluate further in second phase of data analysis.
- NASA failure database is proprietary. Database for public use will be available in 2006.
Will evaluate further in second phase of data analysis.
- COMPSIS [OECD 1999] is an international effort to collect I&C operating experience, and is still at its early stage of data collection.
Will evaluate further in second phase of data analysis.

Task 5 - Hardware Analysis (continued)

- **Population variability distributions using PRISM failure records:**
 - PRISM is a software developed by the Reliability Analysis Center (RAC) for making reliability predictions of series systems, e.g. circuit boards.
 - PRISM contains failure records of components (e.g., microprocessors and RAMs) from different sources (i.e., warranty repair data) in the form of “n failures in m hours”.
 - Large variations in failure data exist among different sources due to different specific designs, operating conditions, manufacturers, etc.
 - Development of Population Variability Distributions:
 - a) Hierarchical Bayes Analysis of PRISM Data.
 - b) More than 20 different digital components were analyzed.
 - c) Wide population variability distributions were obtained due to large variations in failure record.
 - This will be further evaluated in the second phase of data analysis.

Task 5 - Hardware Analysis (continued)

- **Conclusion:**

- PRISM data is main source for hardware failure rate development.
- Generated error factors could be large.
- Second phase of data development will review: possible additional failure modes, and additional databases (Manufactures, Advance Reactor PRA, INL, NASA, COMPSIS, LER/EPIX with cooperation from plants).

Schedule:

Final Report to be completed by August 30, 2005.

Task 6

Selection and Development of Acceptable Hardware Reliability Model

Objective:

Develop reliability model for digital system hardware (i.e., digital RPS system proposed for Oconee).

- Develop reliability block diagrams and transition diagrams that capture the behavior of digital system.
- Review industry guidance on Markov modeling.
- Either a fault tree or a Markov model will then be developed for failure on demand of the system.
- Develop guidance on modeling the behavior of digital features.
- Identify the data needed to support the quantification of the models.
- Comparison of digital and analog designs of I&C systems (i.e., digital RPS system proposed for Oconee).

Estimated Period of Performance:

This task is expected to start in October 2005 and will be completed by December 2007.

Task 7

Hardware Reliability Model Quantification for Selected Platform

Objective:

Quantify hardware reliability model using best available data for selected platform (i.e., digital RPS system proposed for Ocone).

- Discuss important contributors to system failure probability.
- Discuss assumptions that may have significant impacts on the results.

Estimated Period of Performance:

This task is expected to start in October 2006 and will be completed by December 2007.

Task 8

Development of Methods for Modeling Software Failures

Objective:

Develop an acceptable method for including software failures in a digital system probabilistic failure model.

- Review software-induced failure events in different industries to identify the failure modes, failure causes, occurrence frequencies, and the insights on modeling software failures in a PRA.
- Review additional literature to develop basis for modeling software failures in PRA.
 - Address issue of whether software failure rates are meaningful.
 - Consideration of uncertainties.
 - Evaluate different reliability methods (e.g., fault trees, Markov, reliability growth models, etc...).
- Develop quantitative software failure model.
 - Evaluate existing software reliability models.
 - Establish linkage between software and hardware models.
 - Determine software failure parameters that have to be quantified.
 - Different types of software have different effects on digital systems and may have to be modeled differently.
 - Apply them to specific example designs (i.e., digital RPS system proposed for Oconee).

Estimated Period of Performance:

This task is expected to start in July 2005 and will be completed by September 2008.

Task 9

Software Reliability Quantification for Selected Platform

Objective:

Quantify the software failure probabilities identified in Task 8 for selected platform (i.e., digital RPS system proposed for Ocone).

- The results of the task could be used in an integrated model of the digital systems (Task 10).

Estimated Period of Performance:

This task is expected to start in October 2007 and will be completed by September 2008.

Task 10

Digital System Reliability Quantification

Objective:

Perform quantification of the probability of failure on demand of the digital RPS system proposed for Oconee.

- Perform sensitivity calculations to evaluate Important assumptions.
- The combined model (hardware and software) will provide a system model to be integrated with the PRA, Task 11.

Estimated Period of Performance:

This task is expected to start in October 2007 and will be completed by December 2008.

Task 11

Integration of Reliability Models With PRA

Objective:

Integrate the digital system reliability model into the PRA.

- If a Markov model is developed for the Oconee RPS, its integration with a PRA requires that an integration method be developed.
- Develop guidance on when diverse systems can be considered independent (digital systems can be used at 4 different echelons of defense: control, protection, mitigation, and indications. Dependencies may exist between systems at different echelons, e.g., RPS and ATWS mitigation system).

Estimated Period of Performance:

This task is expected to start in October 2007 and will be completed by March 2009.

Task 12

Develop NUREG Report

Objective:

Prepare a NUREG report that documents all the tasks completed in this project.

Estimated Period of Performance:

This task is expected to start in October 2007 and will be completed by March 2009.



CURRENT STATE OF RELIABILITY MODELING METHODOLOGIES FOR DIGITAL SYSTEMS AND ACCEPTANCE CRITERIA FOR NUCLEAR POWER PLANT ASSESSMENTS

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 14, 2005

Steven A. Arndt

Engineering Research Application Branch
Division of Engineering Technology
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)



Background

- U.S. NRC policy encourages the use of PRA and associated analyses to the extent supported by the state-of-the-art
- ACRS issued a Letter Report in 1997 that recommended that the NRC staff develop methods for estimating failure probabilities in software-based digital systems, including commercial off-the-shelf (COTS) software and hardware
- The preferred method of evaluating a digital system is from a system stand point that requires 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

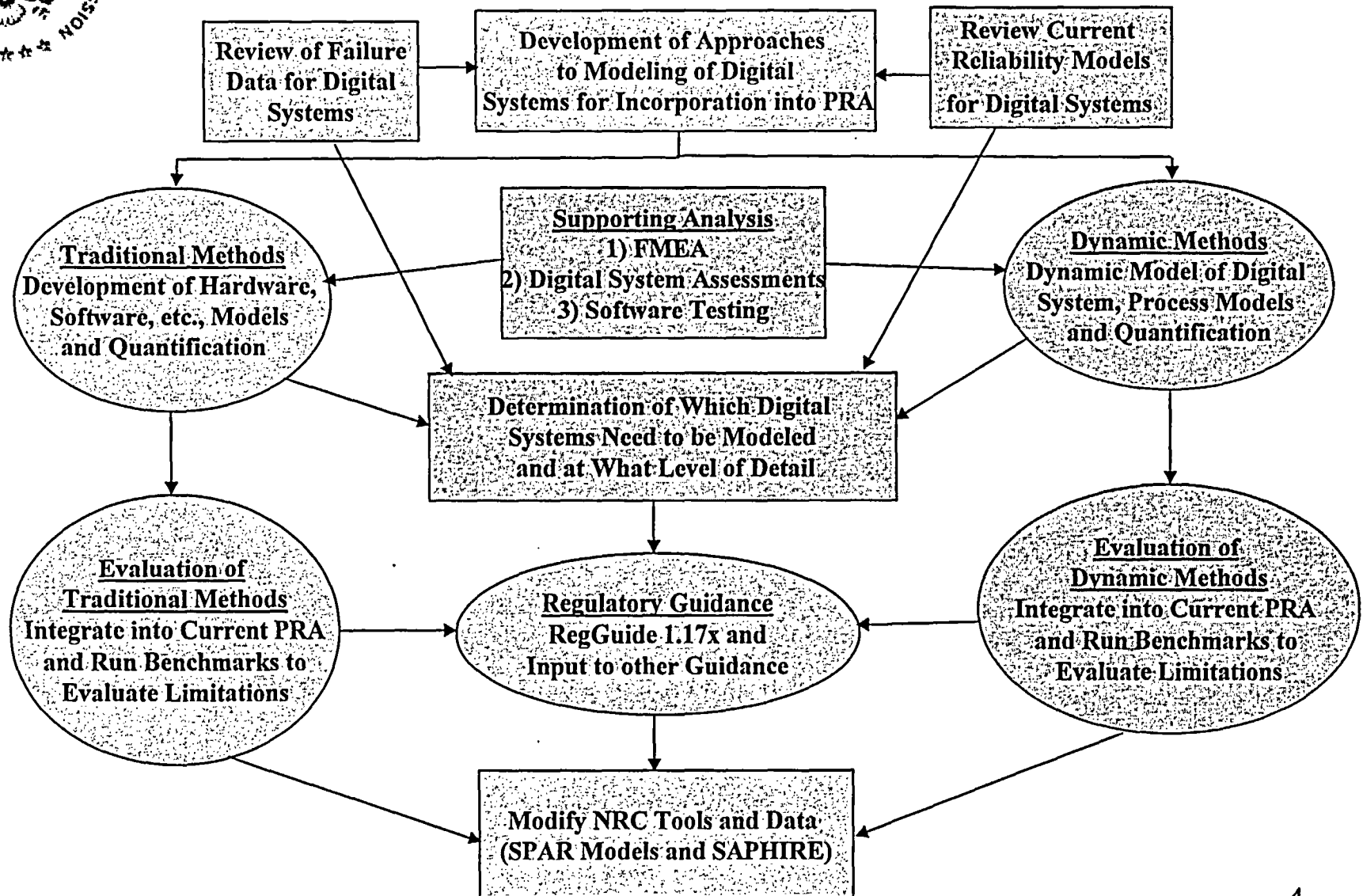


Background (Cont.)

- From a reliability modeling perspective, these conclusions imply that there may be a need to account for the dynamic interactions
 - between digital I&C systems and controlled/monitored plant physical processes (e.g., heatup, pressurization), and
 - within digital I&C systems (e.g., communication between different components, multi-tasking, multiplexing)
- Digital I&C system reliability models accounting for such effects need to be incorporated into the existing PRA to assess whether the Δ CDF due to proposed change in the I&C system vs. existing CDF will be acceptable according to RG 1.174 acceptance criteria



NRC Digital System Risk Program





Objectives

Develop both policies and methods for inclusion of reliability models for digital systems into current generation nuclear power plant PRAs, including

- a pilot study of the proposed methods,
- detailed reviews of the potential pitfalls of the methods developed, and
- detailed reviews of other methods when used to develop Δ CDF and LERF numbers needed to support risk informed regulation of nuclear power plant instrumentation and control criteria



Overall Approach

- Investigate the applicability of the current static event tree/fault tree (ET/FT) approach to digital I&C systems
- Review the advantages and limitations of available dynamic methodologies as they pertain to digital I&C systems relevant to reactor protection and control
- Review other industries for practices in the 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 overall minimum requirements a digital system model must meet for successful incorporation into an existing PRA
- Identify available methodologies that meet these requirements



Differences Between Analog and Digital I&C Systems

- The firmware and software components of digital I&C systems do not demonstrate any wear characteristics and do not respond to accelerated life testing, stress testing, etc.
- The firmware/software reliability cannot be accurately modeled using a bathtub curve approach
- There may be complex interactions between the constituents of the digital I&C system and between the digital I&C system and process physics which may lead to potentially significant dependencies between failures events:
 - Digital I&C systems rely on sequential circuits that have memory. Consequently, digital I&C system outputs may be a function of system history, as well as the rate of progress of the tasks.
 - Tasks may compete for a digital controller's resources which may lead to problems such as deadlock and starvation.
 - The choice of internal/external communication mechanisms for the digital I&C system (such as buses and networks) and the communication protocol affect the rate of data transfer.
 - Ability to coordinate multiple digital controllers directly and explicitly may necessitate a finer degree of communication and coordination between the controllers.
 - A digital controller can remain active and not only react to data, but can anticipate the state of the controlled/monitored system



Differences Between Analog and Digital I&C Systems (Cont.)

- The failure modes of digital I&C system are not well defined:
 - Errors in design and software implementation can cause the digital system to fail due to some specific input being received.
 - The system may fail not only on that specific input but also on other inputs that are semantically similar or even equivalent/correlated
- Software may be able to mask intermittent failures in hardware
 - A protocol for Ethernet is able to coordinate collision of packets transmitted when more than one node on the network attempts to transmit
- Digital I&C systems share data transmissions, functions, and process equipment to a greater degree than analog systems and hence may be more vulnerable to common cause failure



Differences Between Analog and Digital I&C Systems (Cont.)

- It is possible for digital I&C systems to introduce new initiating events:
 - Protocols may introduce dependencies between different systems such that system failures may introduce 'garbage' data as input to the other devices
 - Multi tasking may introduce new failure dependencies between systems.
- Software is not a physical entity and testing alone is not sufficient to verify that software is complete and correct
- Software defects may remain hidden for long periods after a product has been in general use and failures may occur without any advance warning when a particular execution path is exercised



Practices in Other Industries

- Most, if not all, approaches taken by the medical device, defense system, telecommunication industries and the aircraft industry (under the FAA) include software development process, management, and testing as their primary activities to manage digital system risk
- Only the spacecraft industry, under NASA guidance, appears to be moving to a true risk evaluation system using PRAs.
- The NASA guidelines identify
 - black box software reliability models exemplified by the Schneidewind model
 - semi-dynamic methodologies exemplified by the dynamic fault-tree and dynamic flowgraph methodologies.
- There has been NASA supported work using dynamic methodologies (e.g. space shuttle engine assessment).



Need for Dynamic Methodologies

- Dynamic interactions between the plant physical processes and triggered or stochastic logical events of reactor protection and control systems may lead to coupling between failure events
- Cases reported in the literature imply that the conventional ET/FT approach may yield conservative (but maybe overly conservative) results
- Omission of some failure scenarios is possible if dynamic interactions between the plant physical processes and triggered or stochastic logical events are not accounted for*
- Dynamic methodologies will only be needed for systems for which significant interactions are possible

*P. C. CACCIABUE, A. AMENDOLA, G. COJAZZI, "Dynamic Logical Analytical Methodology Versus Fault Tree: The Case Of Auxiliary Feedwater System of a Nuclear Power Plant", *Nucl. Technol.*, **74**, 195-208 (1986)

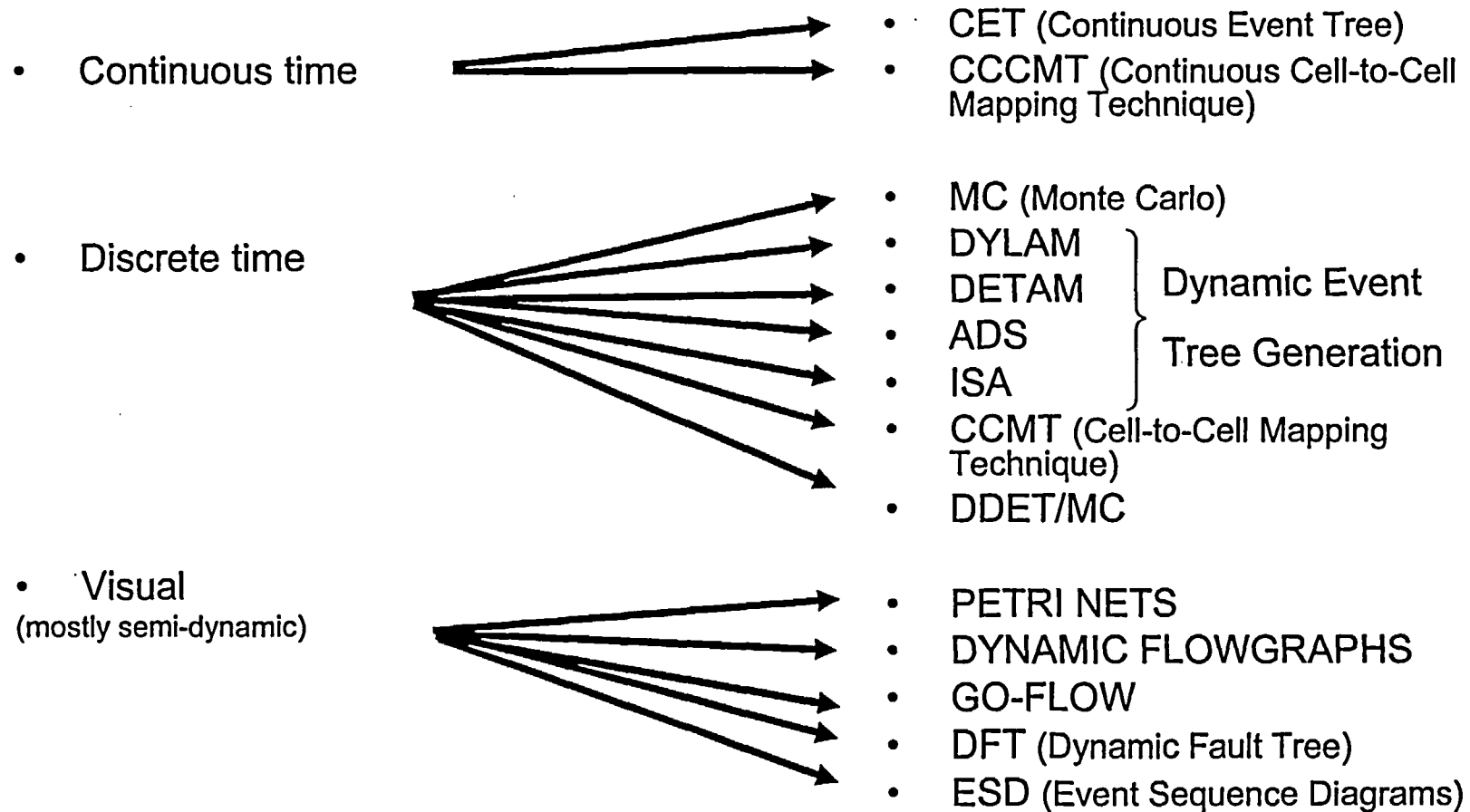


Review of Dynamic Methodologies

- Two types of dynamic interactions need to be accounted for in the reliability modeling of digital reactor protection and control systems:
 - Interaction between the reactor protection and control system and controlled/monitored plant physical processes such as heatup and pressurization of the reactor and level control (Type I interactions)
 - Interaction between the constituents of the reactor protection and control system itself, such as communication between different components, multi-tasking, multiplexing (Type II interactions)
- From a reliability modeling viewpoint, Type I and Type II interactions are separable only for single-input, single-output I&C systems
- Generally it is difficult to integrate a dynamic model into existing plant PRAs, almost all of which are based on the ET/FT approach



Dynamic Methodologies for Type I Interactions





Evaluation of Dynamic/Semi-Dynamic Methodologies

Issue/ Method	Accuracy in the Representation of System Dynamics	Ease of Probabilistic Model Construction	Desirability of Computational Features for Quantification	Compatibility with Existing PRAs
CET	10	5	1	1
CCCM	7	1	3	3
DYLAM	10	7	5	9
DETAM	10	7	5	9
DDET	10	7	5	9
ADS	10	7	5	9
MC	10	6	1	1
DDET/MC	10	6	6	9
ISA	10	7	7	9
CCMT	7	7	3	3
PN	3	5	7	8
DFM	3	5	7	7
ESD	10	4	5	8
GO-FLOW	3	7	8	7

1: Worst – 10: Best



Dynamic Methodologies for Type II Interactions

- Markov models (Johnson)
- Bayesian methodologies (Golay)
- Dynamic flowgraph methodology
- Petri nets
- Test based approaches
- Software metric-based approach
- Black-box models (Schneidewind)



Evaluation of Available Methodologies and Desirable Model Features

Requirements

1. The model must be able to predict future failures well.
2. The model must account for the relevant features of the system under consideration.
3. The model must make valid and plausible assumptions.
4. The model must be able to represent dependencies between failure events accurately and quantitatively
5. The model must be designed so it is not hard for an analyst to learn the concepts and is not hard to implement.
6. The data used in the quantification process must be credible to a significant portion of the technical community.



Evaluation of Available Methodologies and Desirable Model Features

Requirements

7. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones.
8. The model must be able to differentiate between faults that cause function failures and intermittent failures.
9. The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results.
10. The methodology must be able to model the digital I&C system portions of accident scenarios to such a level of detail and completeness that non-digital I&C system portions of the scenario can be properly analyzed and practical decisions can be formulated and analyzed
11. The model should not require highly time-dependent or continuous plant state information.



Evaluation of Available Methodologies and Desirable Model Features

Requirement/ Methodology	1	2	3	4	5	6	7	8	9	10	11
Continuous Event Trees [59]	X	X	X	X	O	?	?	X	?	?	O
Dynamic Event Trees [61,62, 63,64,65, 67]	X	X	X	?	X	?	?	?	X	X	O
Markov Models [30, 60, 68]	X	X	X	X	O	?	X	X	?	?	O
Monte Carlo Simulation [66]	X	X	X	X	?	?	?	?	?	?	O
Petri Nets [45, 46, 47, 69, 70]	X	X	X	X	O	?	?	?	?	?	O
DFM [14, 57]	X	X	X	?	X	?	?	?	X	X	X
Dynamic Fault Trees [71, 72]	X	?	?	?	X	?	X	?	X	?	X
ESD [73]	X	X	X	X	O	?	?	?	X	X	O
GO-FLOW [74,3]	X	?	X	?	O	?	?	?	X	X	X
Bayesian Methodologies [43, 44]	X	?	?	?	O	O	?	?	?	?	X
Test Based Approaches [51]	?	?	X	O	X	?	X	X	?	O	X
Software Metric Based Approaches [52]	O	?	O	O	?	?	X	X	O	O	X
Schneidewind Model [34,53]	X	?	?	?	?	?	?	?	O	O	X

X: Fulfills requirement

O: Does not fulfill requirement

? Needs further study to determine whether or not the methodology fulfills the requirement



Available Methodologies According to Desirable Model Features

- Dynamic flowgraph methodology
- Markov approach or dynamic event tree construction
- Event sequence diagrams
- Petri nets or GO-FLOW
- Monte Carlo simulation



Minimum Acceptance Criteria for Methodologies from a Regulatory Viewpoint

- **The model must be able to quantitatively represent dependencies between failure events accurately, including common cause failures, those arising due to interaction of the digital I&C systems with the controlled process (Type II interactions) and within the digital I&C systems (Type I interactions)**
- **The model should not require highly time-dependent or continuous plant state information**
- **The model must be able to predict future failures well and cannot be purely based on previous experience**
- **The model must make valid and plausible assumptions and the consequences of violating these assumptions need to be identified**

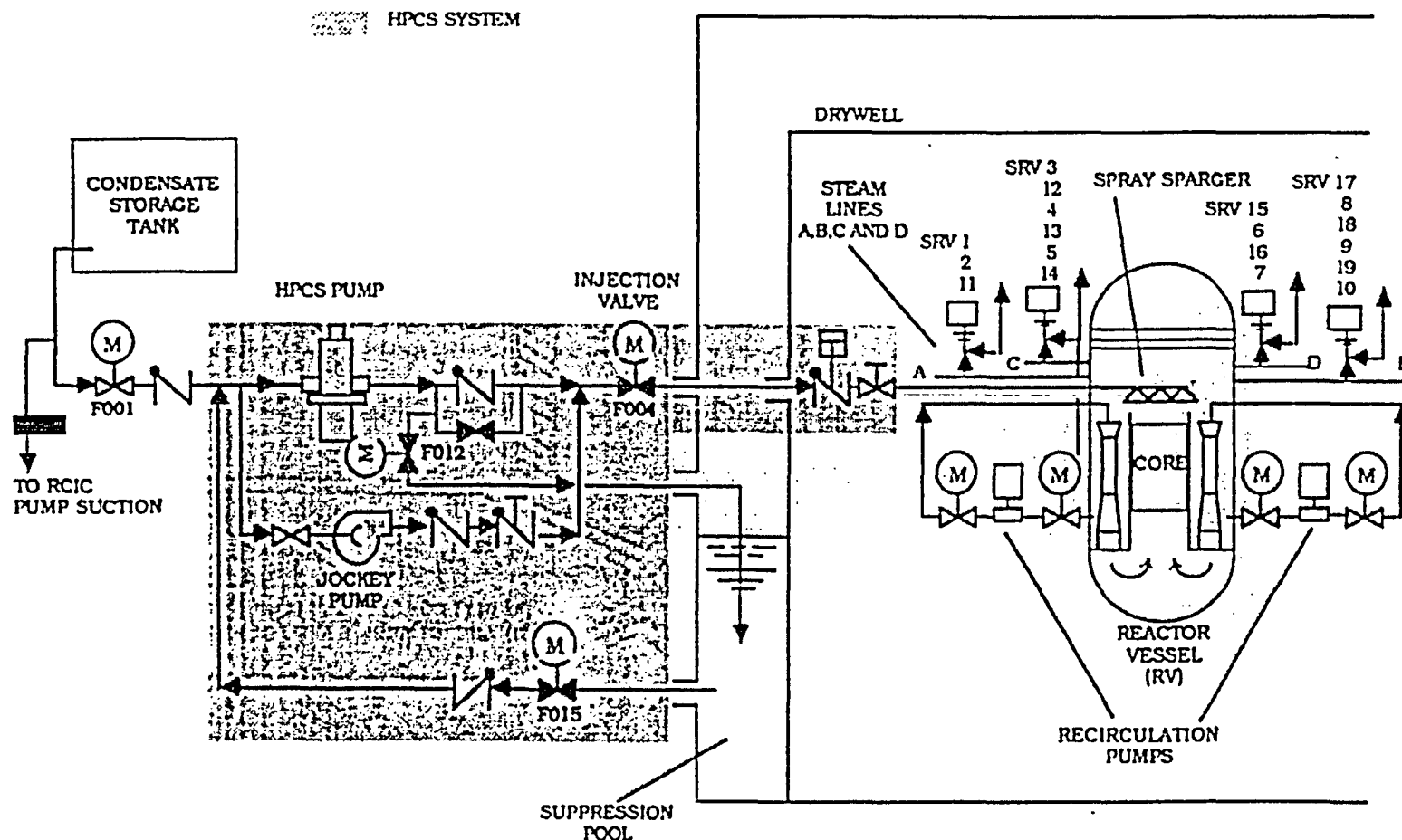


Minimum Acceptance Criteria for Methodologies from a Regulatory Viewpoint (Cont.)

- **The data used in the quantification process must be credible to a significant portion of the technical community**
- **The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones**
- **The model must be able to differentiate between faults that cause function failures and intermittent failures**
- **The model must have the ability to provide uncertainties associated with the results**

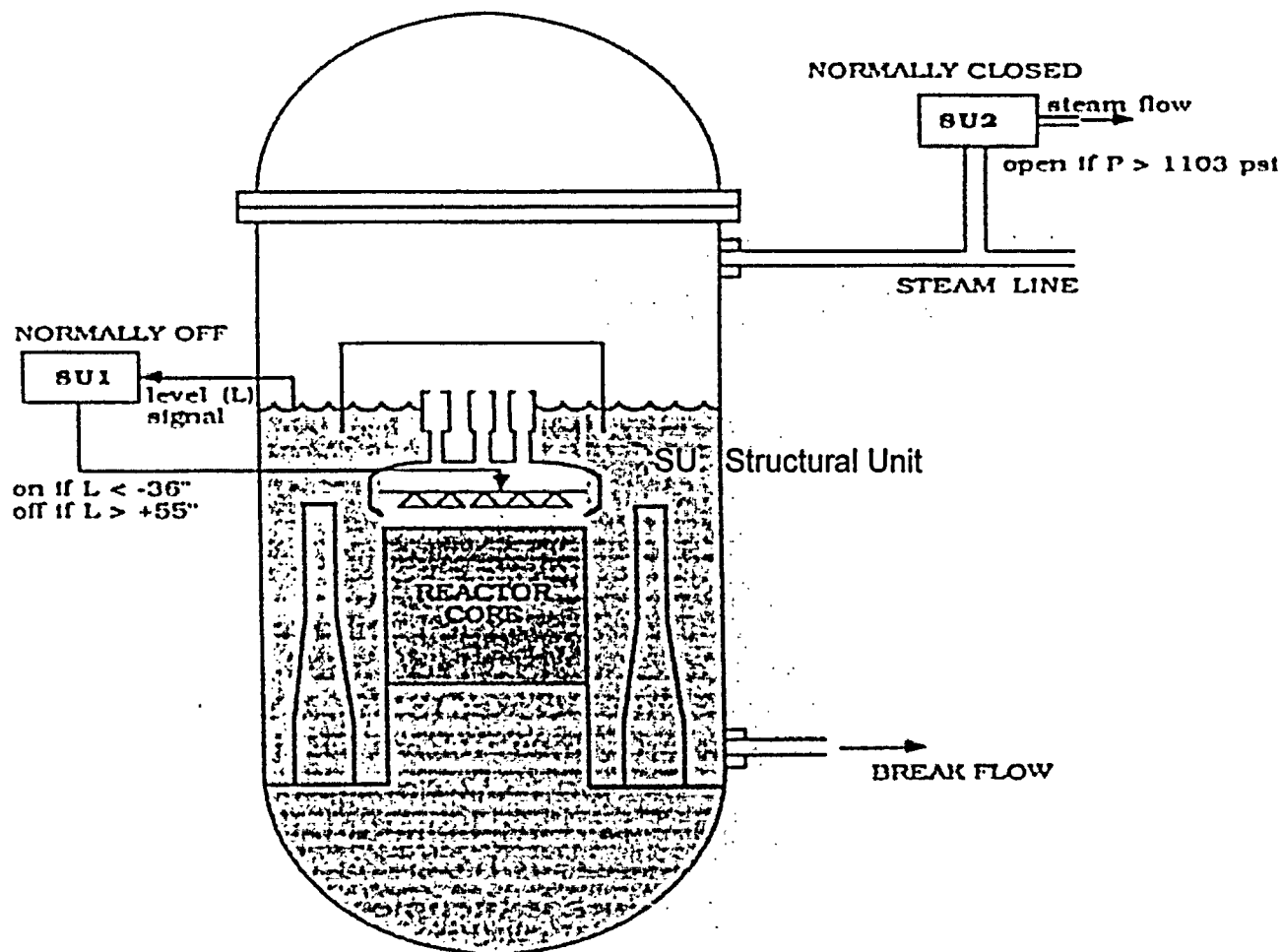


Example for Type I Effects: Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System





Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System: Modularized System





Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System: Example Initiating Event and Assumptions

- 1% double-ended guillotine break
- Pressure reaches 1039.4 psi within 2 minutes following the LOCA
- Level reaches 36.0 in within 2 minutes following the LOCA
- Major contributor to SU 1 failure is injection valve



Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System: Competition Between Top Events*

- Low level (< -148 in) occurs if only SU1 fails-off or only SU2 fails-open
- High level ($> +60$ in) occurs if SU2 fails-closed after SU1 fails-off
- High pressure (> 1110 psi) occurs if the level at the time SU2 fail-closed is such that it takes longer for the level to reach -148 in than the time it takes pressure to reach 1110 psi
- Low level occurs if the level at the time SU2 fail-closed is such that it reaches -148 in before pressure reach 1110 psi
- High level occurs if the level at the time SU2 fails-closed is such that the level reaches $+60$ in before pressure reaches 1110 psi

*M. Hassan, T. Aldemir, "A Data Base Oriented Dynamic Methodology for the Failure Analysis of Closed Loop Control Systems in Process Plants", *Reliab. Engng & System Safety*, 27, 275-322 (February 1990)



Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System: Some Significant Findings*

- The competition between the Top Events does not just depend on the order of SU failure but exact timing of the failure and/or exact magnitudes of the pressure and level at the time of the failure
- ET/FT overestimates low pressure probability by a factor of 3**
- ET/FT overestimates low level probability by a factor of 2**
- ET/FT results for high level and high pressure are close to dynamic methodology results*

**ET/FT results assume the demand on SU1 is 3/h and demand on SU2 is and 30/h

*M. Hassan, T. Aldemir, "A Data Base Oriented Dynamic Methodology for the Failure Analysis of Closed Loop Control Systems in Process Plants", *Reliab.Engng & System Safety*, 27, 275-322 (February 1990)



Conclusions

- **No single available methodology satisfies all the requirements**
- **It is not clear that the data used in the quantification process would be credible to a significant portion of the technical community for any methodology**
- **While DFM ranks as the most promising methodology, it is not clear that it can quantitatively represent dependencies between failure events accurately for all digital I&C systems**
- **An alternative methodology is the Markov approach**



Conclusions (Cont.)

- Scant computational evidence in the literature on dynamic systems seems to indicate that the ET/FT approach yields satisfactory results when a system:
 - has a single failure mode, or,
 - does not have logic loops*, and/or,
 - substantial time delay (with respect to system time constants) between the initiation of the fault and system failure
- Extrapolated to digital I&C systems, existing computational evidence on dynamic systems would indicate that the ET/FT approach may yield satisfactory results when a digital I&C system does not:
 - interact with a process that has multiple Top Events, logic loops* and or substantial time delays between the initiation of the fault and Top Event occurrence,
 - rely on sequential circuits which have memory,
 - have tasks that compete for the I&C system resources, and,
 - anticipate the future states of controlled/monitored processes.

*It may be possible to model logic loops using digraphs for fault-tree construction



Next Steps

- **Two benchmark problems will be defined that respectively capture important features of the existing analog I&C systems and their digital counterparts expected to be encountered in applications**
- **The benchmark problems will be used to compare DFM and the Markov approach with a common set of failure data**
- **If the result of the benchmark study indicates that DFM performs satisfactorily on the benchmark problems, then the impact of analog to digital I&C conversion will be investigated on a full PRA using SAPHIRE**
- **A study will be initiated as to how Markov model outputs can be utilized in a mechanical fashion to provide compatible input to SAPHIRE**
- **Alternatively, the feasibility of developing a dynamic methodology on the SAPHIRE platform may be investigated**