

NUCLEAR REGULATORY COMMISSION

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

Docket Number: Not provided

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

Location: Rockville, Maryland

Date: Tuesday, June 27, 2006

Work Order No.: NRC-1109

Pages 1-296

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

TROY

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

DISCLAIMER

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

June 27, 2006

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on June 27, 2006, 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 NUCLEAR REGULATORY COMMISSION

2 + + + + +

3 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

4 + + + + +

5 MEETING OF THE SUBCOMMITTEE ON DIGITAL

6 INSTRUMENTATION AND CONTROL SYSTEMS

7 + + + + +

8 TUESDAY,

9 JUNE 27, 2006

10
11 The subcommittee meeting convened at the Nuclear
12 Regulatory Commission, Two White Flint North, Room T-
13 2B3, 11545 Rockville Pike, Rockville, Maryland, at
14 8:30 a.m., George E. Apostolakis, Chair, presiding.

15
16 SUBCOMMITTEE MEMBERS PRESENT:

- 17 GEORGE E. APOSTOLAKIS Chair
- 18 MARIO BONACA ACRS Member
- 19 THOMAS S. KRESS ACRS Member
- 20 JOHN H. HICKEL ACRS Consultant

21
22 ACRS STAFF PRESENT:

23 ERIC A. THORNSBURY

24
25
NEAL R. GROSS
COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 NRR STAFF PRESENT:

2 STEVEN ARNDT RES/DFERR

3 TODD HILSMEIER RES/DRASP

4 BILL KEMPER RES/DFERR/IEEB

5

6 ALSO PRESENT:

7 TUNC ALDEMIR Ohio State University

8 TSONG-LUN CHU Brookhaven

9 CARL ELKS UVA

10 BOB ENZINNA AREVA

11 JEFF GAERTNER EPRI

12 TONY HARRIS NEI

13 ALEX MARION NEI

14 GERARDO MARTINEZ-GURIDI

15 Brookhaven

16 THUY NGUYEN EPRI/EDF

17 JEFF STONE Constellation Energy

18 MICHAEL YAU ASCA, Inc.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

A G E N D A

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

Opening Remarks and Objectives 5

G. Apostolakis, ACRS

Introduction and Overview of Digital
System Risk Research Program 8

S. Arndt, RES

Development of Probabilistic Approach for Modeling
Failures of Digital Systems using Dynamic Methods
. 22

S. Arndt, RES

T. Aldemir, OSU

Lunch Break 145

Development of a Probabilistic Approach for Modeling
Failures of Digital Systems using Traditional PRA
Methods 150

T. Hilsmeier, RES

T. Chu, BNL

Break 217

1 Development of Regulatory Guidance for
2 Risk-Informing Digital Systems Reviews 256
3 S. Arndt, RES
4
5 Comments by Industry 286
6 T. Harris, NEI
7
8 Adjourn 296

7.

7.

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

(202) 234-4433

www.nealrgross.com

P R O C E E D I N G S

(8:33:29 a.m.)

CHAIR APOSTOLAKIS: The meeting will now come to order. This is a meeting of the Advisory Committee on Reactor Safeguards, Subcommittee on Digital Instrumentation and Control Systems. I am George Apostolakis, Chairman of the Subcommittee. Members in attendance are Mario Bonaca and Tom Kress. Also in attendance is one of our consultants, Dr. John Hickel. The purpose of this meeting is to review the ongoing digital system risk program, and the development of a regulatory guide on risk-informed digital system reviews. The subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the Full Committee. Eric Thornsbury is the Designated Federal Official for this meeting.

The rules for participating in today's meeting have been announced as part of the notice of this meeting previously published in the *Federal Register* on May 25, 2006. A transcript of the meeting is being kept, and will be made available as stated in the *Federal Register* notice. It is requested that speakers first identify themselves and speak with

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

(202) 234-4433

www.nealrgross.com

1 sufficient clarity and volume so that it can be
2 readily heard.

3 We have received no written comments from
4 members of the public regarding today's meeting.
5 Representatives from industry have requested time to
6 make an oral statement, which we will hear at the end
7 of the meeting. We will now proceed with the meeting,
8 and I call upon Mr. Bill Kemper from the Office of
9 Nuclear Regulatory Research to begin the
10 presentations.

11 MR. KEMPER: Thank you, George. Good
12 morning. My name is Bill Kemper. I'm the Branch
13 Chief of the Instrumentation and Electrical
14 Engineering Branch in the Office of Research. We're
15 here today to provide an update to the ACRS INC
16 Subcommittee on a research program that will provide
17 modeling methods, tools, data, and regulatory guidance
18 by which the Agency can review and improve risk-
19 informed license applications for digital safety
20 systems in nuclear power plants.

21 Currently, digital safety systems license
22 applications for digital safety systems are reviewed
23 and approved using deterministic methods in accordance
24 with Chapter 7 of the Standard Review Plan. Now this
25 research program will enable the Agency to also assess

NEAL R. GROSS

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

1 the contribution of these systems to plant risk during
2 the licensing process.

3 Steve Arndt, who works in the INC Group,
4 the Office of Research, will take the lead for today's
5 presentations. He's the Project Manager for this
6 project. Also, Todd Hilsmeier, to my right here, is
7 working with Steve. He's from our PRA Branch in the
8 Office of Research, and he is also managing a part of
9 this project, as well.

10 They are supported today by staff members
11 from several of our contract organizations. We have
12 folks here from Ohio State University, Tunc Aldemir,
13 and we also have folks here from Brookhaven National
14 Lab, and that would be Louis Chu and Gerardo Martinez.
15 Excuse me. I hope I pronounced that properly. And
16 have I left out anybody else? Is there anybody else
17 here that we want to introduce? Carl Elks is from the
18 University of Virginia, and Michael, who have
19 developed a part of the research program that we're
20 going to use in developing this risk-informed approach
21 here. So we have a lot of material to discuss today,
22 and we really look forward to your insights and
23 feedback on this information.

24 This research project involves the
25 application of modeling methods for digital safety

NEAL R. GROSS

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

1 systems that are relatively new, or at least not used
2 within the nuclear industry at this time, so your
3 advice and counsel would be greatly appreciated during
4 these discussions. I see we have a lot of folks in
5 the room, so there appears to be a lot of interest in
6 this process from others, as well, so look forward to
7 any input that our stakeholders may have, as well. So
8 with that, I'll turn it over to Steve to begin the
9 presentations.

10 MR. ARNDT: Thank you, Bill. As you can
11 see from the schedule today, we have a number of
12 different presentations, and I'm going to try and get
13 through the introduction quite quickly so we have time
14 for the technical discussions. We're going to go
15 through a lot of different areas. If the members or
16 the Chair would like us to concentrate on certain
17 areas and move more quickly on others, please just let
18 me know, and I'll facilitate that. I'd like to keep
19 the meeting as informal as possible, free exchange of
20 information.

21 For those members who might need a little
22 refreshing and John, who I don't think has seen this
23 before, I have a few slides just to introduce the
24 research. As Bill mentioned, the research is intended
25 to investigate potential procedures and methods for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 including reliability models in digital systems in
2 current generation PRAs, develop these methods to the
3 point they can be integrated into agency tools, and
4 developed with necessary regulatory guidance,
5 including understanding what the methods are, and
6 which methods are most usable for this particular
7 purpose, because there are a lot of different digital
8 system modeling methods out there, determine which of
9 these systems need to be modeled in terms of digital
10 systems, how detailed a model, what level of modeling
11 you need to actually put into the PRA, develop and
12 test the methods for realistic applications, and then
13 develop acceptable regulatory guidance associated with
14 that.

15 CHAIR APOSTOLAKIS: Are you going to
16 address the second sub-bullet today?

17 MR. ARNDT: We're going to talk about it
18 a little bit.

19 CHAIR APOSTOLAKIS: Is this what we
20 discussed in the past, the classification of the
21 systems and so on?

22 MR. ARNDT: It's part of the
23 classification. There are several different crossing
24 classification issues, but one of them is the
25 complexity of the system, and how that dictates both

NEAL R. GROSS

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

1 the kinds of modeling methods you need to adequately
2 address them, and what level of integration into the
3 PRA you need. There's other ways of classifying it,
4 depending on other things, but we're going to talk
5 about that a little. That's one the sticking points,
6 and we're challenging parts of this, but we will talk
7 about that at some level. If you have additional
8 questions as it goes forward, please let us know.

9 Issues facing the NRC - we've been talking
10 about this for a number of years. The licensees are
11 replacing analog systems. The industry has expressed
12 interest in risk-informed methods, similar to those
13 laid out in Reg Guide 1.174 as an alternate method for
14 licensing these systems. However, the research into
15 how to do this does not currently support this
16 application, which is the reason why we have a
17 research program.

18 In addition, we're starting to run into
19 situations where other risk applications are being
20 limited or could potentially be limited because the
21 general PRA does not model these systems. As we start
22 doing more tech spec updates, et cetera, et cetera,
23 we're having to exclude digital systems from that
24 piece of those applications because we don't have
25 adequate models. And, of course, the agency analysis

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 methods do not at present private any independent
2 means to support that, so we'll talk a little bit
3 about how we're going to, if the research is
4 successful, integrate these in with the current NRC
5 tools.

6 CHAIR APOSTOLAKIS: Is the industry
7 developing methods along these lines?

8 MR. ARNDT: Yes. And the industry - I
9 think we talked the last time - has proposed a
10 methodology that we're looking at.

11 CHAIR APOSTOLAKIS: Oh, yes.

12 MR. ARNDT: Other industries, like the
13 aviation and space, have proposed methodologies, as
14 well. There are some advantages and disadvantages
15 associated with those.

16 At our subcommittee meeting in June, the
17 ACRS Subcommittee specifically asked that they be
18 consulted as the program progresses, and that's
19 specifically what the purpose of this meeting is. We
20 have some intermediary products. We've shared some of
21 the drafts with the committee, but this is primarily
22 a progress reporting meeting. We've made some
23 progress, and we want to tell you where we are, get
24 your feedback, get your input on that.

25 The committee encouraged the review of

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

1 software-induced failures, and we're going to hear
2 about that today. The committee encouraged critical
3 review of various methods, and we've published some
4 research in that area looking at various methods and
5 what we consider to be the most effective. And the
6 committee also encouraged the staff to view digital
7 systems from a systems standpoint, while acknowledging
8 that there may be some applications that that's not
9 necessary. And we'll talk about that, as well.

10 So we're looking at a number of different
11 areas. It's a rather large and complex program, as
12 you might have guessed from Bill's list of people that
13 are working on it. We'll talk a little bit about how
14 all the pieces fit together. We're basically looking
15 at the various methodologies and developing some
16 benchmarks to assess the relative capabilities and
17 limitations of the different methodologies, at the
18 same time informing our development of a regulatory
19 guidance. We'll talk a little bit about the status of
20 the development of the regulatory guidance at the end
21 of the day. That's basically a preliminary issue. We
22 will, of course, bring the draft regulatory guidance
23 to the Committee before issuing it for public comment,
24 so we're at the early stage of that development right
25 now.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIR APOSTOLAKIS: When is this going to
2 happen, Steve, in the fall?

3 MR. ARNDT: Yes. I have a draft schedule
4 in that presentation.

5 CHAIR APOSTOLAKIS: Okay.

6 MR. ARNDT: But one of the things we want
7 to do is get both stakeholder, and ACRS, and industry
8 input into that, so this is your opportunity to give
9 us some general ideas, are we going down the right
10 path. We're also going to probably have a public
11 meeting in August to get stakeholder input to make
12 sure that the conclusions we're reaching are
13 reasonable and appropriate.

14 CHAIR APOSTOLAKIS: Is this the first time
15 today that you will present this to the public, the
16 regulatory guide?

17 MR. ARNDT: Yes. It's just first thoughts
18 on the regulatory --

19 CHAIR APOSTOLAKIS: The ideas, yes.

20 MR. ARNDT: The ideas.

21 CHAIR APOSTOLAKIS: But this is the first
22 time.

23 MR. ARNDT: The first time, yes. Most of
24 you have seen this diagram. John I don't think has.
25 This is just a structural diagram of how all the

NEAL R. GROSS

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

1 pieces fit in our program. I'll go through it very
2 quickly.

3 This first part is basically developing an
4 approach, come up with an idea of how to do it.
5 Supporting that is the review of the failure data,
6 which was encouraged by the Committee, and the review
7 of the current reliability methods, which we talked
8 about in NUREG 69.01.

9 Supporting the development of the actual
10 analysis is the supporting analysis, understanding how
11 the system works, the failure most effects analysis,
12 the digital system testing, and various other things,
13 and the critical element that a lot of different
14 elements are feeding into, the determination of what
15 systems need to be modeled and at what level. This is
16 an ongoing challenging part.

17 Now this path is a review and evaluation
18 of dynamic methods. This path is review of
19 traditional methods, fault trees, event trees, and
20 supporting methodologies. The idea here it look at
21 both methodologies critically and understand what
22 systems can be modeled at what level using what
23 methodologies, and what assumptions you have to make,
24 and what limitations you have to make in those
25 analyses. All of those will feed into the regulatory

NEAL R. GROSS

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

1 guidance, which we are currently developing, and the
2 development of the supporting tools for the staff.

3 CHAIR APOSTOLAKIS: Isn't the box on the
4 upper left corner, the failure data, one of the most
5 critical activities here? I mean, why doesn't it fit
6 into both the traditional methods and the dynamic
7 methods?

8 MR. ARNDT: It does. There's only so many
9 arrows I can put on my chart. It's a critical element
10 for a number of reasons. One, understanding and
11 assessing what data is out there, what the data spread
12 is in issues like that. Also, understanding how you
13 augment available operational history with other
14 information, like testing data and things like that,
15 is a critical part of all of this. It's a critical
16 part of the traditional methods, the dynamic methods,
17 as well as the determination of what modeling methods
18 you --

19 CHAIR APOSTOLAKIS: But in reading the
20 reports and data and dynamic methods, one gets, at
21 least the way they are now, one gets the impression
22 that these two groups have not communicated, because
23 the data that are -- date, I mean the numbers that are
24 used, or the quantities that are used in the dynamic
25 method report really have nothing to do with the

NEAL R. GROSS

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

1 findings of the failure data report. So at which
2 point is there going to be some integration?

3 MR. ARNDT: Well, I take a little bit of
4 umbrage with^v nothing to do.

5 CHAIR APOSTOLAKIS: Epsilon, they have
6 epsilon to do. I mean, if you read the data report,
7 there's all sorts of things that have happened, and
8 this and that, then you go to the dynamic methods and
9 they say now, this is a transition rate, and precision
10 rate, and there is absolutely no reference to what is
11 out there. And I'm wondering -- you know, it's not --
12 maybe it's something that you intend to do in the
13 future. I don't know. I mean, this is work in
14 progress.

15 MR. ARNDT: It is work in progress, and we
16 do intend to increase the review of these issues,
17 because it's a critical issue. But I think when we
18 review that piece of it today, you'll see that we are
19 including those issues, the operational history of the
20 system, the available failure information associated
21 with components and other things feed into both the
22 traditional methods and the dynamic methods. We may
23 not be articulating it as well as we could in the
24 report, and we certainly want to continue to have
25 cross-fertilization. But yes, I take your point.

NEAL R. GROSS

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

1 As we have discussed, we're structured for
2 three major outcomes; basically, the determination of
3 what needs to be modeled at what level and what
4 accuracy, the development of an independent modeling
5 capability, and development of acceptable criteria for
6 risk approaches.

7 So in summary, what we're looking forward
8 to getting from the ACRS is the review of our
9 progress, advice on the best methods, such as what
10 Professor Apostolakis has just given, meaning the
11 discussion we just had, eventual review and
12 endorsement of the proposed methodologies, and
13 eventual review and endorsement of the regulatory
14 guidance. That will be probably this fall or early
15 winter.

16 CHAIR APOSTOLAKIS: I think, Steve, the
17 middle box there, "Determination of which data systems
18 need to be modeled, at what level of detail", is a
19 critical one, as you know. And you should give it
20 more prominence, in my view. Again, in reading the
21 reports as they are today, one gets the impression
22 again that, for example, the dynamic methods, this it
23 is. We are proposing this, we're going to apply it
24 everywhere. Then you read the Brookhaven report, it's
25 something else.

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 Maybe there ought to be -- I mean, I
2 understand that this is something that you cannot
3 finish now before you do other things, but maybe if
4 you have a skeleton of it, and everybody refers to
5 that, and everybody understands that this thing is
6 going to evolve as we progress, I think that will go
7 a long way towards pacifying some people, because I
8 mean, admittedly what is in this dynamic thing is
9 fairly complex. And you're scratching your head,
10 saying well, do I have to do this for actuation
11 systems, for example. And there is nowhere there
12 something that says hey, this is for a class of
13 systems that have these problems or these
14 characteristics, and I think that would be -- I mean,
15 I appreciate that it's something that you cannot
16 finalize now, but having some sort of a skeleton -
17 based on what we know, this is the way we're going,
18 and this is where this method applies.

19 MR. ARNDT: Yes. At the risk of getting
20 ahead of myself, because we're going to talk a little
21 bit about this later in the day, what we're looking at
22 right now, and again, this is preliminary results, we
23 haven't gotten the Reg Guide ready for prime time yet.

24 CHAIR APOSTOLAKIS: I know. That's why
25 we're here. I mean, I fully agree it's not --

NEAL R. GROSS

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

1 MR. ARNDT: But the concept is there's
2 going to be a set of characteristics, performance
3 characteristics, if you will, that will lead us to
4 particular modeling requirements that will lead us to
5 - or the industry if they choose to go down this path
6 - modeling capabilities for certain systems, some will
7 have relatively simplistic modeling methodology, some
8 will have an appropriate uncertainty analysis and data
9 requirements, et cetera; some will have a higher level
10 of detail, and some will have a still higher level of
11 detail. That then becomes both a regulatory concern
12 for us, how good does it have to be for which
13 application, and then an economic concern for the
14 industry, what do they want to do? So that's
15 basically the idea.

16 CHAIR APOSTOLAKIS: No, I know, but all
17 I'm saying is, maybe you can give us some idea where
18 you're going at this point, without waiting to be
19 ready for prime time.

20 MR. ARNDT: Okay.

21 CHAIR APOSTOLAKIS: It's okay. I mean, I
22 understand these things, and we all understand that
23 these things are evolving. John, do you want to say
24 something?

25 MR. HICKEL: Well, I think I tried to ask

NEAL R. GROSS

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

1 Steve this maybe before, but one thing is this -- it's
2 a split between how much resource do you devote to
3 things like trip and actuation systems, versus
4 emergency diesel load sequencers, versus normal
5 process controls?

6 If I knew what -- do you have a proposed
7 split as to how much attention you're going to put in
8 this area versus that, or is that too preliminary?

9 MR. ARNDT: Well, there is a couple of
10 different ways to answer that question. In terms of
11 attention from a research standpoint, we know certain
12 things, and we don't know certain things, and we know
13 things at various levels, so we put the most attention
14 to the things we know least about so we can get a
15 level of understanding that's appropriate.

16 In terms of regulatory side, and I'm not
17 on the regulatory side, but some of my colleagues are
18 here, the issue is, you want to put the most
19 importance on those things that have the biggest
20 potential for risk to the health and safety of the
21 public, because that's our business. So it's a little
22 bit -- I'm not quite sure what you're getting at by
23 the question.

24 MEMBER KRESS: It looks like a good place
25 for using risk importance measures.

NEAL R. GROSS

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

1 MR. ARNDT: Yes.

2 MEMBER KRESS: You could do that, even
3 though you don't know the failure rate, you can do a
4 risk importance.

5 CHAIR APOSTOLAKIS: At the system level.

6 MR. ARNDT: At the system level, yes.

7 MEMBER KRESS: Yes.

8 MR. ARNDT: Both how important the system
9 is, and how complicated it is, and how important it is
10 to get it right, and/or not miss things is part of the
11 criteria associated with what you're going to do.

12 MR. KEMPER: This is Bill Kemper. If I
13 could just throw something in here. We're going to
14 talk more about during this presentation of a couple
15 of benchmark exercises that we're going to do. We
16 intend to model the digital feedwater system from a
17 current operating nuclear power plant, as well as the
18 reactor protection system, and engineer safety feature
19 system. So we hope by performing a couple of case
20 studies, if you will, and benchmark examples, we'll be
21 able to provide some guidance along the lines of what
22 you're asking here, George.

23 CHAIR APOSTOLAKIS: Yes. Don't
24 misunderstand my comment. I know that you guys have
25 been thinking about it. It's just that I think you

NEAL R. GROSS

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

1 should give it more prominence even now, so the reader
2 will know that we are exploring this area, these kinds
3 of systems, and put it up front in bold face because
4 if you read some of this stuff now and you stop and
5 think what are we trying to do here, you really don't
6 have that help from you. That's all I'm saying.

7 MR. KEMPER: Good comment.

8 CHAIR APOSTOLAKIS: Okay. Who's next?

9 MR. ARNDT: Okay, if you look at your
10 agenda --

11 CHAIR APOSTOLAKIS: It says Arndt and
12 Aldemir.

13 MR. ARNDT: Yes. What we're now going to
14 step through is some of the work on the dynamics, a
15 fairly lengthy presentation. Then we're going to talk
16 through some of the data issues, and some of the
17 traditional methodologies in the afternoon, and then
18 the early thoughts on the Reg Guide at the end.

19 CHAIR APOSTOLAKIS: Okay. So now we have
20 this big package. Right?

21 MR. ARNDT: Yes.

22 CHAIR APOSTOLAKIS: Okay. A lot of
23 slides.

24 MR. ARNDT: Joining me at the table is
25 Professor George Aldemir from Ohio State University.

NEAL R. GROSS

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

1 This presentation is, as you mentioned, a lot of
2 slides. We're going to go through a quick background
3 on why we're looking at dynamic methods, talk a little
4 bit about the first benchmark. As Bill just
5 mentioned, we're going to have a second benchmark.
6 The first benchmark is going to be a system that is
7 more likely to require the dynamic methods. The
8 second benchmark is going to be a system that's less
9 likely to require the dynamic methods. We'll talk a
10 little bit about what it entails. We'll talk a little
11 bit about data, which is obviously a very important
12 issue in this area. We'll talk about the example
13 model that we're going to use to integrate this
14 system, the two methodologies that are being proposed
15 as pilot methodologies for dynamic methods, dynamic
16 flow-graph methodology and Markov; a little bit about
17 if you do this methodology, how you integrate it into
18 a PRA, because the current fleet of PRAs are fault
19 tree/event tree systems, and have an acceptance
20 criteria that's based on Delta CDF or Delta LERF. You
21 need to get those integrated.

22 We'll talk a little bit about interfacing
23 with the current NRC PRA tool, SAPHIRE; procedures and
24 requirements for reliability modeling. Basically,
25 what we've learned in terms of what's necessary to do

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 this based on how far we've gotten on the benchmark so
2 far, and then conclusions to-date.

3 You mentioned, I'm trying to sit at the
4 head of this multi-technical research program, so this
5 is going to be focused in on the particular dynamic
6 methodologies, but part of the objective of this is
7 not only to develop the dynamic methodologies, but
8 also to understand where you need them and where you
9 don't need them, and what aspects can be modeled with
10 what kinds of systems, and what the limitations are.

11 CHAIR APOSTOLAKIS: Since you're talking
12 about an overview, I got a little confused when I read
13 the report, because in Chapter 2, there is a lot of
14 discussion in using the words Markov; for example,
15 2.4.4 says "Modular Markov chain modeling of the
16 DFWCS." And then much to my surprise, there's a whole
17 Chapter 4 on Markov analysis, so what is the -- I
18 mean, can you give me an overview - in Chapter 2 we
19 are doing this, in Chapter 3 we're doing that, and in
20 Chapter 4 we're doing that. I don't see how what you
21 have in Chapter 2 relates to Chapter 4.

22 MR. ARNDT: Okay. In that report, and I
23 apologize to the public. This is a draft report
24 that's not publicly available yet. In that report,
25 which is a report that will be published here in a few

NEAL R. GROSS

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

1 months, Chapter 2 talks about the system and how we
2 develop data for the system. In that analysis, we use
3 a system model to try to understand what data we need.
4 That system model is a Markov model, so in Chapter 2,
5 we're basically talking about our understanding of how
6 the system works, and based on that, what data we
7 need, and how we generate that data. That's one
8 application of Markov associated with trying to
9 understand the system.

10 CHAIR APOSTOLAKIS: I mean, since you have
11 a Chapter 3 on the dynamic flow-graph methodology,
12 shouldn't you be using that also to develop whatever
13 data they need?

14 MR. ARNDT: Yes, but the particular model
15 we're using for understanding the system just happens
16 to be a Markov model. It could have been a dynamic
17 flow-graph model, it could have been --

18 CHAIR APOSTOLAKIS: So this is not a
19 comparison of the methods then.

20 MR. ARNDT: No.

21 CHAIR APOSTOLAKIS: This is focusing on
22 the dynamic model.

23 MR. ARNDT: The chapter on the Markov --

24 CHAIR APOSTOLAKIS: Four.

25 CHAIR APOSTOLAKIS: Three and four are the

NEAL R. GROSS

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

1 two different dynamic methods. Chapter 2 is
2 understanding the system and developing the data
3 necessary for the system, how does it fail, what are
4 the failure modes. We just happened to use a Markov
5 model in that analysis of the system. It could have
6 been any state space model we wanted, we just happened
7 to use a Markov model.

8 CHAIR APOSTOLAKIS: The question is, I
9 mean, if you are producing data for information really
10 about the system in Chapter 2, it should address both
11 methodologies then. I mean, you're already biasing
12 the thing towards the Markov approach. Anyway, is
13 there going to be a presentation on Chapter 2?

14 MR. ARNDT: Yes.

15 CHAIR APOSTOLAKIS: Okay.

16 MR. ARNDT: Okay. As you mentioned, this
17 is a fairly long presentation. Some of it I will try
18 and skim through relatively quickly. Obviously, if
19 there are questions, we can do that, go into detail.
20 Some of it we'll try and talk about a little more
21 detail, but this is basically where we're going.

22 As we mentioned earlier, we're trying to
23 develop the models to support the NRC policy statement
24 that encourages expanded use of PRA in all areas
25 supported by the state-of-the-art and data. We're

NEAL R. GROSS

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

1 developing the various models. We're looking at it
2 from a number of different aspects, but particularly
3 from the system standpoint because that is the
4 preferable way to look at it, and we have been
5 encouraged to do that by this committee, by the
6 National Academy study, and others. However, for the
7 near term, we're going to have to - if we choose to
8 model in a dynamic way, we're going to have to find a
9 way to get back to PRA through some kind of
10 traditional PRA through event tree/fault tree-type
11 applications, so we're also looking at how you get
12 that information into a fault tree/event tree-type of
13 approach. And there's a number of ways out there, we
14 just chose one particular way which we think is
15 particularly encouraging.

16 We're looking at issues that in this part
17 of the project, the dynamic part, that might drive us
18 toward using dynamic methods. Particularly, dynamic
19 interactions between the system and the process that
20 it's involved with in case of a controller, in
21 particular, the physical processes associated with it,
22 as well as internal issues within the digital systems
23 that are either sequential or time-based, or things
24 like that. These we refer to, for convenience, as
25 Type 1 and Type 2 interactions. Some systems, as we

NEAL R. GROSS

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

1 mentioned earlier, will have relatively few Type 1
2 interactions. Actuation systems that just meet a
3 threshold and do a particular action, don't have a lot
4 of process feedback in them. Control systems have a
5 lot of process feedback in them. Depending upon the
6 complexity of the digital system, they may or may not
7 have a lot of Type 2-type interactions. If there's a
8 lot of communications between the different internal
9 systems, if there's data sharing, if there's multi-
10 tasking, there's a potential that there's going to be
11 a lot of interactions that will be sequence-dependent,
12 or time-dependent, and will need a more complicated
13 model.

14 For example, the Turkey Point generator
15 sequencer failure that occurred several years ago,
16 where the system was in diagnostics, and got a real
17 actuation signal, and failed to drop out. That is an
18 internal Type 2 sequential issue that you need to
19 address in some way for that kind of system, if you're
20 going to have a lot of diagnostics, or if you're going
21 to have a lot of fault checking, or if you have a
22 sequential logic that could have timing-dependent
23 failure modes.

24 CHAIR APOSTOLAKIS: To what extent are
25 these systems being used now in safety systems?

NEAL R. GROSS

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

1 MR. ARNDT: It depends on the plant,
2 depends on the particular safety system. There's not
3 been a - let me see if I can say this correctly -
4 there's not been a RPS or ESFAS update in a digital
5 system under the new regulations.

6 CHAIR APOSTOLAKIS: There has or has not?

7 MR. ARNDT: Has not.

8 CHAIR APOSTOLAKIS: Has not.

9 MR. ARNDT: There has been some safety
10 systems that have been upgraded with digital systems,
11 but they're not RPS or ESFAS.

12 CHAIR APOSTOLAKIS: And these are just
13 actuation systems, or there is feedback there, and
14 control?

15 MR. ARNDT: There are feedback systems,
16 simple control systems.

17 CHAIR APOSTOLAKIS: And the staff has
18 approved those? I guess they have.

19 MR. ARNDT: Using the deterministic rules.

20 MR. HICKEL: Hey, George, CE has been
21 running digital protection systems based on stored
22 computer software since 1978.

23 MR. KEMPER: Yes. This is Bill Kemper,
24 again. Yes, there are many digital applications out
25 there. The CPC Plant Protection System that he just

NEAL R. GROSS

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

1 mentioned, for example, is one that's been around for
2 a long time. There's currently digital devices being
3 put in place to replace other antiquated digital
4 systems under 50.59. Very few have been submitted to
5 the agency, though, for license amendment approval, if
6 you will. However, as you're well aware, the Oconee
7 application is really the first full-blown RPS and
8 ESFAS upgrade from analog to digital technology, so
9 that's what we're really dealing with at this point.
10 But as an example, for example, at Palo Verde, they
11 replaced their platform with an ADVENT 160, the
12 "Common Q" processor. Oconee has got, I
13 understanding, in their QB system, TELEPERM, so there
14 are examples of equipment installed out there, but
15 it's not on a very large scale yet. We're just kind
16 of at the beginning of that bow wave, if you will.

17 MR. ARNDT: And there's a significantly
18 larger fraction in the non-safety side.

19 CHAIR APOSTOLAKIS: Yes.

20 MR. ARNDT: Okay. Again, I'll briefly
21 talk about this. This is basically the chart I showed
22 before. This side is the dynamic part, which is what
23 we're going to talk about today, but it also has
24 interactions with these other supporting analysis;
25 particularly, of course, the determination of what

NEAL R. GROSS

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

1 systems need to be modeled.

2 So the objective is to develop procedures
3 and methods for incorporating these reliability
4 methods into a PRA, and what we're doing is we're
5 doing pilot studies, as Bill mentioned, to understand
6 if the proposed methods are capable of modeling the
7 systems adequately, and what are the limitations
8 associated with it. And then understand how you
9 integrate those into the current regulatory structure
10 for risk-informing systems that the NRC has, the 174,
11 Delta CDF and Delta LERF issues for INC, and also look
12 at other deterministic rules associated with that.

13 So this is basically just words associated
14 with what was in that bubble chart; investigate the
15 applicability of current methodologies, review the
16 limitations and advantages of dynamic methodologies,
17 review what other people have been doing, the
18 railroads, space, industry, NASA and other things,
19 review the existing regulatory framework, identify the
20 minimum set of requirements, or at least a preliminary
21 minimum set of requirements, which is going to get
22 evolved as we learn more about how these systems work;
23 take those methodologies, see whether or not they meet
24 the requirements that we've identified, and then test
25 them with benchmarks, so we've done a preliminary

NEAL R. GROSS

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

1 review of the first six of those steps, and determined
2 that the two leading candidates from a dynamic
3 standpoint are a Markov methodology, and a dynamic
4 flow-graph methodology. Each has limitations and
5 advantages both in terms of modeling complexity, the
6 data you need, how you structure it, the amount of
7 information that's necessary, the amount of
8 quantitative versus qualitative information you get.
9 And we're getting leaders in both those areas as
10 subcontractors and contractors to look at that
11 methodology.

12 Okay. The next three or four slides are
13 just a review of the benchmark we chose. The purpose
14 of this is to talk about why we chose this particular
15 benchmark, and how we've set it up. The idea is to
16 have a benchmark that hits the various possible
17 modeling requirements as much as reasonable for a
18 single system, because we're not going to do 30
19 systems to make our decision. We want to do two or
20 three systems to make a reasonable assessment of
21 what's really necessary for practical systems, so we
22 chose the benchmarks in such a way that they're both
23 representative of real systems, and they have a lot of
24 the characteristics of various digital systems, and
25 the feedback processes associated with them.

NEAL R. GROSS

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

1 This particular benchmark is a digital
2 feedwater control system based on an operating plant's
3 digital feedwater system.

4 MR. HICKEL: Which plant?

5 MR. ARNDT: I'd rather not say in a public
6 meeting.

7 MR. HICKEL: It's a real one, though.

8 MR. ARNDT: Yes. We've taken the actual
9 system, we've generalized it a little bit to be
10 representative of this type of system; that is to say,
11 an important to safety, but not safety system that has
12 interactions with the process, and interactions within
13 itself between its component parts. Basic purpose of
14 the feedwater control system is to maintain the level
15 in the steam generators.

16 For the particular scenario we chose, the
17 failure criteria for this particular system is above
18 30 or below 24 inches. This is scenario-dependent.
19 We'll talk about the particular scenario we chose
20 later in the presentation.

21 MEMBER KRESS: Was there a reason for
22 those numbers, like the steam generator loses its
23 effectiveness beyond that or something?

24 MR. ARNDT: Based on the particular
25 scenario, there's numbers -- some other actuation

NEAL R. GROSS

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

1 happens, it either loses its effectiveness, or causes
2 another system to actuate or whatever. Connected
3 basically to^v the main feedwater system that regulates
4 the feedwater pump, the main feedwater valve and
5 bypass valve. The controller in the system's basic
6 purpose is to regulate the steam generator, level the
7 temperature, and deal with other things associated
8 with the steam system.

9 Real quick overview - steam generator
10 system, obviously, there's booster pumps and
11 condensate pumps in here, but just simplified system.
12 You have inputs, power from the reactor, steam flow
13 level, feed^v flow, feed temperature. The system is
14 basically structured with a main computer and a backup
15 computer, a controller which takes information from
16 these computers for the bypass valve, the flow valve,
17 and the feed pump. You have the back-up controller,
18 and I'll talk a little bit about how that's
19 configured.

20 You have a number of different internal
21 inter-connections. This is the Type 2 interactions
22 that I mentioned. The main computer will trip off to
23 the back-up^v computer. It also has a watchdog
24 associated with the various controllers it is
25 providing information for. We also have something

NEAL R. GROSS

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

1 known as a --

2 CHAIR APOSTOLAKIS: You know, when you use
3 terms that are not commonly used by everybody, you
4 should explain that. Watchdog status - I mean, what
5 does that mean? It's probably part of the language of
6 this field.

7 MR. ARNDT: Apologies. Watchdog timer or
8 watchdog status is a commonly used fault tolerant
9 capability among digital systems. The concern is that
10 you either get stuck in the loop, or if you hang the
11 computer, or you do not progress through the system,
12 watchdog, you can configure it in a number of
13 different ways, but in this most basic configuration
14 is waiting for certain things to happen. If it
15 doesn't happen under a certain time cycle, or under a
16 certain set of conditions, it will flag an error, or
17 trip the system out, or go from a primary system to a
18 backup system.

19 CHAIR APOSTOLAKIS: Good.

20 MR. ARNDT: The only point of this slide
21 is basically there's a number of different internal
22 connections associated with how the system works, how
23 it feeds from one system to another, what the fault
24 tolerant capabilities are, if the main computer does
25 not continue to update, the controllers will take 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 last signal. It will identify issues to the operator
2 that will allow the operator to go into manual mode,
3 between the different controllers going between the
4 various modes of operation, full power and low power
5 operation. The point being, there is indications
6 associated with it that lead us to have Type 2
7 interactions in the system.

8 The input parameters are cross-tied based
9 on the various channels, as you would expect, to
10 reduce the likelihood of single failure criteria.
11 Control laws are non-trivial, and I won't go through
12 all these in detail, but they have a number of fairly
13 complex control laws associated with the demand, the
14 compensated air, and the level, both for the flow, the
15 level, the power, the positions for all the different
16 valves, and the speeds. The point here is, there's a
17 lot of process dynamics that can feed back into the
18 control system that makes when the system fails and
19 when which pieces of the system fail important.

20 CHAIR APOSTOLAKIS: So these laws are used
21 by either dynamic methodology?

22 MR. ARNDT: These laws are used by the
23 dynamic.

24 CHAIR APOSTOLAKIS: Are they also being
25 used by DFM?

1 MR. ARNDT: They're being used by both of
2 the dynamic methodologies. This is the system. We'll
3 talk about how we model the system in both the dynamic
4 methodologies later in the presentation.

5 MR. HICKEL: I guess one question is, is
6 this system taking the original PID controller and
7 converting it to an equivalent digital, or is this
8 something that's a revolutionary system that's trying
9 to feed forward, or something like that?

10 MR. ARNDT: It's basically a conversation
11 of the PID controller that was originally in there.
12 There's some added features, but basically that's
13 where we are.

14 This is just some more basic information
15 on the control laws. The issue here is because of the
16 way the control laws are developed, the current state
17 of the system is dependent on the historical
18 information in the digital system, so there's history
19 in the state space.

20 As I mentioned before, there's a number of
21 fault tolerant capabilities in the system. One of the
22 reasons we care about this is, it touches on a lot of
23 the potential reasons why you would need a dynamic
24 methodology, the DFM, the Markov, or something else,
25 as opposed to a simple fault tree/event tree. So 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 controllers for the main feed valve, backup feed valve
2 and the feed pump for the control systems to the
3 corresponding feed control points provides fault
4 tolerance in case the computers fail, gives the
5 operator time to intervene, switch from automatic to
6 manual. The computers are independently wired to
7 different power sources. You can have different kinds
8 of single failure controllers, single failure modes.
9 The algorithms take a relatively short time compared
10 to the response frequency, the physical process.
11 There's a watchdog timer, as I explained earlier, on
12 each of the two computers, the backup and the main
13 computer. If the set point - if the system fails,
14 the computers will fall back to a pre-programmed set
15 point value. Each of the computers has a validation
16 and verification of the inputs, so that there's a
17 number of different fault tolerant features associated
18 with the controllers that may lead to Type 2 dynamic
19 interactions.

20 CHAIR APOSTOLAKIS: So these are included
21 in the two methodologies? They said yes.

22 MR. ARNDT: I'm sorry. Again, the input
23 ranges are checked, the backup computer propagates the
24 sensor data.

25 MR. HICKEL: What's a PDI controller? I

1 know what a PID controller is. Is that just -- is
2 that a typo on the --

3 MR. ARNDT: No, that's really what it's
4 called. It's --

5 MR. HICKEL: Portional Derivative Plus
6 Integral, instead of --

7 MR. ARNDT: No.

8 MR. KEMPER: No, this is Bill Kemper. The
9 particular plant where this system is deployed, that
10 controller normally monitors, if my memory serves me
11 right, differential pressure across the main feedwater
12 valve, so it's called PDI. It's an indicator. In the
13 fail mode, it reverts to a control device for one of
14 the SD's head, either the main feed valve or the
15 bypass valve controller.

16 MR. ARNDT: It serves for the purposes of
17 the dynamic interactions, as basically a backup to the
18 other controllers in the system.

19 As I mentioned as we were going along, the
20 system incorporates all the properties of a loosely
21 coupled system; that is to say, it has a lot of the
22 properties we care about when we're trying to
23 determine what level of modeling detail we need to
24 address. Some of the properties it doesn't
25 incorporate, but those systems may not be important to

NEAL R. GROSS

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

1 the kinds of controllers and digital systems that are
2 actually in nuclear power plants. When we wrote the
3 issues for digital systems, we wrote them as general
4 as possible, so we included things like networking and
5 shared external resources.

6 Without knowing what the licensee is going
7 to bring to us in terms of a configuration, we wanted
8 to be as general as possible. We understand that
9 most, particularly safety system, digital systems are
10 going to be used in a real-time safety system. We're
11 not going to have networking resources, or shared
12 external resources, so that may be a less important
13 criteria which will eventually drop out of a
14 regulatory guidance. We wanted to start general, and
15 focus in.

16 MEMBER BONACA: I have a simple question
17 here, Steve.

18 MR. ARNDT: Yes, sir.

19 MEMBER BONACA: You know, some plants
20 already have this system, this feature. Has any plant
21 attempted to model in their PRA these control systems?

22 MR. ARNDT: There are models of control
23 and protection systems in PRAs. They tend to be, and
24 I don't know what all 103 PRAs look like in detail,
25 some of them are very, very general.

NEAL R. GROSS

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

1 MR. KEMPER: Black box.

2 MR. ARNDT: Black box, and most of them,
3 I would say, are incorporated as sub-components of the
4 system as a whole. There are some models, some of
5 them - I'll use a non-U.S. example to be safe, such as
6 the Seiswell B model, is fairly detailed. Seiswell
7 has a fairly detailed PRA model of their control and
8 instrumentation systems, and protection systems.
9 They're not a dynamic model, they can't capture the
10 kind of dynamic interactions we're talking about. Do
11 they need to? Well, that's part of the reason we're
12 doing the research, is to see whether they need to or
13 not. But most of them are fairly general, and some of
14 them are very black box, as John mentioned.

15 MEMBER BONACA: Yes. Okay, thank you.

16 MR. ARNDT: As I mentioned earlier, the
17 system includes system history as part of the control
18 laws, so there are opportunities to create artifacts
19 and/or create situations where the exact timing and
20 sequence of events might be very important.

21 At this point, I'd like Professor Aldemir,
22 who did this particular analysis, to walk you through
23 an example of what can happen in this case associated
24 with timing failure sequences.

25 MR. ALDEMIR: In the first slide here on

NEAL R. GROSS

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

1 the left, you're seeing the normal behavior of the
2 system. Incidentally, this is simulating a situation
3 where the initiating event is a turbine trip with main
4 computer failed. And the reason why it's failed, is
5 so that the state space is limited for illustrations.
6 This example is taken from the report that we just
7 went through earlier, and in this report, we are
8 trying to illustrate how these methodologies work, and
9 for the ease of understanding, we chose a simpler
10 system with a smaller state space, so it does not
11 represent the whole controller. That's why we
12 purposefully assumed that the main computer failed, to
13 reduce the state space.

14 So here you see the normal behavior of the
15 system, level starts -- okay. The scenario is such
16 that we're operating at full power, turbine trips, and
17 within 10 seconds the power is reduced to 6.6 percent
18 of nominal power with feedwater flow following, so you
19 have these oscillations until the level stabilizes
20 around 100 seconds. Incidentally, these time
21 constants may not really refer to the actual plant,
22 but these are time constants still lead to believable
23 behavior of the system, credible behavior of the
24 system.

25 MR. HICKEL: Could I ask a question?

NEAL R. GROSS

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

1 MR. ALDEMIR: Sure.

2 MR. HICKEL: You say it's a turbine trip.

3 MR. ALDEMIR: Yes.

4 MR. HICKEL: Are we talking a plant that
5 has a big steam bypass system?

6 MR. ALDEMIR: Not to my knowledge.

7 MR. HICKEL: I don't understand the level
8 - to understand the level in the generator, you've got
9 to know what the pressure is doing, so if you trip the
10 turbine, you've taken away the load.

11 MR. ALDEMIR: Right.

12 MR. HICKEL: Steam wants to go somewhere.

13 MR. ALDEMIR: Right.

14 MR. HICKEL: If you don't take it
15 somewhere, pressure is going to go way up, level is
16 going to go way down. How is that just oscillating --

17

18 MR. ALDEMIR: We are tripping -- the
19 reactor trips.

20 MR. HICKEL: Right. Okay.

21 MR. ALDEMIR: So within 10 seconds or so,
22 the power is down to 6 percent. That's where this
23 scenario starts. So at the beginning of the scenario,
24 at least as I've shown on this slide, power is 6.6
25 percent of nominal, which is 1500 megawatts, and then

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 feedwater is at that nominal flow. Then through the
2 bypass flow valve, in this situation, the main flow
3 valve is not active. The bypass valve is active. It
4 is trying to regulate the flow so that it reaches the
5 set point. I mean, it stays at the set point, which
6 is by convention, zero.

7 CHAIR APOSTOLAKIS: These are the results
8 of the solution to what, to the laws that you showed
9 us earlier?

10 MR. ALDEMIR: Not all equations -- this
11 particular initiating event, according to the control
12 laws, is such that only three or four of those
13 equations are relevant.

14 CHAIR APOSTOLAKIS: But this is the output
15 of what?

16 MR. ALDEMIR: Part of the equations that
17 you saw in the earlier slide.

18 CHAIR APOSTOLAKIS: And anything else?

19 MR. ALDEMIR: I'm not sure if I'm
20 following.

21 CHAIR APOSTOLAKIS: You're talking about
22 the steam generators --

23 MR. ALDEMIR: Oh, oh, oh, I'm sorry. Yes.
24 Well, thank you for the remark. In those equations
25 then, I don't know how easy it's going to be for me to

NEAL R. GROSS

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

1 go back in slides, but in the equation that governs
2 the level change, there is feedwater flow input, and
3 steam flow out. And these are, of course, related.
4 Now this relation is described by a steam generator
5 module, which was developed -- the one that we're
6 going to use is developed by our subcontractor, ASCA.
7 Also, the developers of the dynamic flow-graph
8 methodology.

9 In this particular example, we are not
10 using that steam package because, as I said, for
11 simplicity of illustration or the ease of
12 illustration, we are trying to put down equations that
13 you can easily follow, so in this equation, the steam
14 flow is assumed to be constant, and the feed flow is
15 used through a simplified pipe and valve model, also
16 taken from NUREG 64.65, which illustrates how the
17 dynamic flow-graph methodology works. Thank you,
18 Professor Apostolakis. I missed that process part.

19 Now here, this is very interesting, and
20 actually, it was a surprise for us, too. If you
21 notice, up to 600 seconds nothing happens here.
22 Everything is beautiful, everything is maintained at
23 zero level. If you let it run longer, suddenly you
24 have a kink in the system, suddenly through this
25 control. Now this was by accident. Turns out that

NEAL R. GROSS

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

1 our colleague who was doing the programming put an
2 artificial or unnecessary bound on one of the
3 parameters, and it's basically an artifact. The real
4 system does not do that, if you program it carefully.
5 But well, we are trying to model software faults, so
6 this is the kind of experience that you can have with
7 the model. Incidentally --

8 CHAIR APOSTOLAKIS: Your own people make
9 mistakes?

10 MR. KEMPER: Hard to believe, isn't it?

11 MR. ALDEMIR: Well, I mean, it was
12 fortunate, because then we created an artifact in the
13 system without intending. Incidentally, these types
14 of events have been observed in real life. And in the
15 report that was being referred to earlier, we cited
16 about four or five examples, where these kinds of
17 events were observed in plants either through the
18 process, complexity of the process, longevity of the
19 process, or actual error in the tuning of the
20 controller. So the benchmark does capture these type
21 of events. Well, I'll come to that later on, but
22 talking about the requirements - can it produce
23 observed failures? Yes, this is one of the cases
24 where we can produce observed failures, because these
25 things have been observed in actual plants.

NEAL R. GROSS

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

1 Now another interesting thing here is that
2 - and this is, again, not intentional. We did not
3 choose the parameter so that we'll have this behavior.
4 It just so happened that we did have this behavior,
5 the discoveries were accidental, too.

6 In this situation, bypass flow valve, we
7 took curves here. Let's take the first one. The blue
8 one, the steam generator is chugging along, and the
9 level is changing. And at 43 seconds, bypass flow
10 valve fails stuck, and you have a low level. If the
11 bypass flow valve fails stuck at 44 seconds, you have
12 high level. One second difference, two different
13 failure modes.

14 MR. HICKEL: The valve was modulating,
15 obviously?

16 MR. ALDEMIR: That's exactly right. And
17 the stuck mode is such that it just gets stuck and so
18 it has to refer back to the history-dependent
19 information, and just so happens at that time, exactly
20 where the level is, you may have totally different
21 modes.

22 CHAIR APOSTOLAKIS: So what do we learn
23 from this?

24 MR. ALDEMIR: We learn from this that it
25 is very important to model the timing of events in the

NEAL R. GROSS

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

1 reliability model, so it's an illustration of why we
2 may need dynamic models.

3 CHAIR APOSTOLAKIS: A one second
4 difference?

5 MR. ALDEMIR: One second difference. And
6 as I said, this wasn't intentional. Purely by
7 accident, we chose the time clusters for the system.
8 We did an analysis. I don't think we have it in the
9 slides, but it is in the report. We did a little
10 analysis of the controller to see what kind of
11 parameter ranges will lead to stable behavior, and
12 arbitrarily chose time constants, and just so happens
13 that this is the type of behavior we observed.

14 CHAIR APOSTOLAKIS: What do you mean by
15 "time constants"? Which one did you choose --

16 MR. ALDEMIR: If you go to the -- again,
17 I don't know how easy for me to switch, but if you
18 look at the original equations, there are a number of
19 controller parameters.

20 CHAIR APOSTOLAKIS: Okay. Okay.

21 MEMBER KRESS: Couldn't you consider
22 either one of those paths a failure, and not have to
23 know that time --

24 MR. ALDEMIR: Yes, we may have to. For
25 example, I mean, in this situation, I hope I'm

NEAL R. GROSS

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

1 recalling this correctly.

2 MEMBER KRESS: I'm very skeptical about
3 one second timing.

4 MR. ALDEMIR: As I said, it was surprising
5 to us, too. But that's what we have observed.
6 Incidentally, this type of difference in failure modes
7 is not the first time that we're observing in this
8 system. We have a publication in 1989 where we are
9 using the HIPCO system, bleed cooling of BWR. This is
10 NUREG 69.01, where again, the timing of events are
11 very important, and it can take you to high level or
12 low level.

13 MEMBER KRESS: Would you do something
14 different depending on which of those modes --

15 MR. ALDEMIR: Yes. For example, in this
16 situation what happens is that if we hit the low level
17 - now I hope I can recall this correctly - if we hit
18 the -- right now we are dealing with the bypass flow
19 valve, turbine is not available. So if we hit the low
20 level -- sorry, we are dealing with the auxiliary
21 system, I think. We hit the low level, and then the
22 turbine is made available as a heat sink, and then the
23 main flow controller comes into play. And if we hit
24 the high level, I'm assuming that this is going to be
25 the performance of the steam generators. So in the

NEAL R. GROSS

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

1 HIPCO system[^] that we used earlier, if you hit the low
2 level - now that becomes a safety-related action,
3 because it actuates the LPCI system or LPCS system.
4 So if you hit the high level, you don't do anything.

5 MEMBER KRESS: Explain to me why the high
6 level is a problem.

7 MR. ALDEMIR: High level, I presume, this
8 is the steam dryers performance deteriorating.

9 MR. KEMPER: This is Bill Kemper. Yes,
10 this plant is a PWR with U-tube steam generators, so
11 high level,[^] the problem is just as Tunc said, the
12 dryers and everything becomes immersed in water,
13 carry-over and damage the equipment.

14 MR. ALDEMIR: So the failure mode is
15 important in the sense that, in general, because one
16 may lead to a safety-related action.

17 CHAIR APOSTOLAKIS: But, I guess, I'm
18 thinking, again, in terms of traditional modeling.
19 The two failure modes would be recognized by the
20 analysts, I think, if they lead to different
21 sequences. And, again, is the issue of the timing, 43
22 versus 44 seconds, important, as long as they
23 recognize that different things may happen, depending
24 on whether you're high or low.

25 MR. ALDEMIR: If we are running a

NEAL R. GROSS

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

1 qualitative analysis, you are right. Now if we are
2 doing a PRA and quantifying it, it makes a lot of
3 difference in quantification whether you go to one
4 failure mode or the other failure mode. And we have
5 --

6 CHAIR APOSTOLAKIS: Yes, but the guy who
7 does an event tree will do that. He will just -- the
8 only thing he will ignore, the way I understand it, is
9 the fact that there is a difference of one second
10 there to go to one to the other, but you will have
11 this mode and that mode.

12 MR. HICKEL: This is not unique to
13 digital. I could postulate the same kind of issue on
14 an old analog system. The feed reg valve - if the reg
15 valve locks up, it's going to either fail high or fail
16 low. The relevance to digital is what I'm trying to
17 understand.

18 CHAIR APOSTOLAKIS: Yes. But isn't it
19 correct, though, that if you do a PRA and you
20 recognize that there are two failure modes, you will
21 have them there. What you will not have is the
22 timing, and if the timing is important, I bet you a
23 good PRA analyst will find a way to include that
24 there, too. Now just one second difference --

25 MEMBER KRESS: I could see where the

NEAL R. GROSS

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

1 timing, though, my affect the liability probabilities.

2 MR. ALDEMIR: That's right.

3 MR. ARNDT: There's two primary issues,
4 yes. In all likelihood, if you've done a good failure
5 modes and effects analysis, and know the different
6 kinds of failure modes you might end up with, in a
7 traditional fault tree-type analysis, you'll have
8 these different failures. There's two issues. One,
9 depending upon the complexity, this is actually a
10 relatively simple set of scenarios. There are some
11 scenarios that are much more difficult to see just by
12 looking at and trying to analyze and see whether or
13 not you have captured all the different failure modes.
14 Simple systems, much higher probability you're going
15 to capture all the failure modes; more complicated
16 systems, more interactions, more dynamics, less
17 probability.

18 The other thing is, as we've talked about,
19 if you're trying to quantify the system, it's much
20 more difficult to get a good quantification if you're
21 not including all the characteristics of the system,
22 such as these characteristics. The point is, we're
23 trying to understand what factors may influence the
24 level of modeling detail that's necessary. Okay?

25 To answer John's question, a lot of these

NEAL R. GROSS

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

1 things - well, actually, the vast majority of these
2 things are associated with system complexity, not
3 necessarily digital, although there are some things
4 that are digital-specific. The fact is, because
5 digital systems tend to be more complex, at least at
6 the micro level, you tend to run into more of these
7 issues. It doesn't mean you can't make a very simple
8 digital system. Okay?

9 PARTICIPANT: Deja vue, wonderful timing,
10 one of George's big issues.

11 MEMBER KRESS: We'll let Mario be --

12 MR. ARNDT: I'm going to go through three
13 or four slides here. This was the issue that
14 Professor Apostolakis brought up earlier associated
15 with how we are structuring understanding the system
16 in terms of what the data is. And in any basic data
17 generation or data gathering process, you want to have
18 a systematic methodology to look at what data you
19 need, which is dependent upon both the system and the
20 model you're trying to generate the data for. You
21 choose the model of the system that is reasonable for
22 the level of detail you need. You choose plausible
23 modeling assumptions associated with that. You look
24 at all the parameters that need to be modeled in a
25 logical way and you work through the process,

NEAL R. GROSS

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

1 understanding the uncertainties, and trying to
2 understand the critical parameters, and the
3 statistical information necessary to get a good
4 confidence bound on that system.

5 Like any system - in this case we happen
6 to be choosing two dynamic methodologies, DFM and
7 Markov - you need models that are supported by
8 observable credible data. In this particular case,
9 what we start with is historical plant data and
10 database information for the components. In this
11 case, we looked at the RAC Prism database, there are
12 other databases out there. You then go and look at
13 the specific plant data, if you have any. This is
14 important, particularly in digital systems, because
15 you have to map the entire input space. And in
16 George's parlance, the context of the system. In
17 traditional digital or software modeling, you usually
18 talk about the operational profile. It's basically
19 the same concept. What is the space of all possible
20 inputs, and what's the probabilities associated with
21 those?

22 You can get a lot of that information from
23 the plant historical data, if you happen to have it.
24 The information you don't have, or need additional
25 information on it, you look at other mechanisms

NEAL R. GROSS

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

1 associated with it. In terms of hardware, you might
2 look at stress testing of the system or environmental
3 testing of the system, in terms of digital systems you
4 usually look at different kinds of stress testing of
5 the system, or testing of the various possible failure
6 modes associated with it. The methodology we chose,
7 which we happen to like, but is not the only way to do
8 it, is a fault injection campaign, which looks at the
9 potential failure modes, both safe failure modes and
10 unsafe failure modes, and then maps back through a
11 system model, in this case the Markov model, the
12 potential input spaces that are necessary to get those
13 critical output failures. But the purpose here is
14 simply to augment the data, get a good understanding
15 of what the failure rates likely will be.

16 CHAIR APOSTOLAKIS: Now there is a number
17 of diagrams and discussion in the report that I don't
18 see you having here, so when would be a good time to
19 raise the questions?

20 MR. ARNDT: Give me two or three slides.
21 If you have additional questions, we can do it there.

22 CHAIR APOSTOLAKIS: Okay.

23 MR. ARNDT: If you'll note, at the very
24 end of that package, we have additional backup slides
25 to talk to these issues, if you want to talk to them.

NEAL R. GROSS

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

1 MEMBER KRESS: On this slide, though, I
2 presume coverage means that part of the input space
3 you didn't fault inject or what? Could you explain
4 what "coverage" is to me? Let's put it that way.

5 MR. ARNDT: Coverage is a generic term
6 used in digital system modeling analysis. There's
7 several different ways you can model it, but it's
8 basically a determination of the likelihood that
9 you're not going to detect a failure mode based on the
10 test that you conducted.

11 MEMBER KRESS: Because you can't do all
12 the range of inputs that are possible.

13 MR. ARNDT: That's correct.

14 CHAIR APOSTOLAKIS: This is where I have
15 a problem with the report. On page 2-30, there's an
16 incredible statement. "Suppose if we test and get no
17 undetected failure modes, by the fundamental law
18 testing, testing reveals the presence of errors, not
19 the absence of them. We must establish a lower bound
20 for the non-coverage one minus C termed with a non-
21 zero number. What is often done is to assume that one
22 undetected failure occurred in the testing." This is
23 incredible that we see something like this now. We've
24 been discussing this in PRA space for decades, and to
25 say that I have zero failures; therefore, I will

NEAL R. GROSS

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

1 assume one is just something -- and then it says,
2 "This assumption has a well-founded statistical theory
3 and legacy, Reference 54", which I found. And the
4 title reference is "Estimating the probability of
5 failure when testing reveals no failures", and I
6 couldn't find anywhere the suggestion that you assume
7 one failure. So this is a completely false statement,
8 and I don't know why it's being made. And as far as
9 I'm concerned, it undermines the credibility of the
10 whole thing.

11 MR. ELKS: If I may --

12 CHAIR APOSTOLAKIS: Yes, you may. You can
13 come to the microphone, identify yourself.

14 MR. ELKS: Carl Elks, University of
15 Virginia. We put that section in there, and I'll be
16 the person identifying myself as citing that reference
17 and using that. That was Dr. Dave Nichols at the
18 University -- I mean, at William and Mary University,
19 who I was working with at the time when we were doing
20 this type of work.

21 Essentially, this is a software testing
22 technique that has tried to establish through Bayesian
23 methods when you are trying to test something and you
24 do not get any type of estimation of any type of
25 failures, what's the worst case that you can do on

NEAL R. GROSS

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

1 this? Now this was applied on a number of different
2 software testing techniques, as well, on fault
3 tolerance techniques. That's why I stated the case
4 that there is a legacy of using this. We have used
5 this, also, at the University of Virginia on several
6 different fault tolerant architectures when we did
7 lots and lots of testing on them, and we found no
8 errors to establish, again, a bound for this type of
9 thing.

10 Now does that mean that we're going to use
11 that particular technique all the time? No, that was
12 a suggestion that we could use based upon this type of
13 model that we're working on, so I'm not suggesting to
14 the committee at all that this particular technique is
15 the only technique we can use. I'm suggesting that
16 that has been used. It has some statistical reference
17 in legacy in the assessment of safety critical and
18 reliability systems.

19 CHAIR APOSTOLAKIS: But the paper that is
20 being cited is a rigorous paper using Bayesian methods
21 deriving distributions using zero failures or
22 findings. And if one wanted to be conservative, one
23 could select a percentile of this distribution and use
24 that, and not assume that there is one failure, which
25 is something that really is arbitrary as anything. So

NEAL R. GROSS

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

1 I -- anyway, okay.

2 MR. ELKS: Okay.

3 CHAIR APOSTOLAKIS: Thank you.

4 MR. KEMPER: This is Bill Kemper, very
5 good comment. Thank you for the comment, George.
6 Thank you.

7 CHAIR APOSTOLAKIS: There are many other
8 questions I have on this particular section, 2.4.2.
9 And I don't know what the best way is. Again, and I
10 have asked this question in the past - there are three
11 states. Okay? Normal, fail safe failure, dangerous.
12 And then it says, "Associated with each state
13 transition is a parameter that indicates the rate
14 lambda at which the failure occurs. And again, I'm
15 trying to understand, what does that mean? And then
16 an hour later, I read the BNL report on data, and they
17 say that they found a 36 percent of failures due to
18 requirements analysis, 27 percent are due to faults
19 that are introduced during upgrades or modifications.
20 And I'm scratching my head now, does this lambda
21 include these things? What does it include, is it
22 hardware failures only? I mean, on the one hand, I
23 have BNL telling me that 36 percent of failures are
24 due to requirements, which I knew, maybe not the 36
25 percent, but I knew it was a pretty high percentage.

NEAL R. GROSS

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

1 And now I see a transition rate that tells per unit
2 time, there is a constant probability of going from
3 this state to that state. And we have raised this
4 issue before, that before we jump into these Markov
5 models, we really have to scrutinize the meaning of
6 these transition rates. I mean, it's a convenient
7 mathematical tool, I admit, but what does it mean?

8 MR. ARNDT: Okay. Let me try and address
9 this briefly. Obviously, if you want to go into a lot
10 of detail, depending upon the amount of time we have
11 today, we can have a separate discussion on this
12 specific issue, if you like. But the work that's done
13 by BNL is looking at specific - how you add up those
14 different failures, what kind of failures are they,
15 what kind of failures you need to look at, et cetera.
16 The Markov and DFM modeling methodologies are system-
17 based modeling methodologies. They look at how does
18 the system as a whole fail, so the various failure
19 rates, and we don't need to have them be constant
20 failure rates, they can be - or transition rates.
21 They can be non-constant, if we choose to. We simply
22 are using that as a methodology right now, but if the
23 data indicates that we need time-dependent failure
24 rates, we can do that.

25 Looking at how you transition from one

1 state space^v to another, those failure rates, or
2 transition rates, depending on whether it's going to
3 a fail state or not, are a particular failure. The
4 stuff we're talking about in the BNL can be caused by
5 a number of different things. It could be caused by
6 hardware failure, could be caused by a system failure,
7 could be caused by interaction between the hardware
8 and the software. What we're trying to do in the BNL
9 failure database work is understand how do you
10 populate that failure database, and what has to be
11 included in it? Some of those will be failures that
12 are driving a system from one state to another.

13 CHAIR APOSTOLAKIS: But, Steve, if we have
14 design errors where design is used in the broader
15 sense, includes requirements, includes specification
16 errors and so on, and these are a significant
17 percentage of the observed failures in the past,
18 failure rates do not account for those, because with
19 a failure rate you are saying my system is working
20 now, and there is a certain probability per unit time
21 that it will^v move to some other state.

22 MR. ARNDT: Correct.

23 CHAIR APOSTOLAKIS: Here it's working now,
24 but if it enters another regime where there is,
25 indeed, a specification error, it will not work,

NEAL R. GROSS

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

1 period. There is no -- so what is the time? Is it
2 the transition rate to that regime, in which case the
3 fault manifests itself?

4 MR. ARNDT: Yes, exactly.

5 CHAIR APOSTOLAKIS: But that's the kind of
6 thing I'd like to see in these reports. I mean, don't
7 just throw out this is -- then there is other
8 statement, "The probability of being in a fail safe
9 state or a fail unsafe state can be solved using
10 sarcastic Markov modeling." How on earth do you know?
11 What do you mean, that's a postulate on your part.
12 This scrutiny of the assumptions is something that I
13 would really like to see, and have a detailed scenario
14 of what we mean by these failure rates. And when you
15 have -- if you look at the BNL report, for example,
16 and you say yes, this is the rate of going into that
17 area where there may be an error, pick a few and see
18 whether that kind of interpretation or explanation
19 makes sense, because we are really -- I mean, this is
20 very important stuff, and there is a danger here, not
21 that you guys are doing that, of course. I don't
22 expect you to do that, but it's the danger that
23 because there is a model some place, we're going to
24 force this -- you know the Procrustian bed?

25 MR. ARNDT: Yes.

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

1 CHAIR APOSTOLAKIS: Okay. Everybody knows
2 about the Procrustian bed now. So that's good, so
3 this is the kind of thing that bothers me when I read
4 this.

5 MR. ARNDT: Okay. We can articulate that
6 much better.

7 CHAIR APOSTOLAKIS: I mean, the CIs, and
8 the other question, of course, is okay, I inject the
9 fault, I find the problem. Don't I fix that if I find
10 the problem?

11 MR. ARNDT: Yes, you do.

12 CHAIR APOSTOLAKIS: So how does that play
13 into all this? I mean, if every time I find an error
14 - you see, in standard PRA with hardware failures -
15 okay, the pump fails. We expect that, it's random
16 failures and so on. The nature of the problems you
17 are finding here is different.

18 MR. ARNDT: That's correct. It's
19 different.

20 CHAIR APOSTOLAKIS: And you'd fix them, so
21 the question is now what do I do after I fix them? Do
22 I say I found three faults, but then I fixed them, so
23 what's going on here? By the way, NASA has the same
24 problem as we speak, because they fix everything.
25 Okay? They change the design of the system, and some

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 people claim then the past record doesn't apply.

2 MR. ARNDT: And there's really two things
3 we're trying to understand to support these kinds of
4 modeling issues. One is, what is the likelihood of
5 faults remaining in the system we've tested, and there
6 are methods associated with that. And the other thing
7 is, what is the likelihood that we haven't tested
8 everything, which is basically the coverage concept.
9 You develop a structure by which you go from the
10 failed states that you know would be bad, through a
11 model to understand what input space you need to test,
12 and you test a significant fraction of that.

13 CHAIR APOSTOLAKIS: No, I understand that,
14 and I think it's a very difficult problem. I mean,
15 the step of measuring, go to a model, and what kind of
16 model. But I'm not saying that the fault injection
17 method is no good, but you really have to be careful
18 what information you're getting out of it, and how
19 you're going to use it.

20 MR. ARNDT: Exactly.

21 CHAIR APOSTOLAKIS: Not arbitrarily say
22 I'm going to assume this, I'm going to assume that,
23 and keep going. I mean, that's not - especially in
24 this regulatory space, that's not the way to do
25 things.

NEAL R. GROSS

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

1 MR. ARNDT: Right. As I think I mentioned
2 earlier, the tool that we developed, obviously, for
3 our independent assessment may not be the same tool or
4 same strategy that the licensees choose, but we want
5 to understand the capabilities of the various
6 methodologies.

7 CHAIR APOSTOLAKIS: Now there is a table
8 of failure rates presumably produced by default
9 injection method on page 2-34, and there are some -- I
10 mean, the rates are on the order of 10 to the minus 6
11 per hour, but two questions here. One, they seem to
12 be focused on hardware components. They don't include
13 software failures. Right? Is that correct?

14 MR. ARNDT: This particular methodology
15 looks at the system as a whole.

16 CHAIR APOSTOLAKIS: But these components
17 are part of the controller. Right?

18 MR. ARNDT: Yes.

19 CHAIR APOSTOLAKIS: But it does not --
20 they don't include software faults, where all the
21 components are working but there is an error --

22 MR. HICKEL: You've got a bug.

23 CHAIR APOSTOLAKIS: Yes, you've got a bug.

24 MR. ARNDT: Right. That particular chart
25 does not, no.

1 CHAIR APOSTOLAKIS: It does not.

2 MR. ARNDT: But the methodology looks at
3 any kind of failure, and then it traces it backwards
4 through the system to determine whether or not that
5 failure manifests itself by a software bug, a firmware
6 bug, a hardware bug, a random failure of whatever.
7 This particular one did not do that.

8 CHAIR APOSTOLAKIS: Okay. Now again, when
9 you see something like that, there is a great
10 temptation to go to the BNL reports. And on page 14
11 of the collection of failure data, there are all sorts
12 of failure rates for various components, and how do
13 they compare with this table, 2.4.1 in this report?
14 This is the kind of coordination, it seems to me, that
15 maybe you haven't done yet because these things are
16 still being produced, but at some point, you can't
17 have a table in the report from BNL that has numbers
18 for all kinds of things, and then another table with
19 different numbers, unless there is a reason.

20 MR. ARNDT: Yes.

21 CHAIR APOSTOLAKIS: If there is a reason,
22 then that's fine. So that's a comment here, that
23 these reports, they have to feed into each other.

24 MR. ARNDT: Yes. Absolutely.

25 CHAIR APOSTOLAKIS: And the BNL report, of

NEAL R. GROSS

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

1 course, reports actual events.

2 MR. ARNDT: Yes.

3 CHAIR APOSTOLAKIS: As opposed to
4 producing using fault injection methods and so on,
5 which on the other hand, is very system-specific,
6 which has a great value.

7 MR. ARNDT: Yes. Exactly.

8 MR. KEMPER: This is Bill Kemper. If I
9 can just interject something here; we do intend to go
10 through the BNL information in much more detail,
11 George.

12 CHAIR APOSTOLAKIS: Good.

13 MR. KEMPER: So maybe some of these
14 questions might be answered as Todd and BNL goes
15 through that information.

16 MR. ARNDT: Okay.

17 CHAIR APOSTOLAKIS: But again, Steve, in
18 Chapter 2 of this report, using whatever method, there
19 are failure rates of components and coverage factors,
20 and all these refer to hardware. Is that correct? No
21 faults in logic, or bugs, or whatever.

22 MR. ARNDT: The point of this report is to
23 demonstrate the methodology, not to talk about the
24 results. There will be a subsequent report that talks
25 about the results of this benchmark.

1 CHAIR APOSTOLAKIS: No, I understand that,
2 but if the methodology is limited to hardware failure,
3 that's something we want to know.

4 MR. ARNDT: No, it's not.

5 CHAIR APOSTOLAKIS: Okay. By the way, you
6 tell me when a convenient point is to take a break.

7 MR. ARNDT: Okay.

8 CHAIR APOSTOLAKIS: You decide.

9 MR. ARNDT: Shortly.

10 CHAIR APOSTOLAKIS: Shortly.

11 MR. ARNDT: I've got about three or four
12 more slides I want to do.

13 CHAIR APOSTOLAKIS: Okay.

14 MR. ARNDT: Briefly, the methodology is
15 here. Since we've talked about a lot of this stuff,
16 I will go through it real quickly. As we mentioned
17 earlier, we developed a model of how the system works,
18 state space model of how the system works. It can be
19 anything you want. We're using a Markov model. You
20 developed a statistical model associated with what you
21 need to test based on different kind of failure states
22 you have, how you do the modeling. You develop an
23 operational profile; that is to say, the context of
24 the system, what are the inputs, what are the
25 different inputs it's going to see, what are the

NEAL R. GROSS

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

1 different interactions it's going to have? You
2 construct a fault list based on how the system will
3 interact and what potential failures you're going to
4 have, back that through your model and come up with a
5 list of potential faults you need to inject. You look
6 at what is known as fault equivalents, which is a
7 methodology to look at how the different input states
8 would map to different output states, the same way you
9 would do Latin Hypercube or various kinds of modeling
10 methodologies to improve the statistics, a Monte Carlo
11 calculation. You use that information to get for
12 these systems the list of faults that you would need
13 to do, you run the experiment, and you get the data.

14 CHAIR APOSTOLAKIS: So this is a design of
15 a fault injection process.

16 MR. ARNDT: This is a design of a fault
17 injection process.

18 MR. HICKEL: Let's clarify, when you say
19 "a fault injection process", are you talking about
20 faults that are -- where somebody corrupts maybe,
21 let's say the set of stored constants, and then you
22 let the thing do it?

23 MR. ARNDT: That would be one way to do
24 it, yes.

25 MR. HICKEL: Or are you talking about

NEAL R. GROSS

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

1 faults injected by simulating a failed sensor input,
2 or both?

3 MR. ARNDT: Both.

4 MR. HICKEL: You're doing both.

5 MR. ARNDT: You look at all the different
6 possible faults associated with the system. It could
7 be failed inputs, it could be failed outputs, it could
8 be corruptions, it could be software failures if you
9 choose to do it that way.

10 CHAIR APOSTOLAKIS: But these don't
11 necessarily have to be failures. I mean, I can select
12 the values of the parameters that are extremely
13 unlikely, and I can run the program. That's not part
14 of fault injection. That's not a fault.

15 MR. ARNDT: No, that's not a fault.

16 CHAIR APOSTOLAKIS: It's a rare event.

17 MR. ARNDT: That's the operational
18 profile. That's the space of inputs that's the system
19 could possibly see.

20 CHAIR APOSTOLAKIS: Yes, I understand.
21 But people do this as part of this --

22 MR. ARNDT: Yes. And the way you
23 construct that is you look at both operational
24 history, what has the system seen, and also what
25 inputs will drive you to failures.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: Now shouldn't there --
2 I'm sorry. Complete your thought.

3 MR. ARNDT: No, that's fine.

4 CHAIR APOSTOLAKIS: Okay. Shouldn't there
5 be a statistical model there? It seems to me, one
6 great challenge here is that there is a Box 8A or
7 something that says we fix the faults. Yes, I mean,
8 it's not that you are producing K failures and then
9 trials, and then you go back and say well, now I'll do
10 my Bayesian dance and so on. You fix those. So now
11 what does that mean? Now what --

12 MR. HICKEL: Like George LaLuce and the
13 rectification of ATWS 20 years ago.

14 CHAIR APOSTOLAKIS: Exactly. Exactly.
15 Yes, sure. Yes, that's a similar thing. And the
16 models I have seen out there, they are full of
17 assumptions about these things, although this paper
18 that was from the - I think it was from the IEEE -
19 yes, "Transactions in Software Engineering" - that was
20 a pretty serious paper, by the way.

21 MR. ARNDT: There's been some fairly
22 significant work in this area. And the concept of
23 fault injection goes back to the paper by Voso a
24 number of years ago that looked at how this works.
25 And there's been a lot of work in this area, and the

NEAL R. GROSS

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

1 idea is both to have a very high likelihood of
2 uncovering failures, but also understanding them at a
3 much level greater detail what that tells you about
4 the future behavior of the system.

5 CHAIR APOSTOLAKIS: That's right.

6 MR. ARNDT: And that's what we're
7 basically using it for in this application. Let me
8 step through this, as basically the methodology that
9 is used to go with that chart.

10 CHAIR APOSTOLAKIS: Yes, I think we
11 discussed this.

12 MR. ARNDT: One of the big issues is the
13 operational profile or the context. In our case,
14 we're actually collecting data from the plant that we
15 got the system from, as well as understanding the
16 other possible assessments, and all that is at the
17 control of the assessor.

18 This is just basically a chart that goes
19 through and talks to the fact that we're not going to
20 use a complete representation. We're going to break
21 it down into modules or super components.

22 CHAIR APOSTOLAKIS: Yes, but this is where
23 I got confused, as I said earlier. I mean, in Chapter
24 2, I thought you're presenting the system, the control
25 laws and this and that.

NEAL R. GROSS

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

1 MR. ARNDT: Right.

2 CHAIR APOSTOLAKIS: And then I saw this
3 Markov thing, and confused -- there was a Chapter 4 in
4 Markov.

5 MR. ARNDT: Right. Again, this is simply
6 one way of representing the state space.

7 CHAIR APOSTOLAKIS: But are these rates
8 that are produced in Chapter 2 used by Professor
9 Aldemir in his Chapter 4?

10 MR. ARNDT: Yes.

11 CHAIR APOSTOLAKIS: So maybe you should
12 move them then, because they are not used by DFM, I
13 don't think. They are used by DFM?

14 MR. ARNDT: Yes. That's why it's
15 structured this way.

16 CHAIR APOSTOLAKIS: Okay.

17 MR. ARNDT: We'll get to that after the
18 break.

19 CHAIR APOSTOLAKIS: We'll get to that,
20 yes.

21 MR. ARNDT: This is just a representation
22 of how we put the various blocks together, the
23 sensors, the main computers.

24 CHAIR APOSTOLAKIS: Well, this is it now.
25 We have failure, or transition rates, or failures

NEAL R. GROSS

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

1 rates for each one of these boxes.

2 MR. ARNDT: We're going to have.

3 CHAIR APOSTOLAKIS: Well, that's what
4 Chapter 2 does. Right?

5 MR. ARNDT: That's the methodology we're
6 going to use to integrate the data we have with the
7 testing we're going to do.

8 CHAIR APOSTOLAKIS: Yes. And, again, the
9 issue of software problems is not covered by this
10 picture.

11 MR. ARNDT: Let me -- this is one example
12 of a state space diagram. They're functional states.
13 You have an operational state, you have an operational
14 state but with a loss of input, you have an
15 operational state with a loss of output, you have an
16 operational state that is unable to detect internal
17 failures. Doesn't matter whether this is a hardware
18 failure, rather hardware fault or software fault, or
19 how the fault occurs in this particular methodology.
20 It matters that the system goes from an operational
21 state to a not operational state, or failed state
22 based on some fault in the system. It doesn't matter
23 in this particular model --

24 CHAIR APOSTOLAKIS: But, again, the
25 question is, when you say "some fault", can you model

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 all faults through the lambdas and the CIs. That's
2 really the question.

3 MR. ARNDT: In theory, yes.

4 CHAIR APOSTOLAKIS: Well, but I'd like to
5 see some discussion of that, a little deeper.

6 MR. ARNDT: Okay.

7 CHAIR APOSTOLAKIS: Why you can do that.
8 And the CIs^u there, they really have a tremendous
9 impact. I mean, the CI itself is .99, .999, so one
10 minus that, you're talking about 10 to the minus 2,
11 and 3, and so on. And, again, they have to be
12 scrutinized why the number is .99.

13 MR. ARNDT: Right.

14 CHAIR APOSTOLAKIS: Okay. Good.

15 MR. ARNDT: And this is just the chart
16 that you talked about. And at this point, we're going
17 to talk about the PRA model and the actual modeling
18 methodologies, and this is a good time for a break.

19 CHAIR APOSTOLAKIS: Very good. So we will
20 reconvene at 10:25.

21 (Whereupon, the proceedings went off the
22 record at 10:10:18 a.m. and went back on the record at
23 10:28:12 a.m.)

24 CHAIR APOSTOLAKIS: Okay. Let's go back
25 in session. Steve.

NEAL R. GROSS

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

1 MR. ARNDT: We're going to continue with
2 Professor Aldemir talking about the PRA model and the
3 DFM and Markov analysis, but before we start that, I
4 thought it would be profitable for the Subcommittee to
5 talk a couple of minutes about fault injection
6 methodology; in particular, just to answer a few of
7 the open questions from the last discussion. If this
8 is not enough, we can have this as a separate topic at
9 our next meeting. We'd probably want to do that,
10 anyway. But while we're here, let's take five minutes
11 and talk to a couple of the specific issues.

12 Carl Elks from the University of Virginia
13 is here with us, and he will talk for a couple of
14 minutes on that and answer your direct questions.
15 Carl.

16 MR. ELKS: Okay. My name is Carl Elks
17 from the University of Virginia. Just to give a
18 little background, I started out doing fault injection
19 experimentation and testing at NASA Langley Research
20 Center in the early 90s, so I have some experienced
21 based on this, along with modeling fault tolerant
22 safety critical systems, and transitioning into formal
23 methods at the University of Virginia, and also
24 experimentation into safety critical systems.

25 The last discussion, we sort of talked

NEAL R. GROSS

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

1 about conceptually what fault injection is, but I
2 wanted to kind of just put a little finer point on
3 some of the issues. Fault injection is a specific
4 kind of testing regime to collect information out of
5 the system to go into the models that we were talking
6 about, specifically some of the Markov models, and
7 even the dynamic flow-graph models. So the two
8 parameters of interest to us as fault injection
9 experimentalists are coverage, and we define coverage
10 as the probability that an error detection mechanism
11 or a fault detected given that a fault has occurred in
12 the system is what we typically define as coverage.
13 That is of importance to us because that also defines
14 how well the system is responding to specific types of
15 faults and fault classes.

16 Traditionally, fault injection has really
17 addressed the issue of hardware-type faults, and other
18 types of faults. There is work, and like Steve said,
19 we're trying to transition this into the area of
20 certain types of possibly design-type faults. That is
21 certainly something that we are working with this
22 committee to kind of address that. And more
23 importantly, I think what Dr. Apostolakis said, that
24 we really need to be mindful of, is we really need to
25 state what the assumptions are behind all of the

NEAL R. GROSS

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

1 models that we're creating here, the data that is
2 going into those models, and how that data has to
3 instantiated into models to get credible results out
4 of the system. And so one of the things that we have
5 been doing at the University of Virginia is trying to
6 develop a process by which these assumptions are
7 explicitly stated. And we probably haven't done a
8 great job of presenting that here today, but I wanted
9 to state that that is a very, very important part of
10 the research, to be very, very rigorous and scientific
11 about how this information is generated, what
12 assumptions are made there. And more importantly, can
13 those assumptions be challenged and discharged with
14 credible evidence.

15 CHAIR APOSTOLAKIS: Now the definition
16 that is given in the report, for an example it says,
17 "Say we inject 100 faults into the feedback loop, and
18 we get two erroneous responses that were not detected
19 by the system, then the non-coverage one minus C for
20 that failure model is .02 ratio, and the coverage is
21 .98." So the idea then of C is that you inject the
22 number of faults addressing a specific potential
23 failure mode?

24 MR. ELKS: That's correct.

25 CHAIR APOSTOLAKIS: Which you don't know

NEAL R. GROSS

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

1 in advance.

2 MR. ELKS: Well, one of the things that
3 Steve had me do early on in this project is to try to
4 look at what I call generic failure mode taxonomy of
5 INC systems, which would help us identify what are the
6 important failure modes of this particular system, so
7 that we could have some guided representation of
8 exactly where to go into the system and inject these
9 types of failures.

10 There are a number of different ways to
11 conduct fault injection campaigns. One of them is
12 what I call this guided fault injection. We're
13 actually looking at particular hazards of the system
14 that are either known, postulated, or some other
15 theoretical method to say we need to look at this and
16 go into the system and try to stimulate those and see
17 what the responses are.

18 There's what I call the old school method,
19 which is more random fault injection, where we
20 statistically just go in and perform fault injections
21 anywhere into the system and see what the response is.
22 That type of fault injection is somewhat fruitless
23 because you get a lot of non-responses out of the
24 system, because you might be putting faults into
25 spaces where the program is not executing. You might

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 be putting it into spaces where there is actually no
2 -- the timing and the actual data do not line up so
3 that you'll get a response.

4 What we have tried to do at the University
5 of Virginia is to use a combination of those two,
6 based upon the information that comes from the system
7 plant engineers who tell us, what is the most -- what
8 do you worry about the most happening with this
9 system? Give us your most dangerous fault list, so to
10 speak. That's what I call it.

11 When I go in and talk to plant engineers
12 or system engineers, I want them to give me this type
13 of information so that I, as an experimentalist, and
14 as a system analyst, can begin looking at the
15 hardware/software interactions of the system to
16 determine what types of things could go wrong to
17 produce that most dangerous fault list.

18 CHAIR APOSTOLAKIS: Okay. If we pursue
19 this example a little further, you inject the 100
20 faults.

21 MR. ELKS: Yes.

22 CHAIR APOSTOLAKIS: Ninety-eight of them,
23 the system becomes aware of them. That's what you
24 mean.

25 MR. ELKS: It's detected by the error

NEAL R. GROSS

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

1 detection mechanisms.

2 CHAIR APOSTOLAKIS: How do I calculate
3 this transition rate lambda?

4 MR. ELKS: You don't get transition rate
5 lambda out of fault injection experiments.

6 CHAIR APOSTOLAKIS: Oh, okay.

7 MR. ELKS: What you get out -- you
8 essentially get the coverage.

9 CHAIR APOSTOLAKIS: How do you get the
10 transition rate?

11 MR. ELKS: The transition rate is input to
12 the model. It really has nothing to do with the fault
13 injection campaigns. The fault injection campaigns
14 are strictly -- it's a stimulus response-type of
15 testing-type thing. I'm trying to test the error
16 detection mechanisms in the system to determine if
17 they can detect certain types of faults.

18 CHAIR APOSTOLAKIS: So Table 2.4.1 then,
19 the dependability parameters for the DFWCS system,
20 where do these come from? I mean, I understand now
21 where the Cs came from, where did the lambdas come
22 from?

23 MR. ELKS: The lambdas come from,
24 basically, talking with the plant engineers.

25 CHAIR APOSTOLAKIS: Oh, they're expert

NEAL R. GROSS

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

1 opinions?

2 MR. ELKS: Collected on actual collected
3 failure data rates, and also from the RAC Prism
4 database of those two, so they're estimates based upon
5 actual data, and actual database data.

6 CHAIR APOSTOLAKIS: It would be useful to
7 see what data are used to produce this at some point.

8 MR. ELKS: This also opens up another
9 issue. I think Dr. Apostolakis talked about this, was
10 the viability of the failure rate data. I mean, these
11 particular numbers that we have here come from both
12 historical plant data, and out of a commercial
13 database. It is known that these types of failure
14 rates have a certain amount of uncertainty to them,
15 because they're taken across a wide spectrum of
16 applications, and everything like that. So when we
17 typically do our analysis, either reliability or
18 safety analysis, we do sensitivity analysis also with
19 respect to some of these failure rates and coverage
20 rates to see where the system is most sensitive to a
21 particular failure rate, or a particular coverage
22 rate, because that is also information that you can
23 feed forward into the process to say this particular
24 component has a failure rate, but if we vary that
25 failure rate, the system reliability is impact

NEAL R. GROSS

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

1 greatest on this particular two parameters, so it's
2 also a way of determining certain other aspects of the
3 system that you just don't plug numbers into the model
4 and get a number out. You kind of have to look at it
5 in also in kind of what I would call a qualitative
6 way.

7 CHAIR APOSTOLAKIS: So it seems to me that
8 a very important question we have to address at some
9 point is these lambdas.

10 MR. ELKS: Yes.

11 CHAIR APOSTOLAKIS: How they relate to
12 what Brookhaven is doing, or other information, or
13 whatever.

14 MR. ARNDT: We will at our next meeting
15 have a specific session on data, both in terms of
16 what's out there --

17 CHAIR APOSTOLAKIS: That mic is not
18 working.

19 MR. ARNDT: We'll take as an action for
20 our next meeting to have a specific session to talk
21 about both what the data is out there, how we propose
22 to use the data for our own internal independent
23 validation methodology, and issues for the regulatory
24 guide on data. And we'll talk about this, we'll talk
25 about the more generic data work that Brookhaven is

NEAL R. GROSS

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

1 doing, and roll that in. You'll get some of that in
2 the discussion later this afternoon, but we'll take an
3 action to have a specific session on that next time.

4 CHAIR APOSTOLAKIS: Very good.

5 MR. ELKS: So I guess the last final thing
6 I would like to say is this issue between the
7 hardware/software interaction. The way that we inject
8 faults into the system can be represented as some type
9 of corruption of a register file and a microprocessor,
10 or anything. And we typically represent that as kind
11 of like some type of hardware failure in a
12 microprocessor, and I'm using a microprocessor as an
13 example here as something that we inject faults into.

14 In addition, we can also kind of represent
15 - there's two ways to kind of represent sort of
16 software-type failures, and those have to do with sort
17 of like constructs that could be into the system that
18 are activated by certain types of profiles that are
19 going on in the system, as well. That's two different
20 distinctions that we make. And the third thing that
21 I would like to make is, is that as you're conducting
22 this experiment, as I'm going through injecting errors
23 into the system and everything like that, there's a
24 very likely, and we've seen this at the University of
25 Virginia, and I've seen it at NASA - it's very likely

NEAL R. GROSS

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

1 that you find that an error detection mechanism or
2 some other component of the system behaves in a way
3 that it wasn't intended. It's a specification error,
4 it's a design error at that point in time. And we
5 look at it and we go oh, okay. This is a true bug
6 into the system. So the technique addresses both
7 types of faults, but in a legacy sense, it originally
8 started out as hardware and has since transitioned in
9 to represent these hardware/software-type interaction
10 faults, as well.

11 CHAIR APOSTOLAKIS: Great. Thank you. So
12 this is an action item for the future.

13 MR. ALDEMIR: Well, what I'm going to
14 start talking about is the example PRA model that we
15 have adopted. And the reason for adopting a PRA model
16 is that eventually we would like to quantify the
17 effects of digital versus analog, or the effect of
18 switching over to a digital system on the overall core
19 malfrequency and the large early release frequencies.
20 The plant we chose is a NUREG 11.50 plant. It's a
21 three-loop design, and we are assuming that the
22 control system is applicable to each of the loops.

23 So the example, the event that is used in
24 this report that was being referred to is a turbine
25 three trip event. We talked about it earlier. This

NEAL R. GROSS

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

1 is the conventional event tree analysis of the event,
2 and since everybody is familiar with this procedure
3 here and the events, I'm not going to go through that.
4 But basically, we tried to keep the water level in the
5 steam generator using the oscillator feedwater system.
6 If it doesn't work, then we switch over to main
7 feedwater system, making the turbine active, and then
8 you have another number of sequence of events
9 following that, which are not going to be all that
10 much relevant to our example. This is the rest of the
11 turbine event tree, and as I said, as far as our
12 control system is concerned, we are not so much
13 concerned with this part of the event tree.

14 Now the methodologies we have identified
15 earlier, and these were among the conclusions of NUREG
16 69.01, is that the dynamic flow-graph methodology and
17 Markov methodology, and as distinct from what has been
18 discussed earlier with respect to Chapter 2 of this
19 report, that is a methodology to decide what sort of
20 faults to inject, and where to inject them. This
21 Markov methodology is to predict system reliability,
22 or rather, is a reliability model of the system, and
23 it needs input from the earlier discussion of data
24 generation.

25 The first methodology, dynamic flow-graph

NEAL R. GROSS

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

1 methodology, was developed by ASCA in the early 90s to
2 support risk assessment. The software was used in
3 safety analysis of several software control systems,
4 and the results validated dynamic flow-graph's
5 methodologies, ability to handle software/hardware
6 interactions, and to perform dynamic analyses,
7 specific applications, digital feedwater control
8 system in a pressurized water reactor which was
9 published as NUREG/CR 6465, control system for the
10 combustion module, one system of a shuttle experiment.

11 The important features, graphic modeling
12 environment and automated analysis engine that can
13 handle cause/effect relationships, time-dependent
14 relationships, feedback loops, the state vectors
15 represent key process parameters, and mapping between
16 the state vectors governed by multi-rated logic rules
17 which are represented through decision tables,
18 transfer boxes, transition boxes in the graphical
19 mode. And we'll see examples of these in a little
20 while.

21 Once you construct the DFM dynamic flow-
22 graph model, you can either analyze it inductively or
23 deductively. Now in the inductive mode, it's the
24 forward-tracking/discrete-event-simulation mode, you
25 are trying to identify the possible combination of

NEAL R. GROSS

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

1 components failures, even initiating event, and
2 deductively you are going backwards and given the
3 undesirable event you are trying to identify what sort
4 of event sequences have caused it. And you can
5 interrogate the dynamic flow-graph methodology model
6 several different ways, and again, as I indicated,
7 deductively/inductively. And also, there is another
8 mode that will come later on that will allow you to
9 decide what type of testing you can perform.

10 In the deductive mode, the software
11 identifies prime implicants, and these are distinct
12 from minimal cut sets in the sense that they are
13 multi-valued logical equivalent of minimal cut sets.
14 And, particularly, they become important when you have
15 the events - the importance of time-dependence of
16 events, like the example I told you. In fact, we have
17 identified - when I say we, I mean ASCA has identified
18 these two different failure modes that differed by a
19 second or so by using dynamic flow-graph methodology,
20 and I'll come to that in a little while.

21 This is a fairly standard approach.

22 CHAIR APOSTOLAKIS: The first bullet is
23 interesting. Do you have probabilities for all the
24 events that appear in the prime implicants? That's
25 multi-valued, right?

NEAL R. GROSS

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

1 MR. ALDEMIR: Well, the prime implicants
2 will depend on what sort of basic event, so to speak,
3 we have considered, what sort of failure modes, what
4 the state space consists of. So if we have data for
5 the state space, this will feed input -- this will
6 feed into the DFM. So basically, lambda times Delta
7 T, since we are doing discrete-event-simulation, is
8 going to give you those probabilities, the lambdas
9 that we talked about earlier times the time increment.

10 CHAIR APOSTOLAKIS: They don't rely on
11 transition rates here, do they?

12 MR. ALDEMIR: Well, in the quantification
13 process -- well, DFM you can use in different modes.
14 You can use it for qualitative analysis, get the prime
15 implicant, or you can quantify the prime implicants,
16 and they --

17 CHAIR APOSTOLAKIS: Then these will have
18 events such as this parameter is between A and B. And
19 there is a probability that that parameter is there.
20 Then at the next step, there is a transition
21 probability that a parameter moves to another
22 interval? That's where I get lost.

23 MR. ALDEMIR: Well, we are not -- okay.
24 That would be the initiating event, distribution. Now
25 if we're talking about - if the system states include

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 parameter values being in certain intervals, and are
2 you referring to the dynamics of it, or are you
3 referring to the modeling parameters?

4 CHAIR APOSTOLAKIS: All the parameters are
5 selected at the beginning.

6 MR. ALDEMIR: Okay. So we're talking
7 about the modeling parameters --

8 CHAIR APOSTOLAKIS: Yes. Yes.

9 MR. ALDEMIR: -- that represent the
10 dynamics. At this point, neither of these
11 methodologies - well, I have to clarify that later on
12 - Markov does it a little bit the way I'm going to
13 define it, but that is not our emphasis in the
14 modeling. We're assuming that those are given. Now
15 what would happen if they change would be the subject
16 matter of a sensitivity analysis.

17 CHAIR APOSTOLAKIS: At some point it would
18 be useful to try to relate the prime implicants to the
19 states that you have in the Markov model.

20 MR. ALDEMIR: Actually, what we are
21 planning to do is compare the prime implicants --
22 actually, you will see in a little while that both
23 Markov methodologies, and I'm referring to the one in
24 Chapter 4 of the report, and DFM, are pretty much the
25 same thing. We can produce, the results of

NEAL R. GROSS

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

1 exchangeable. One has some advantage in a certain
2 area, and the other one has advantage in a certain
3 area, but we are doing pretty much the same thing. In
4 fact, what we are planning to do is to generate prime
5 -- Markov can generate prime implicants, as well. So
6 we will generate independently these prime implicants,
7 compare them, and resolve the differences. That's one
8 of the exercises that we are planning to do. We have
9 already done it in a partial way, but since we are
10 doing this independently purposefully so that we don't
11 influence each other, we have assumed different
12 initial conditions.

13 CHAIR APOSTOLAKIS: Does the Markov model
14 use multi-valued logic?

15 MR. ALDEMIR: Yes.

16 CHAIR APOSTOLAKIS: So you will have a
17 chapter at some point in the future where you will do
18 these things?

19 MR. ALDEMIR: In this report, we'll --
20 okay. The report is out for review right now, and it
21 will be revised, depending upon the reviewer comments.
22 And if this is a point that they also would like to
23 see, it's a matter of also timing issues. If there's
24 time, we will put this comparison in this one. It's
25 a matter of timing, actually, the deadlines. It's a

NEAL R. GROSS

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

1 matter of doing some of the analysis again.

2 Now if there is no time to do it for this
3 report, what we will definitely do is for the next
4 report, where we will quantify what qualitative
5 comparison and quantitative comparison, and resolve
6 the differences.

7 CHAIR APOSTOLAKIS: Maybe it would be wise
8 to include that comparison in this report, because if
9 this report is issued separately, then people may
10 assume that either methodology is fine, and the NRC
11 published it, so we can do it.

12 MR. ALDEMIR: Oh, I see what you're
13 saying.

14 CHAIR APOSTOLAKIS: But if you have a
15 comparison.

16 MR. ALDEMIR: Good point.

17 CHAIR APOSTOLAKIS: And also, a critical
18 evaluation of the rates. I think these things go
19 together.

20 MR. ARNDT: Yes. The idea is that this is
21 a staged approach. We looked at the various
22 methodologies that might be appropriate, we chose a
23 few that we thought would capture the characteristics
24 we were interested in, and how they could be
25 constructed, which is the purpose of this report. And

NEAL R. GROSS

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

1 then the next report will be how well those systems
2 actually work in doing these kinds of analyses.

3 CHAIR APOSTOLAKIS: What's the rush for
4 publishing this one?

5 MR. ARNDT: There's no rush. The point
6 is, before we go forward with the regulatory guide
7 saying these are ways that we think are acceptable,
8 and it's nice to be able to point to a document that
9 is in the public domain to articulate that.

10 CHAIR APOSTOLAKIS: But it seems to me
11 that you will be in a better position to define what's
12 acceptable if you do this comparison. Bill?

13 MR. KEMPER: Yes. Bill Kemper, again.
14 Thank you. Steve has kind of hit the nail on the head
15 here. We're really under internal pressure of our own
16 to try to move on with this and get some regulatory
17 guidance out there as soon as we can, because we think
18 the industry really is desirous of this. This series
19 of NUREGs, as Steve said, will provide the
20 underpinning or the regulatory bases, if you will, for
21 the Reg Guide itself. And also, we have an industry
22 public meeting coming up in August, which we've had to
23 slip a couple of times, and I'm hoping dearly that we
24 don't have to slip it again, so this plays into that,
25 as well. We want to have as much information out

NEAL R. GROSS

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

1 there available to the public before that public
2 meeting.

3 CHAIR APOSTOLAKIS: I still think, though,
4 that the critical evaluation of the failure rates and
5 position rates should be in this report.

6 MR. KEMPER: Well, what we can do is we'll
7 look at the time implications of that, and if we can
8 do it, Tunc, Steve, do you all see any reason not to
9 do that? I mean, assuming that it doesn't completely
10 washout our schedule here, obviously.

11 MR. ARNDT: The intention is all of these
12 issues will be covered by the time we finish with
13 third report. It's just a matter of which report and
14 what the exact timing is, and whether or not it
15 becomes logistically challenging to publish this
16 report with that information that may delay it so far
17 that it makes no sense to publish the third report.
18 There's logistical issues here, as well.

19 CHAIR APOSTOLAKIS: But if the source of
20 doubt regarding the applicability of Markov systems is
21 this meaning of the REGS, it seems to me you should
22 address it. I'm not asking for a major treatise, but
23 you should address it in the report, and acknowledge
24 that there is this issue, and here is our answer.

25 MR. ARNDT: We certainly need to

NEAL R. GROSS

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

1 acknowledge that it's an open technical issue, and
2 this is how we are choosing to work it, and this is
3 why.

4 CHAIR APOSTOLAKIS: So are you saying that
5 the regulatory guide will refer to these methods?

6 MR. ARNDT: It will reference this as
7 information, but as we've talked about about four
8 times already, there is going to be some systems that
9 don't need this sophisticated modeling, so that part
10 of it will reference other sections. But the
11 information we've learned in developing this
12 information is something that we want to use as a
13 technical basis for the decisions that we have in the
14 regulatory guide. If we say that there are some
15 systems that need this level of modeling, then we need
16 to point to both open literature and NRC literature
17 that says this is what our issues are.

18 CHAIR APOSTOLAKIS: Well, I mean, I
19 appreciate the issue of schedule and all that, but I
20 mean, certain things are really important.

21 MR. ARNDT: We appreciate the --

22 CHAIR APOSTOLAKIS: Do we comment on NUREG
23 reports? We do.

24 MR. THORNSBURY: Some.

25 MR. KEMPER: You can, but generally we

NEAL R. GROSS

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

1 don't ask that you do that.

2 CHAIR APOSTOLAKIS: But we can volunteer.

3 MR. KEMPER: You certainly can.

4 MR. THORNSBURY: You're a member of the
5 public, too, George.

6 MR. KEMPER: This is true, you are a
7 member of the public. Well, I think Steve's point
8 here is we will do what we can to address that and
9 move forward, try to preserve our schedule commitments
10 as best we can.

11 MR. ALDEMIR: We will also try to see if
12 we can have at least a qualitative comparison of the
13 prime implicants that we get from Markov and DFM.
14 That was already in the --

15 CHAIR APOSTOLAKIS: It's fine to have
16 something and then say more details will be somewhere
17 else.

18 MR. ALDEMIR: No, I think we have --

19 CHAIR APOSTOLAKIS: But not to say
20 anything is not really acceptable.

21 MR. ALDEMIR: If we are using the same
22 scenario to simulate it, it only stands to reason that
23 we compare the results, and try to resolve as many
24 difference as possible. It may not be possible to
25 resolve all of them, in which case we'll then defer to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the third --

2 CHAIR APOSTOLAKIS: By the way, I think it
3 needs a good editing job, this report.

4 MR. ARNDT: Yes. The version that you got
5 was a very early version. We wanted to provide you
6 the information for your technical background.

7 MR. ALDEMIR: The DFM analysis --

8 CHAIR APOSTOLAKIS: Say you have an actual
9 replication of this? Are you going to show the
10 actual --

11 MR. ALDEMIR: Yes. You want me to skip
12 all this?

13 CHAIR APOSTOLAKIS: Maybe you can go
14 there.

15 MR. ALDEMIR: Okay.

16 CHAIR APOSTOLAKIS: Because I don't think
17 this means anything to anybody who is not familiar
18 with the method.

19 MR. ALDEMIR: Okay. Let me first do kind
20 of -- anticipate where we are going, and as I said in
21 the beginning of my presentation, that we will
22 eventually need to integrate these models into an
23 existing PRA. So this is one way you can do the
24 integration, and we are using SAPPHIRE as the tool, and
25 the turbine trip event as the initiating event. You

NEAL R. GROSS

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

1 can, in the graphical mode, you can simply graphically
2 insert these types of -- the event sequences that have
3 been obtained through prime implicants into the event
4 tree. Then I will show you later on, and we
5 illustrated this for Markov - I'm sorry, the dynamic
6 flow-graph methodology, and then for Markov I will use
7 another mode of SAPHIRE input to show how we can
8 include them -- incorporate them into SAPHIRE. But
9 both methodologies can be used in both modes.

10 So example initiating event --

11 CHAIR APOSTOLAKIS: Let me -- let's go
12 back one second. This is a static representation of
13 the system.

14 MR. ALDEMIR: Right.

15 CHAIR APOSTOLAKIS: And you are doing a
16 dynamic analysis. So how am I to interpret the event
17 MFW phase? When?

18 MR. ALDEMIR: Okay.

19 CHAIR APOSTOLAKIS: Are you going to give
20 me a global event or what?

21 MR. ALDEMIR: In this particular -- that's
22 a very valid point. In this particular illustration,
23 the timing doesn't matter. The event sequences, I
24 mean, the prime implicants, the timing is not an issue
25 here. So if that's not an issue, then we can take it

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 simply incorporate it statically into a fault
2 tree.

3 CHAIR APOSTOLAKIS: It's not an issue?

4 MR. ALDEMIR: In this particular example
5 that we're talking about.

6 CHAIR APOSTOLAKIS: So why are we using
7 dynamic --

8 MR. ALDEMIR: No, no. We chose an
9 initiating event, example initiating event. Now in
10 this situation, we have two types of responses, either
11 the system behaves and fails in one mode versus the
12 other. So we get the prime implicants that lead to
13 these events. Now there are - I forgot the number,
14 but there are about 11 implicants, prime implicants
15 that lead to one type of failure, and then five, six,
16 or seven that lead to the other. We conglomerate them
17 so you have top event failure - I mean, sorry - high
18 level or low level.

19 Now, again, coming back to why are we
20 doing this dynamically? Well, you may be able to
21 identify the faults, I mean, the failure modes. And,
22 in fact, you have to specify them up front what sort
23 of failure modes you're going to have. The question
24 is, when you start quantifying them, unless you take
25 the dynamics into account, you may get different

NEAL R. GROSS

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

1 results.

2 CHAIR APOSTOLAKIS: But then how far you
3 will go into time? I mean, this still says failure of
4 the main feedwater --

5 MR. ALDEMIR: These are all valid issues.

6 These are --

7 CHAIR APOSTOLAKIS: Are you going to say
8 I'm going to 100 seconds, 50 seconds?

9 MR. ALDEMIR: These are all valid --

10 CHAIR APOSTOLAKIS: Is it possible that
11 you may even create another branch?

12 MR. ALDEMIR: These are all valid issues.

13 CHAIR APOSTOLAKIS: So we haven't resolved
14 those yet.

15 MR. ALDEMIR: No.

16 CHAIR APOSTOLAKIS: Okay.

17 MR. ALDEMIR: In fact, some of them are
18 not resolvable.

19 CHAIR APOSTOLAKIS: Whoa, whoa. We're not
20 squaring the circle here.

21 MR. ALDEMIR: Well, the issue is the
22 following. If you have an existing PRA based on a
23 static model, you generate the dynamic model. All
24 these issues that you brought up are valid. Well,
25 then you have to make certain assumptions. For

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 example, you look at the event tree and they say how
2 was this generated? What was my assumption on the
3 initiating event here? And then you go back to your
4 dynamic model and use the same initiating event, then
5 things will match.

6 CHAIR APOSTOLAKIS: But you will address
7 this some time in the future.

8 MR. ALDEMIR: That's why we are doing it
9 in the third report. That's why --

10 CHAIR APOSTOLAKIS: Well, that's the
11 thing, again. I mean, if you issue this report and a
12 guy tries to make some real life decisions using this
13 as a basis, and then this question comes to his or her
14 mind, I mean, how useful is the report? I mean, there
15 are important issues that have to be addressed.

16 MR. ALDEMIR: Again, we are assuming that
17 the existing PRA does not change, we cannot change
18 that, so the question is how can we fit it best into
19 the existing PRA. So one way - and all these issues
20 that you brought up are relevant, so then we look at
21 how the original PRA was constructed, and try to make
22 the same assumptions in our representation.

23 CHAIR APOSTOLAKIS: Will you at least have
24 in your conclusion section a discussion of these
25 issues, without necessarily giving an answer?

NEAL R. GROSS

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

1 MR. ALDEMIR: Yes, sure.

2 CHAIR APOSTOLAKIS: Because, you know, a
3 user will feel much better if he appreciates or he
4 realizes that the authors of the report appreciated
5 these issues.

6 MR. ALDEMIR: As I expressed, how far you
7 are going to go, same thing with the event tree - I
8 mean, you come to a stop when you reach a consequence
9 of interest to you, and the same thing you can do
10 this. You can do it for the dynamic methodologies,
11 you can follow them as far as the events in the event
12 tree go.

13 CHAIR APOSTOLAKIS: That's one approach.

14 MR. ALDEMIR: Yes, I mean that's one way.

15 CHAIR APOSTOLAKIS: That makes sense.

16 MR. ALDEMIR: But a key issue here is,
17 when you are tying up these links, am I making the
18 same assumptions in the linkage. And then you have to
19 see what the initial assumptions were in the event
20 tree generation so that you generate your dynamic
21 methodology or dynamic event tree the same way. And,
22 of course, you may need to -- if you have no
23 information, what if you have no information? Then
24 you do a sensitivity analysis on the initial
25 conditions, try to see how much of a difference it

NEAL R. GROSS

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

1 will make as far as consequences and event development
2 goes, as to what assumptions you make in initial
3 events. But this is what we will defer to as
4 epistemic uncertainty.

5 CHAIR APOSTOLAKIS: Yes. Everybody refers
6 to it. Another thought occurred to me - there was a
7 question last time you guys were - I mean, Steve was
8 before the Full Committee - there was a question from
9 a member, or a comment, that universities really
10 produce methods and ideas and all that, but then there
11 is this extra step of making something operational,
12 where you need now the regulatory guides, guys, or
13 National Laboratory to take over and make it
14 practical. And, Steve, you said yes, that we are at
15 the stage we're producing ideas and methods, and there
16 will be a second step. But today, I get the
17 impression that you're going into regulatory guide
18 directly, without having this intermediate step, where
19 somebody actually uses these, trying to make it --

20 MR. ARNDT: We're going to talk a little
21 --

22 CHAIR APOSTOLAKIS: -- say "practical".

23 MR. ARNDT: We're going to talk a little
24 bit about that later in the afternoon. There's three
25 things you need to understand.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: There's a lot of
2 things I need to understand.

3 MR. ARNDT: From a structural standpoint.

4 CHAIR APOSTOLAKIS: Okay.

5 MR. ARNDT: We go back to my bubble chart.
6 One of the issues is developing a practical
7 independent assessment methodology for the NRC. In
8 that case, let's talk about that for 30 seconds. We
9 come up with the ideas, we look at the limitations, we
10 look at the advantages and disadvantages of various
11 methodologies, we look at the data, we come up with an
12 idea, then we transition that to the people who do
13 this for practical day-to-day basis, in our case, the
14 INL lab that runs the SAPHIRE and SPAR program. That
15 is part of the plan for that part of the program. And
16 we'll actually talk about that briefly today.

17 The other part is the development of
18 guidance as to what we consider to be acceptable for
19 review that the industry can bring in. We can do that
20 in one of two ways. We can develop it and say this is
21 an acceptable methodology, and go through all the gory
22 details of what we think is acceptable or not, or we
23 can write basically a performance-based regulatory
24 guide that says we don't care what methodology you
25 use, so long as it meets certain criteria.

NEAL R. GROSS

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

1 At this point, we're planning on going
2 down the second path, rather than the first path, for
3 a number of reasons. One, because there's a lot of
4 different ways to do this. We're looking at three,
5 the traditional fault tree/event tree methodologies,
6 the DFM and the Markov. There are others. We have
7 different characteristics, different aspects of that.
8 The work that we are doing to develop our own
9 independent assessment methodology will inform the
10 development of our regulatory guidance, and we will
11 point to some of that information as reasons why we
12 make particular decisions in our regulatory guidance.

13 CHAIR APOSTOLAKIS: Okay. It will be
14 exciting when we review the regulatory guide.

15 MR. ARNDT: For a whole bunch of people.

16 CHAIR APOSTOLAKIS: I can see people
17 getting very enthusiastic when you tell them find the
18 prime implicants.

19 MR. ALDEMIR: Do you want me to go through
20 the DFM model construction procedure? The idea is --

21 CHAIR APOSTOLAKIS: Well, keep going. I
22 don't know. We will stop you when we think --

23 MR. ALDEMIR: Okay. The idea is basically
24 a graph theory oriented approach. We take the
25 discretized process parameters as nodes, we represent

NEAL R. GROSS

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

1 them as nodes, and we have transfer function between
2 the nodes expressed as decision tables. So in this
3 chart, which corresponds to what I have described as
4 the example initiating event, it's DFM modeling of the
5 same event sequence, or the system, the part of the
6 system that involves that event sequence.

7 CHAIR APOSTOLAKIS: So where are the
8 control laws in this --

9 MR. ALDEMIR: Controls laws are going to
10 be going through the transfer boxes. It's going to be
11 represented as the decision tables --

12 CHAIR APOSTOLAKIS: Easy to develop
13 decision tables using control laws.

14 MR. ALDEMIR: Now, my understanding is,
15 actually, we can ask Mike --

16 CHAIR APOSTOLAKIS: Mike is here. Right?

17 MR. ALDEMIR: Why don't you come and
18 explain?

19 CHAIR APOSTOLAKIS: Identify yourself.

20 MR. YAU: Michael Yau, ASCA, Incorporated.
21 To answer Professor Apostolakis' first question
22 regarding the control laws, the key parameters in the
23 control logic are the ones highlighted inside the
24 green brackets.

25 CHAIR APOSTOLAKIS: Okay, on the left.

NEAL R. GROSS

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

1 MR. YAU: On the left. That's right.

2 CHAIR APOSTOLAKIS: So am I to understand
3 there is a decision table behind each of these symbols
4 there?

5 MR. YAU: Right.

6 CHAIR APOSTOLAKIS: And then you did what?
7 How did you develop these? I mean, you solved the
8 equations?

9 MR. YAU: Basically, I -- in the control
10 law translated into a software sub-routine, I supplied
11 a range of inputs for the sub-routine, and then from
12 the outputs, look at the outputs and then build the
13 decision tables from the relationship between the
14 inputs and the outputs.

15 CHAIR APOSTOLAKIS: And time comes into
16 this? I mean, the decision table, again, is a static
17 representation.

18 MR. YAU: Not necessarily. Decision table
19 can be a dynamic representation in the sense that you
20 supply the inputs at a time step before, and then you
21 get the outputs a time step later.

22 CHAIR APOSTOLAKIS: And that's time
23 independent? You see what I'm saying? No, it can't
24 be.

25 MR. ALDEMIR: It could be time

1 independent, if the system --

2 CHAIR APOSTOLAKIS: Could be, but --

3 MR. ALDEMIR: If the system is autonomous,
4 yes. If it is not, then they create another decision
5 table, basically.

6 CHAIR APOSTOLAKIS: And what's the time
7 step here, Mike?

8 MR. YAU: Right now in the model that we
9 are putting, it's assumed we are running -- the
10 decision tables were built based on time step of 10
11 clock cycles.

12 MR. ALDEMIR: In this example, the system
13 is not autonomous because the decay -- the heat
14 generation rate is an exclusive function of time, so
15 the decision tables will have to be built as a
16 function of time.

17 CHAIR APOSTOLAKIS: Have they been built
18 that way? I mean, that's an important point. I mean
19 --

20 MR. ALDEMIR: Yes.

21 CHAIR APOSTOLAKIS: They have.

22 MR. ALDEMIR: Well, Michael will help me
23 out, but this --

24 MR. YAU: Well, actually the decay heat
25 part is really part of the input to the software.

NEAL R. GROSS

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

1 It's the compensated power, and we -- in the input
2 used to generate the decision table, we sample a range
3 of the input power from zero percent to 100 percent,
4 so you have the representation, if the power is in
5 this range, we've got these set of outputs. If the
6 power is in a different range --

7 MR. ALDEMIR: They are basically
8 converting to the autonomous system in this situation.

9 CHAIR APOSTOLAKIS: Okay.

10 MR. ALDEMIR: So the decision table will
11 be static. But you can do it dynamically, so it's
12 just a matter of depending upon how the system
13 representation is.

14 MR. ARNDT: The real point here is the
15 level of detail you need in the model, be it this
16 model or any other, is dependent upon the amount of
17 the features of the system that you need to capture
18 for it to be an appropriately representative model.
19 So, for example, when we talked about the aspects of
20 the model, the watchdog timer, if the main computer
21 has a fault, it'll shift to the backup computer.
22 That's a time sequence. There's issues associated
23 with the characteristics of the system, so the amount
24 of timing you have and the amount of detail you have
25 is based on the amount -- the feature of the system

NEAL R. GROSS

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

1 you want to capture.

2 CHAIR APOSTOLAKIS: Yes, but at the same
3 time, if by capturing those features you come up with
4 a methodology that is completely unmanageable --

5 MR. ARNDT: Well, that's the point of
6 doing the study, to see whether or not you can do
7 that.

8 CHAIR APOSTOLAKIS: So this was
9 manageable, Michael?

10 MR. YAU: For this simplified benchmark
11 system, it is. But let's say if you have a more
12 complicated software module that models a common
13 filter, I don't think you can do a practical decision
14 table that way. I think you have to rely on some
15 clever method of dividing the input space into
16 different contexts, and then rely on testing to build
17 the decision table.

18 CHAIR APOSTOLAKIS: I see. There's a way
19 around.

20 MR. YAU: There's a way around, yes, sir.

21 CHAIR APOSTOLAKIS: Okay. Let's go on.

22 MR. ALDEMIR: Since you are here, why
23 don't you step through these.

24 MR. YAU: So, basically, from the DFM
25 model that was constructed to represent the feedwater

NEAL R. GROSS

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

1 control system and the steam generator, we could
2 analyze this model for different top events. The two
3 top events of interest are the steam generator at a
4 high level, and the steam generator at a low level.
5 These top events were defined as a conjunction of the
6 state of the knocks represented by the DFM model, and
7 the top event that this third bullet corresponds to is
8 the high level top event.

9 The level was discretized into five
10 states, two, one, zero, negative one, and negative
11 two; two being the highest, and negative two being the
12 lowest. What this top event says is that I want to
13 find out what are the prime implicants that could lead
14 me to the highest level at time zero, while passing
15 through level one at time T minus 1, and starting from
16 the normal level at T minus 2. Given that the ELP and
17 the CZL variables are zero, that means you don't
18 accumulate a lot of errors inside the PID control
19 logic. There are not a lot of integral errors in the
20 control logic, so you're basically starting from a
21 very nominal state, and then somehow progress to the
22 high level. And then the DFM model was analyzed
23 deductively for two time steps for that top event, and
24 the 11 prime implicants were identified.

25 CHAIR APOSTOLAKIS: So this is now for

1 what time, [^]time zero? The 11 prime implicants at
2 which time?

3 MR. YAU: At time minus two. We were
4 backtracking two time steps, so our top event occurs
5 at time zero. But we find out things that happen
6 before --

7 CHAIR APOSTOLAKIS: You go back two times,
8 yes.

9 MR. YAU: Right. Before.

10 CHAIR APOSTOLAKIS: So 11 prime implicants
11 for time zero.

12 MR. YAU: Right.

13 CHAIR APOSTOLAKIS: Right.

14 MR. YAU: And then --

15 CHAIR APOSTOLAKIS: And did you guys find
16 this 44 second --

17 MR. YAU: No. Actually -- the fact is
18 that these prime implicants, they don't tell you
19 exactly okay, this thing happens at 44 seconds. It
20 just gives you the initial condition, and one of those
21 initial conditions [^]corresponds to the 44 second case.
22 Let's say we focus on prime implicant number 5, it
23 says the level was normal at time T minus 2, the level
24 error is nominal, the compensated level is nominal.
25 But then at that moment, the feed flow is greater than

NEAL R. GROSS

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

1 the steam flow, and then your bypass flow valve failed
2 stuck. And that's the condition at 44 seconds,
3 because at that moment feed flow is greater than steam
4 flow, and if your bypass flow valve got stuck, then
5 the feed flow/steam flow mismatch will lead you to a
6 high level. That's basically what the prime implicant
7 tells you. It doesn't tell you that you have to look
8 specifically at 44 seconds, but you have to look for
9 cases where the steam flow and the feed flow mismatch,
10 and then you can have a stuck position.

11 CHAIR APOSTOLAKIS: Now you report the
12 probability here of 2.5 ten to the minus 4, not there,
13 in the report.

14 MR. YAU: We removed those, because
15 basically those numbers were assumed numbers, and we
16 subsequently removed those.

17 CHAIR APOSTOLAKIS: All right. I was
18 trying to find out why they're in the --

19 MR. ALDEMIR: No, we removed those
20 numbers.

21 MEMBER BONACA: Forget it now.

22 MR. YAU: Those numbers are basically used
23 to illustrate how you could go from the prime --

24 CHAIR APOSTOLAKIS: Okay. Let's say you
25 want to quantify this, again, prime implicant five,

NEAL R. GROSS

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

1 level is normal at T minus 2. That's one, right. I
2 mean that's -- yes, really normal is one.

3 MR. YAU: I think you could get those
4 numbers from the operational profile. The level may
5 be --

6 CHAIR APOSTOLAKIS: A very high
7 probability of --

8 MR. YAU: Yes, that's right.

9 CHAIR APOSTOLAKIS: Level error is
10 nominal.

11 MR. YAU: It comes from the operational
12 profile in the software. Basically, you accumulated
13 a very small error, and you can easily correct this.

14 CHAIR APOSTOLAKIS: You can have a
15 probability for that?

16 MR. YAU: I don't know how to generate
17 that, at the moment.

18 CHAIR APOSTOLAKIS: Ahh, okay.
19 Compensated level is nominal. Tunc, you want to say
20 something?

21 MR. ALDEMIR: These are initial
22 conditions, basically.

23 CHAIR APOSTOLAKIS: All of these are
24 initial -- yes, but --

25 MR. ALDEMIR: Blue are initial conditions.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: Why are they initial?

2 MR. ALDEMIR: Because you have third order
3 system, you need three initial conditions.

4 CHAIR APOSTOLAKIS: If it goes back two
5 steps. Okay, fine. But still -- okay, so these are
6 -- feed flow greater than steam flow. That's red,
7 right? So that's not an initial condition. So how
8 would you get that probability?

9 MR. YAU: We don't have an answer right
10 now, but I would venture to speculate that you would
11 try to quantify it by looking at the operational
12 profile and see how the steam flow and feed flow
13 profile under this initial condition.

14 CHAIR APOSTOLAKIS: So we do have some
15 issue here how to get those probabilities, so the main
16 value of this is the qualitative --

17 MR. YAU: Qualitative at the moment.
18 That's right.

19 CHAIR APOSTOLAKIS: What it takes, what
20 kind of states it takes to lead to the undesirable
21 event.

22 MR. YAU: Right. As Professor Apostolakis
23 pointed out earlier, from this qualitative analysis,
24 you might want to really fix these kind of issues
25 before even you try to quantify them. You may want to

NEAL R. GROSS

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

1 have some check --

2 CHAIR APOSTOLAKIS: And then you have the
3 same problem like everybody else.

4 MR. YAU: That's right.

5 CHAIR APOSTOLAKIS: The only thing you can
6 do is just assume some rates. If other people can do
7 it, you can do it.

8 MR. ALDEMIR: Again, they had such -- how
9 you would get the number, operational profile, you
10 need some input data, like in any other initial event
11 --

12 CHAIR APOSTOLAKIS: Well, what do you mean
13 by "operational profile"?

14 MR. ALDEMIR: How many times have you
15 observed this kind of event.

16 CHAIR APOSTOLAKIS: At T minus 2, zero.

17 MR. ALDEMIR: No, no. No, no.

18 CHAIR APOSTOLAKIS: Oh, come on.

19 MR. ALDEMIR: How many times have you
20 observed feedwater being - what is it - feed flow
21 being larger than steam flow? The minus 2 is not
22 relevant here. It's just the probable distribution
23 that's relevant.

24 CHAIR APOSTOLAKIS: I don't know. We'll
25 have to think about that. That's certainly an input

NEAL R. GROSS

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

1 to it.

2 MR. ALDEMIR: But, I mean, you would
3 definitely need inputs. Again, the dynamic analysis,
4 like any other -- even with normal event tree efforts,
5 you would still need to observe or know how system
6 will behave as a function of time --

7 CHAIR APOSTOLAKIS: I understand that, and
8 I think right now, I think that the greatest value of
9 what you guys are doing is qualitative. That's my
10 view. And the jury is out whether the quantitative
11 information is realistic and practical. That's my
12 view. Two guys nod, two refuses to -- that's fine.
13 That's fine.

14 MR. ALDEMIR: If I start responding, this
15 is going to get into a more philosophical mode. In
16 any kind of engineering field, we do the best we can.

17 CHAIR APOSTOLAKIS: Oh, don't -- yes,
18 okay. Let's go on.

19 MR. ALDEMIR: I mean, we cannot say wait,
20 we don't have anything.

21 CHAIR APOSTOLAKIS: I understand.

22 MR. ALDEMIR: Okay. Should I go through
23 these fast, or are we --

24 MR. YAU: Actually, I could just skip
25 through them really quickly.

NEAL R. GROSS

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

1 MR. ALDEMIR: Well, you might as well say
2 a few words.

3 CHAIR APOSTOLAKIS: Let me understand this
4 T equals zero. So this is the actual start of the
5 transient, the zero, or is it your zero?

6 MR. YAU: My zero. It's not the start of
7 the transient.

8 CHAIR APOSTOLAKIS: It could be any time,
9 actually.

10 MR. YAU: Right.

11 CHAIR APOSTOLAKIS: Okay.

12 MR. YAU: Basically, what I'm saying is
13 that my top even time is this zero.

14 CHAIR APOSTOLAKIS: I understand. Why did
15 you choose to go back only two time steps, and not
16 three?

17 MR. YAU: Because in the simplified model,
18 I know that the level could go from zero to two in two
19 time steps, so that's the minimum number of time steps
20 required to get there.

21 CHAIR APOSTOLAKIS: I see. So there's
22 some logic.

23 MR. YAU: Right.

24 CHAIR APOSTOLAKIS: Okay. That's good.

25 MR. ALDEMIR: Should I --

1 CHAIR APOSTOLAKIS: Yes, let's skip now.
2 Remember, you have to finish at 12:00.

3 MR. ALDEMIR: I know. It's going to be
4 hard. Well, I will just then try to go through the
5 Markov methodology fairly fast. But before we start,
6 this is, again, a way to predict the system
7 reliability, so it's a predictive model. And what we
8 are using earlier was a kind of an inductive model to
9 figure out what kind of inputs, what kind of faults
10 we're supposed to be injecting, so these things are
11 totally disassociated, except that the former model,
12 the one that is used for fault injection, helps to
13 feed data into this model or DFM.

14 CHAIR APOSTOLAKIS: The discussion we just
15 had, with DFM, Mike produced the prime implicants,
16 which are qualitative insights into the system without
17 using any quantitative information. Can the Markov
18 model produce qualitative results without failure rate
19 numbers? ↘

20 MR. ALDEMIR: I'll show you. I'll show
21 you in a little while. It does. This is a recent
22 development, incidentally; developed as part of
23 another project. So in the Markov methodology, we --

24 CHAIR APOSTOLAKIS: Why do you call it
25 Markov?

1 MR. ALDEMIR: Because it's a Markov model.
2 I mean, the main -- we discussed this with other
3 member of ASCA, and the main difference between two
4 methodologies is, in the decision tables they assume
5 zero one, we assume non-zero values, as well, non-
6 zero/non-one, we're in-between, as well. That's the
7 only difference.

8 CHAIR APOSTOLAKIS: But the problem --
9 what I don't understand is this. In the Markov
10 model, you start with a Markov diagram, which you
11 build. Correct? The states.

12 MR. ALDEMIR: Yes. But the same states go
13 into DFM, too. They have to --

14 CHAIR APOSTOLAKIS: Well, in there is the
15 truth tables?

16 MR. ALDEMIR: Well, you need to have some
17 certain states of the system so that you can figure
18 out what possible -- to construct your decision
19 tables, you need --

20 CHAIR APOSTOLAKIS: Well, I really think
21 you need a closing chapter with some of these things.

22 MR. ALDEMIR: As I said, we will do
23 comparisons. Now it is going to be difficult to
24 relate one to one, because then the report is going to
25 become unmanageable, because if you look at the

NEAL R. GROSS

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

1 report, we don't have too much on DFM because it's
2 already been out there. There's one NUREG already
3 published on it, 64.65.

4 CHAIR APOSTOLAKIS: Sure, sure, sure. But
5 some comparison, I think, would be useful on the basic
6 stuff. Yes, you see the experienced guy. Say yes.

7 MR. ALDEMIR: Okay. Yes.

8 CHAIR APOSTOLAKIS: But we are
9 experienced, too. We'll hold you to it.

10 MR. ALDEMIR: Okay.

11 CHAIR APOSTOLAKIS: You know, at this time
12 maybe going to details like cell-to-cell and all that
13 probably doesn't serve much of a purpose, so if you
14 can give us the flavor of the approach, because you'll
15 never finish, otherwise.

16 MR. ALDEMIR: Right. Okay. Let me then
17 give you the flavor of the approach, what I just said
18 earlier. I'll skip through these probabilities. So
19 this is going to be something -- sorry, go ahead.

20 CHAIR APOSTOLAKIS: The equations, the
21 control laws, how do you use them in the Markov model?

22 MR. ALDEMIR: As I said, the only
23 distinction between us - I mean not us - between
24 Markov methodology and DFM is how we construct the
25 decision tables. In our approach, in the DFM

NEAL R. GROSS

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

1 methodology, we use to one-to-one mapping, and correct
2 me if I'm wrong, Mike - one-to-one mapping, so it's
3 always zero or one. You still partition the process
4 variables into ranges, and then you take one point
5 from one end table, try to see where it will go
6 following the system equations in a given specified
7 time.

8 DFM uses one way, not because it's not
9 capable of using more than one, it's just that the
10 model becomes unmanageable. So in the Markov
11 approach, the same philosophy, except using more than
12 one point to start from each partition to map into
13 each partition, to other partitions. So when the
14 decision tables of DFM are zeroes and ones, Markov
15 produces decision tables which may have values in-
16 between. So that's the example that I was going --
17 this is kind of showing you how the mapping scheme is
18 done. This is our representation of the transitions
19 between each component state, between component
20 states. These go as inputs into the Markov model.
21 This is how you would construct these transition
22 probabilities from process variable --

23 CHAIR APOSTOLAKIS: Your cell-to-cell --

24 MR. ALDEMIR: Cell-to-cell mapping, that's
25 correct. This is the kind of decision table --

1 CHAIR APOSTOLAKIS: Go back one. I
2 remember in the report you say somewhere that some of
3 these factors can be obtained from look-up tables, or
4 am I - I don't remember correctly?

5 MR. ALDEMIR: It depends on the complexity
6 of the system. If the system -- the equations
7 describing the system dynamics is a convenient way of
8 -- well, one way of system modeling. You may actually
9 use look-up tables if you have experimental data on
10 system performance. Say that the system performance
11 is not that complicated, and you have -- let's say you
12 know that if I am in this interval, I will be in that
13 other interval based on experimental data, based on
14 observation, based on expert judgment, if you want to.

15 CHAIR APOSTOLAKIS: Otherwise, you produce
16 it?

17 MR. ALDEMIR: Otherwise, you can produce
18 them through the -- I mean, you just need a system
19 model, whether it be qualitative, quantitative,
20 doesn't really matter, integral, differential
21 equation, as long as you can map one time step to the
22 other time step, and both methodologies do the same
23 thing, both DFM and Markov do the same thing.

24 CHAIR APOSTOLAKIS: All right. Let's go
25 on.

1 MR. ALDEMIR: This is the kind of decision
2 table that you will build, and from what I understand,
3 DFM does pretty much the same thing. The differences
4 you see are here. These are not all zeroes and ones.
5 There are probabilities associated with these
6 transitions. And it's not because DFM cannot do it,
7 it's just that the model becomes very complicated.
8 They choose usually not to do it.

9 CHAIR APOSTOLAKIS: This is the kind of
10 thing that would be nice to explain a little bit in
11 the report. I really think it would go a long way --

12 MR. ALDEMIR: The similarities, we --

13 CHAIR APOSTOLAKIS: Similarity, why you
14 have .33 and they don't. I mean, it's not a big deal.

15 MR. ALDEMIR: Sure, sure. No, there's no
16 problem with that, no.

17 CHAIR APOSTOLAKIS: Within half an hour,
18 can't you --

19 MR. ALDEMIR: No, no, no. Actually, as I
20 said, we are planning to do --

21 CHAIR APOSTOLAKIS: No, refer to that you
22 cannot do it, or what? It cannot be done?

23 MR. ALDEMIR: No, we will do it. We were
24 planning to do it, as I said, after the -- we are
25 waiting for the reviewer's comments to come in. When

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 we are revising the report, we will compare these
2 methodologies and try to resolve as many differences
3 as possible.

4 CHAIR APOSTOLAKIS: The question in my
5 mind is, and I know you've answered a few times but
6 it's not clear, probably because I don't understand
7 this. It seems to me that the DFM guys can produce
8 qualitative results that are useful without resorting
9 to any probabilities or transition rates, and you
10 can't. Now you say that you can, so that's something
11 that I would like to see.

12 MR. ALDEMIR: You can see these -- you can
13 regard each of these squares as a placeholder, non-
14 zeroes as placeholders. You can regard them, if you
15 want to make your life simple, we can regard them as
16 ones, any time you have a non-zero probability, and
17 that tells you how we can do that qualitatively. This
18 is the --

19 CHAIR APOSTOLAKIS: Arabic.

20 MR. ALDEMIR: Well, hopefully these are
21 all going to be Meccanite. Incidentally, what we are
22 doing here --

23 MR. HICKEL: It's Greek, George. It's
24 Greek.

25 CHAIR APOSTOLAKIS: If it looked Greek to

1 me it would be okay.

2 MR. ALDEMIR: It's too small, and the
3 resolution isn't that good, but these are lambdas and
4 mus, which is Greek, yes. So eventually, the reason
5 why we called it Markov is because of this, and this
6 is a Markov process, and this has the properties of
7 Markov. But as you will see in a little while, we can
8 take this model, irrespective of the numbers we
9 produce, and we can generate dynamic --

10 CHAIR APOSTOLAKIS: That's what I want to
11 understand.

12 MR. ALDEMIR: Sure. Okay.

13 CHAIR APOSTOLAKIS: Now the last one that
14 has a word that is very popular, "importance".

15 MR. ALDEMIR: This is importance defined
16 after Lambert, but it is not one of the popular
17 importance, but it's Lambert.

18 CHAIR APOSTOLAKIS: Who is that? Is that
19 --

20 MR. ALDEMIR: Yes. This is from the paper
21 published in 1989, so it's old. We don't use it any
22 more, but --

23 CHAIR APOSTOLAKIS: Thesis.

24 MR. ALDEMIR: Pardon me?

25 CHAIR APOSTOLAKIS: That was his Ph.D.

NEAL R. GROSS

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

1 thesis.

2 MR. ALDEMIR: No, no, no, no. Lambert was
3 already working at that. Lawrence Livermore, I think.

4 CHAIR APOSTOLAKIS: Because it's typical
5 of students, he published the paper ten years later,
6 except for Mike here.

7 MR. ALDEMIR: This is, again, integration
8 process. How do we do that? DFM I had already shown.
9 Now coming to the point that interests you more, what
10 we do is that we take the transition matrix, and we
11 convert it into a dynamic event tree.

12 CHAIR APOSTOLAKIS: Who did that, the
13 DETs?

14 MR. ALDEMIR: The Markov model, the
15 transition matrix that --

16 CHAIR APOSTOLAKIS: I mean, who introduced
17 the term? I remember somebody.

18 MR. ALDEMIR: Dynamic event tree?

19 CHAIR APOSTOLAKIS: Yes. Was it you?

20 MR. ALDEMIR: We did. I don't want to
21 take undue credit, because I'm not too sure if it is
22 Amandela and the associates, or us, but somebody -- we
23 will use --

24 CHAIR APOSTOLAKIS: But Nathan Soo had
25 something else.

NEAL R. GROSS

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

1 MR. ALDEMIR: Yes.

2 CHAIR APOSTOLAKIS: What did he call it?

3 DETM.

4 MR. ALDEMIR: Well, DETM is -- again, the
5 word "dynamic" is there. Dynamic Event something - I
6 forgot what the T stood for.

7 CHAIR APOSTOLAKIS: So the time has come
8 for all these things to become useful?

9 MR. ALDEMIR: I would like to take this
10 opportunity to point out to the foresight of Professor
11 Apostolakis --

12 CHAIR APOSTOLAKIS: When was the work trip
13 you organized --

14 MR. ALDEMIR: 1992. Maybe it's not the
15 proper place, but I would like to acknowledge
16 Professor Apostolakis' foresight. If he had not
17 supported these activities through the Reliability
18 Engineering and System Safety, none of this stuff
19 would be here today. It would be very hard to
20 publish. I remember I spent about a year to publish
21 my first paper.

22 CHAIR APOSTOLAKIS: Flattery, but let's
23 keep going now.

24 MR. ALDEMIR: No, I really am serious
25 about it. It's not a flattery, but I am serious about

NEAL R. GROSS

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

1 this. Anyway, this is the -- we take the decision
2 tree - sorry, transition matrix - represent it in a
3 data structure of this sort, which corresponds to a
4 dynamic event tree like you saw. This is showing you
5 the actual data structure. This is on the left. It's
6 showing how the event tree is going to look like from
7 this data structure. Zeroes or Os stand for
8 operational modes, Xs failed modes, plus means high,
9 and I think -- no, plus means on and then X means off.
10 So these are -- the symbols here are showing the state
11 of the components, and how the system evolves. And
12 this is overflow, overflow.

13 I'll skip through these. These are the
14 algorithms that actually generate the trees.

15 CHAIR APOSTOLAKIS: Yes. Let's go to the
16 real thing.

17 MR. ALDEMIR: Well, this is how the event
18 tree looks like, basically, on the left.

19 CHAIR APOSTOLAKIS: That's it. I believe
20 you. No, what I'm saying is there is no doubt that
21 you have done your homework here. Take us to what
22 really matters. So your --

23 MR. ALDEMIR: Once we produce the event
24 trees - that we have done, pretty much - then the
25 question is how you take this, and then we have the

NEAL R. GROSS

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

1 input structure that is compatible with SAPHIRE.

2 CHAIR APOSTOLAKIS: And we still have that
3 problem how far to go, but as you said earlier, maybe
4 it's --

5 MR. ALDEMIR: There is another --

6 CHAIR APOSTOLAKIS: Or something else
7 happens.

8 MR. ALDEMIR: There are two issues here.
9 One of them is, are we matching what is already in the
10 fault tree through choice of initial condition,
11 duration of the scenario, and so forth. That is one
12 issue that can be resolved. The other part, how do we
13 process after we input this time dependent information
14 into the overall PRA, how do we process it, because
15 right now none of these techniques will see the time
16 dependence, including SAPHIRE, won't see the time --
17 they will immediately, the moment you start
18 constructing fault trees, all that time information is
19 lost. So we found a trick, so to speak, to process
20 this, and DFM is doing the same thing. We are time
21 stamping the events.

22 CHAIR APOSTOLAKIS: Why did you think it
23 necessary to give us a history of SAPHIRE, but it was
24 IRRAS.

25 MR. ALDEMIR: Completeness.

1 CHAIR APOSTOLAKIS: But I'm curious,
2 several modules were written to compliment IRRAS. Is
3 that correct?

4 MR. ALDEMIR: No, not compliment. That's
5 a misspelling. Complement with an E, not I. This is
6 -- at the beginning of the talk I said, we are using
7 the graphical input mode for DFM to illustrate how DFM
8 results can be incorporated into SAPHIRE. This is how
9 we can -- we are using the Markov model to illustrate,
10 still qualitatively only, no numbers - how we can use
11 the textual mode of input to incorporate the event
12 tree into SAPHIRE. And this is the actual file, this
13 is actual SAPHIRE input. This is the event tree on
14 the left in detail.

15 CHAIR APOSTOLAKIS: So, Steve, you said
16 earlier that, if I understand correctly, SAPHIRE
17 experts at Idaho will get involved at some point?

18 MR. ARNDT: Of course, since this is
19 research, if this proves to be practical and useful,
20 we will transition this to the people at Idaho. We're
21 already working with Curtis and other people.

22 CHAIR APOSTOLAKIS: But maybe on the way
23 of deciding whether it's practical, you should bring
24 them in a little bit and have them look at this.

25 MR. ARNDT: Oh, absolutely. Absolutely.

1 And part of Tunc's team includes people who work with
2 Curtis on internships, and other things, as well as -
3 I'll take a 20-second digression. Because this is a
4 both technically challenging and important issue,
5 we're doing extensive peer reviews of this work, and
6 Curtis, as it turns out, is one of the peer reviewers
7 of this work, so we're keeping the SAPHIRE people in
8 the loop in a number of different ways.

9 CHAIR APOSTOLAKIS: Okay.

10 MR. ALDEMIR: SAPHIRE people know exactly
11 what's going on. In fact, some of the algorithms that
12 were developed were developed within the scope of
13 another project. But the reason I wanted to show this
14 slide is to address the practicality issue. Suppose
15 I'm a utility and I don't want to get involved with
16 these fancy methodologies, how can I do it? Well,
17 this is one way.

18 We are also trying to generate the Markov
19 model -- how should I say - mechanize the Markov model
20 for generation procedure. DFM is already fail user
21 friendly, so once you generate the event trees, the
22 rest here - this is exactly how we would enter them
23 from a practical viewpoint. So it's not speculation,
24 you can actually do it.

25 What comes out of the SAPHIRE is a fault

NEAL R. GROSS

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

1 tree structure like this. Now these time events,
2 these events will have time information in them. It
3 is conceivable that that time information is
4 inconsistent, because SAPHIRE has no idea what's going
5 on except just looking at these. Each time stamped
6 event is another separate event, so you will need to
7 process the outcome to remove the inconsistencies.
8 And we do the same thing with DFM. This is exactly
9 step-by-step instructions as to how you would do, a
10 practitioner with SAPHIRE would be doing this, and we
11 have done it. I have two students right now working
12 with Curtis on these issues in Idaho.

13 So, again, I just indicated the steps to
14 show that it is doable. I have another 20 minutes,
15 maybe. Any questions on the methodologies? Can I
16 just -- okay.

17 CHAIR APOSTOLAKIS: I think we raised them
18 as we went along.

19 MR. ALDEMIR: Now the benchmark, when
20 Steve Arndt was talking about the benchmark problem,
21 he emphasized certain features of it, and some time
22 ago, about a half a year ago we published a paper in
23 PSA '05 as to what requirements a benchmark model
24 should have that it is representative of the digital
25 technology as it exists today, and as it relates to

NEAL R. GROSS

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

1 nuclear reactors. And it's a fairly busy slide. I'm
2 not going to go through every item, but two distinct,
3 two main items are that we classify systems as loosely
4 controlled coupled systems, and tightly controlled
5 coupled systems.

6 Loosely controlled coupled systems are the
7 ones where the failure events may be statistically
8 dependent due to the process, as I showed earlier, how
9 the -- through the dynamics, or it can be through
10 direct wire connections, or communication networking.
11 So we defined a number of properties that the
12 benchmark system should have to test the effectiveness
13 of the methodology that is going to be used for
14 digital system evaluations. And the benchmark problem
15 satisfied most of the requirements. It is also a
16 practical system. It is representative of the
17 feedwater control systems you've been operating PWRs.

18 Some of the requirements that are less
19 relevant to systems used in nuclear reactor protection
20 systems are not represented by the benchmark system,
21 and as Steve Arndt pointed those out, networking, for
22 example, shared external resources. And two
23 particular challenging feature of the benchmark system
24 are that we have some of the fault tolerance
25 capabilities requires consideration of system history,

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 which is particularly challenging issue in reliability
2 modeling. And as I said, system failure mode may
3 depend on the exact timing of failure modes.

4 How do we meet the modeling requirements
5 that we have listed in NUREG 69.01, and again, I'm not
6 going to go through these, this graph. So just to
7 show how they meet them, first of all, requirement one
8 - neither methodology, it basically says that it
9 should not be based on purely operating experience.
10 In other words, you observe certain failures, you
11 build a failure model that only duplicates those, but
12 cannot really look into the future. You identify
13 failures modes, the only failure modes that you have
14 for the system are the ones that you observe for the
15 overall system, system configurations that lead to
16 failure.

17 CHAIR APOSTOLAKIS: But you should be able
18 to go to actual occurrences and convince --

19 MR. ALDEMIR: That's right.

20 CHAIR APOSTOLAKIS: -- yourself that you
21 could have found them.

22 MR. ALDEMIR: That's why I quoted the -- I
23 showed the artifact generation. We have actually --
24 we do have an artifact which we can predict it's
25 going to occur. And it did happen in real life, not

NEAL R. GROSS

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

1 for the exact same system, of course, but it shows the
2 potential of the methodology that it can. So both
3 methodologies can account for all the features of the
4 benchmark system. This is requirement two. Both
5 methodologies make valid and plausible assumptions.

6 CHAIR APOSTOLAKIS: That's where I need to
7 be convinced.

8 MR. ALDEMIR: Well, okay. That's why I
9 gave a little example here, a little footnote. For
10 example, I'll read this - "For example, the assumption
11 that the process dynamics can be represented through
12 a Markov transition matrix or a decision table of DFM,
13 have been validated through previous work, lots of
14 publications on this."

15 CHAIR APOSTOLAKIS: Have been, what did
16 you say, validated? Wow.

17 MR. ALDEMIR: Well, depends on how you
18 define the word "validated". Demonstrated, better
19 maybe. "Similarly, normal operation of the benchmark
20 system and its assumed failure modes were based on
21 operating PWRs, as well as other digital INC systems
22 encountered in practice. Both methodologies can
23 account for all the features of the benchmark system,
24 so the valid and plausible assumptions --

25 CHAIR APOSTOLAKIS: I really think I need

NEAL R. GROSS

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

1 to see solid arguments of the validation of the lambda
2 J. I really do.

3 MR. ALDEMIR: You're referring to the --

4 CHAIR APOSTOLAKIS: Transitions.

5 MR. ALDEMIR: Transitions.

6 CHAIR APOSTOLAKIS: Okay. Let's go on.

7 MR. ALDEMIR: Both methodologies can
8 quantitatively represent dependencies between failure
9 events accurately. And, again, assuming that the data
10 are correct, the modeling procedure is doing that, and
11 these are other types of failures that the models can
12 account for, intermittent versus functional. Both
13 methodologies yield information that is usable by,
14 let's say, a conventional methodology.

15 CHAIR APOSTOLAKIS: So your prime
16 implicants or cut sets have been compared to Mike's --

17

18 MR. ALDEMIR: That's what I said we are
19 trying to do.

20 CHAIR APOSTOLAKIS: Oh, you're trying to
21 do. Okay.

22 MR. ALDEMIR: That is something that we
23 should be -- we can do this qualitatively. Well, we
24 tried to resolve the --

25 CHAIR APOSTOLAKIS: No, I'm not talking

NEAL R. GROSS

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

1 about the numbers. I'm talking about here is what
2 they found.

3 MR. ALDEMIR: Right.

4 CHAIR APOSTOLAKIS: Eleven prime
5 implicants that Mike mentioned. Here is what we
6 found, and if we look at them, they're almost the
7 same.

8 MR. ALDEMIR: Right. Well, we'll do that
9 . We'll do that.

10 CHAIR APOSTOLAKIS: Okay.

11 MR. ALDEMIR: Okay. Also, they yield
12 enough information, or they model the system in such
13 sufficient detail and completion that the non-digital
14 IC system portions of the scenario can be properly
15 analyzed, and so we are not just concentrated on
16 software issues, and that relates to the question
17 raised earlier. Well, this is what we would observe
18 in the analog systems, as well. True, but the
19 combination may produce new results.

20 CHAIR APOSTOLAKIS: So you guys are taking
21 now for granted that we are looking at the system
22 centric approach, right? This is what you're doing,
23 you're looking at the system itself, and the software
24 is just embedded in it.

25 MR. ALDEMIR: That's exactly right.

NEAL R. GROSS

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

1 That's the philosophy we have adopted in the
2 beginning. And, again, as Steve --

3 CHAIR APOSTOLAKIS: But for actuation
4 systems, that may not be what you want to do.

5 MR. ALDEMIR: Right. But this is
6 something that, again, how are we going to implement
7 --

8 CHAIR APOSTOLAKIS: I understand.

9 MR. ALDEMIR: This is a future issue, but
10 maybe in a kind of hierarchical fashion, use the
11 classical first, then use DFM, then you go to maybe
12 more detailed Markov, or maybe put DFM in the
13 probability mode.

14 CHAIR APOSTOLAKIS: Are there any plans to
15 look at very simple actuation systems?

16 MR. ALDEMIR: Yes, I think they do. The
17 second benchmark here we talk about those.

18 CHAIR APOSTOLAKIS: Okay.

19 MR. ALDEMIR: Now, challenges. They have
20 substantially steeper learning curves and more labor
21 intensive than conventional event tree/fault tree
22 methodology, but they can be alleviated by developing
23 user-friendly tools. And this is also in the further
24 future plans, not near future.

25 The other challenge, this has come up

NEAL R. GROSS

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

1 during this meeting through and through, is that the
2 failure data used by either methodology for
3 quantification not necessarily credible to a
4 significant portion of technical community. However,
5 as has also been pointed out, there are efforts to
6 remedy this. And also, both methodologies can be used
7 in a purely qualitative mode to obtain information
8 about the important failure modes of the system, even
9 the numbers are not relevant.

10 And, again, another requirement that we
11 would like to have is that the methodologies don't
12 require highly time dependent, continuous plant state
13 information, and these methodologies do. Depending on
14 what system we're talking about, if the physics are
15 there, if the process is complicated, there will be no
16 way around it. Otherwise, you are not representing
17 your system. We've got to do this. If, on the other
18 hand, the system is simple actuation system, you don't
19 need fancy dynamics and fancy methodologies, or a lot
20 of states.

21 We haven't even addressed in this problem
22 the communication issues, for example, in these
23 digital systems, for example, which may require a
24 large number of states. But if they don't, simple
25 actuation systems, maybe even the conventional method

NEAL R. GROSS

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

1 would work well. So in that respect, the hierarchical
2 approach could probably be better, use the standard
3 fault tree/event tree approach. You want to check
4 your results, go to the DFM, maybe, and then either
5 normal mode, probabilistic mode, or maybe go to a more
6 refined model. So these are, again, speculations as
7 to how we can practically implement and validate these
8 methodologies against each other. So, in other words,
9 kind of -- I don't know if validation is the right
10 word, or verification, but basically, to make sure
11 that the results that we are getting make sense.

12 And I think I'll just summarize and leave
13 it to Steve to talk about future work. So we have
14 basically specified a digital INC system that can be
15 used to evaluate methodologies proposed for the
16 reliability modeling of digital INC systems using a
17 common set of hardware/software/firmware states. The
18 benchmark system specification includes procedures for
19 system component failure mode identification and
20 failure data acquisition. By failure mode
21 identification, I mean we are doing an FMEA, and
22 that's in the report, as well.

23 We have used an example initiating event
24 to illustrate how these methodologies, the dynamic
25 flow-graph methodology and Markov methodology can be

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 used for the reliability modeling of digital INC
2 systems. We chose these methodologies because they
3 were identified as the more promising methodologies by
4 NUREG 69.01. And both methodologies can be used to
5 obtain qualitative, as well as quantitative
6 reliability information for digital systems.

7 We have discussed the possible challenges
8 with the methodologies, most of which can be resolved.
9 And, finally, and maybe very importantly, some
10 properties of the benchmark system considered in this
11 first, that it may not apply to all reactor protection
12 and control systems. So if for digital INC systems
13 which may have less complex interaction between the
14 failure events, the conventional event tree/fault tree
15 approach may be adequate for the reliability modeling
16 of the system.

17 CHAIR APOSTOLAKIS: At the workshop in
18 August, are you planning to present this to the
19 industry?

20 MR. ARNDT: Let me answer your question,
21 then talk a little bit about this issue. The workshop
22 in August is primarily going to be discussing what
23 needs to be, and what is appropriate for a regulatory
24 guide in this area. Obviously, this idea of a graded
25 approach to the kind of modeling that is necessary is

NEAL R. GROSS

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

1 one important part of that. It's not the only
2 important part, but is one important part of that.
3 And the philosophy, based on what we've learned so
4 far, will be discussed. I don't know if that answers
5 your question exactly or not.

6 CHAIR APOSTOLAKIS: How would the
7 stakeholders understand better what you guys are doing
8 here? You will give a draft of the NUREG out? No.

9 MR. ARNDT: Not at that point. We're
10 going to go through a process to both explain our
11 ideas, starting with the presentation this afternoon
12 and in the discussion in August, and then finally, the
13 draft Reg Guide that we sent out for public comment.
14 At the same time, get input in terms of both what they
15 consider to be practicable, as well as whether or not
16 they have significant technical problems with our
17 approach. So we'll lay out what we think is necessary
18 in terms of acceptance criteria and modeling detail,
19 and all the other issues that we talked about, as well
20 as a structure and strategy for what the Reg Guide
21 would look like.

22 CHAIR APOSTOLAKIS: When in August is
23 this?

24 MR. ARNDT: We haven't defined the date,
25 but we'll probably define that in the next week or so.

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

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: Okay. In terms of the modeling effort, the next steps, and we've talked about some of these and whether or not they should be incorporated in this document we're currently working on, or wait for the next document, we're going to be finishing the detailed reliability modeling of the full benchmark system, look at all the different prime implicants for all the different scenarios, same for the DFM and the conventional approach. We're going to do a qualitative comparison of the different modeling methodologies we've looked at. We're going to do a qualitative evaluation based on the data from field data, as well as the fault injection experiments. We're going to incorporate that into the selected PRA and look at not only can it be done, but how difficult is it in practice, and then we're going to do this again for a separate benchmark, which looks at the other end of the extreme.

The idea of defining two benchmarks is to get as many of the different characteristics as possible in the two different benchmarks. This is an important to safety but not safety system that is a control system that has a lot of dynamic interactions.

NEAL R. GROSS

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

1 The other benchmark, which is not defined yet, but is
2 the one that's going to be an actuation system, will
3 be a simpler system with less dynamics, but probably
4 higher redundancy and issues like that, because it'll
5 be a RPS, so it'll have different characteristics.
6 And from that information, we hope to be able to make
7 judgments, both in terms of our own modeling
8 capability and we will require in a regulated
9 application.

10 That's what we're going to talk about in
11 terms of the dynamic analysis. This afternoon we're
12 going to talk about some of the failure issues,
13 software failure analysis, software database, and a
14 little bit of the traditional PRA. And then at the
15 end of the afternoon, we'll have a short discussion of
16 where we stand in terms of our philosophy right now
17 for the Reg Guide, and then the industry wants to make
18 some oral comments.

19 CHAIR APOSTOLAKIS: Any questions from the
20 persons around the table? Members of the public,
21 comments, questions?

22 MR. ENZINNA: If you don't mind.

23 CHAIR APOSTOLAKIS: I don't mind at all.

24 MR. ENZINNA: I'm Bob Enzinna. I work at
25 AREVA in the PRA Department. I have some experience

NEAL R. GROSS

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

1 creating PRA models for large INC systems. One
2 comment. On your slide 51, you've got a matrix there
3 that fills the page. And I'm noting that this example
4 you have is fairly simple compared to what we have in
5 real plants. If you were to do that model on a system
6 that I've been working on recently, you'd need a much
7 bigger piece of paper. And I'm concerned about how
8 this would scale up to a large application, and I
9 implore you to test that thoroughly before you put
10 this out there and recommend its use.

11 CHAIR APOSTOLAKIS: Is your approach
12 available to the staff?

13 MR. ENZINNA: We can talk about that. I
14 can't make any commitments for my company without
15 talking to the people that own the systems, but
16 certainly, we're open to that.

17 The second comment I'd like to make, I'm
18 having trouble seeing how this dynamic stuff is going
19 to fit into my PRA. Ninety percent of what I need to
20 model, I think, in the PRA is the protection system,
21 the stuff that happens post trip. Most of this
22 dynamic stuff, the dynamic issues that you're talking
23 about seem to be applicable to control systems, like
24 the main feedwater you're talking about, stuff that
25 systems that mostly are out of the picture once the

NEAL R. GROSS

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

1 reactor trip occurs. Most PRA practitioners wouldn't
2 even attempt to model initiating event frequencies
3 with both in a model unless absolutely necessary,
4 because they're not good predictors. The best
5 predictor for that is data from operating history, and
6 I would propose that a reasonable approach for these
7 systems is to use historical data, use a conservative
8 value until we got some operating experience to
9 quantify those frequencies. I can't see putting a
10 detailed model like this in place to estimate
11 initiating event frequencies. And main feedwater, the
12 example you've chosen, you know, has some credit and
13 some accident sequences after trip, but it's not the
14 primary defense. It's a non-safety system. The thing
15 we're relying on the most in accidents like you're
16 talking about are EFW system, feed and bleed, things
17 that are safety assured, and are going to be actuated
18 by the operator, or by the protection system. Thank
19 you.

20 CHAIR APOSTOLAKIS: Thank you. Anybody
21 else?

22 MR. NGUYEN: Yes. My name is Thuy, and
23 I'm a loaned employee to EPRI from EDF, Electricity de
24 France. I have a question. The digital systems, of
25 course, do fail, and the research program you

NEAL R. GROSS

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

1 presented aims at modeling and understanding the
2 failures, but they also provide, I would say, nice
3 features that help in making the electro mechanical
4 equipment more reliable. Is this also part of your
5 modeling efforts and representing digital systems in
6 PRA?

7 MR. ARNDT: Yes. And there's two issues
8 associated with that. One is actually modeling
9 whatever system it is to the level of complexity
10 necessary to include the features that are important.
11 For example, some of the fault tolerant features, the
12 redundant features and other systems that are
13 specifically designed to increase the reliability of
14 the systems.

15 The issue there is, of course, data, but
16 also to some extent you trade the level of modeling
17 complexity with the amount of credit you want to give
18 to these systems that are specifically designed to
19 improve the reliability. So from a regulatory
20 standpoint, we have a bit of a challenge there,
21 because if we wish to take credit for the very good,
22 and in most cases very effective mechanisms that
23 modern digital systems have to increase their
24 reliability, fault tolerant systems, high quality
25 components, redundancy, and things like that, we also

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 have to find a mechanism by which to validate they're
2 operating correctly, and that they're being modeled
3 appropriately. So we are aware of that, we want to
4 include those features in our modeling, but the
5 challenge is by including those features in our
6 modeling, it adds to the complexity of the modeling.
7 So yes, we are aware of those issues, and are looking
8 at that as part of our research.

9 To go back to the earlier gentleman's
10 comments, we are aware that there is a large number of
11 systems that will probably be able to be modeled at a
12 less complicated level than what we're talking about
13 here. The point of this work is to understand where
14 those thresholds are, as well as understand what is
15 acceptable associated with modeling of the more
16 complex systems. The system we chose right here is
17 relatively simple in terms of the size of the system.
18 More complicated systems can be modularized and dealt
19 with in that way, if necessary, based on their
20 complexity, and what actions they take based on the
21 process. And I'm sure we will have some more
22 discussions about this at the end of the day.

23 CHAIR APOSTOLAKIS: Any other comments?
24 Okay. Thank you very much, Steve and Tunc, and
25 Michael and Carl. We'll recess until 1:00.

1 (Whereupon, the proceedings went off the
2 record at 12:01:37 p.m. and went back on the record at
3 1:06:09 p.m.)

4 CHAIR APOSTOLAKIS: Okay. We're back.
5 Steve, you want to introduce the subject?

6 MR. ARNDT: Yes. We're now going to have
7 a series of presentations led by Todd Hilsmeier, who
8 is working on some of the data issues, and also the
9 traditional reliability modeling methods, and some of
10 the folks from Brookhaven National Laboratory. And at
11 the conclusion of that part of the discussion, I'll
12 lead a short discussion of where we are on development
13 of regulatory guidance. With that short introduce,
14 I'm going to turn it over to Todd.

15 MR. HILSMEIER: Thank you, Steve. My name
16 is Todd Hilsmeier from Office of Nuclear Regulatory
17 Research, and Division of Assessment of Special
18 Project. And today, Louis Chu from Brookhaven
19 National Laboratory, Gerardo Martinez from Brookhaven,
20 and myself will be presenting development of a
21 probabilistic approach for modeling failures of
22 digital systems using traditional PRA methods.

23 The presentation outline will include a
24 background information review of the project plan that
25 we presented last year at the ACRS Subcommittee

NEAL R. GROSS

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

1 Meeting, then provide the status of the project, then
2 we'll go into the meat of the presentation, which
3 Louis Chu from Brookhaven National Lab will discuss
4 development of the failure parameter database for
5 hardware, and Gerardo Martinez and Louis Chu will
6 review the software failure events induced by software
7 faults.

8 Regarding background information, NRC has
9 a very comprehensive digital system research plan, and
10 part of that plan is to develop probabilistic failure
11 models for digital systems that can be integrated into
12 PRAs using dynamic and traditional PRA methods, as
13 Steve Arndt pointed out earlier in the day. And the
14 digital system PRA project, which is a project that
15 we're working on, uses traditional PRA methods to
16 develop probabilistic failure model for digital
17 systems. And this chart was presented earlier today
18 by Steve Arndt, and it shows the NRC's digital system
19 risk program. And as you see, NRC is developing
20 dynamic methods and traditional methods, and both
21 methods feed into the development of the regulatory
22 guidance.

23 And though we're working on these methods
24 in parallel, we're also working together to develop
25 the methods through exchange of information, through

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 peer review of each other's products, and through
2 meetings to make sure that we're on schedule and
3 meeting each other's needs.

4 Matter of fact, Bill Kemper and Steve
5 Arndt, they're, in my eyes, are our customer. And
6 because this project is very challenging, it's all
7 about team work. And tomorrow we have a technical
8 meeting between the dynamic group and traditional
9 methods group to discuss future steps of the project.
10 And then on Thursday, the dynamics group and
11 traditional group will be going to NASA to discuss
12 exchange of digital system data between the
13 organizations.

14 CHAIR APOSTOLAKIS: Which NASA are you
15 visiting?

16 MR. HILSMEIER: The headquarters with Dr.
17 Dezfuli and Mike Stamatelatos.

18 CHAIR APOSTOLAKIS: Stamatelatos.

19 MR. HILSMEIER: Yes. Thank you.

20 CHAIR APOSTOLAKIS: An easy name.

21 MR. HILSMEIER: So we're looking forward
22 to that meeting. This should be useful for both
23 projects.

24 The objective of the digital system PRA
25 project is to develop probabilistic failure model for

NEAL R. GROSS

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

1 digital systems using traditional PRA methods. And
2 also, the objective is to provide input into the reg
3 guidance on PRA modeling of digital systems.

4 This slide shows a high level summary of
5 the research plan using traditional PRA methods to
6 develop probabilistic failure model for digital
7 systems. And the detailed research plan, as I
8 mentioned earlier, was presented at ACRS Subcommittee
9 meeting last year, and tasks one and two involves
10 seeing how other industries model and manage digital
11 system reliability. And this task was completed and
12 presented at last year's ACRS Subcommittee meeting.

13 Task three involves documentation of our
14 results of our work, and that's ongoing. And task
15 four involves developing a failure mode effect
16 analysis, and dependency analysis for digital
17 feedwater control system, which is our case study.

18 CHAIR APOSTOLAKIS: Why not a fault tree
19 analysis?

20 MR. HILSMEIER: Excuse me?

21 CHAIR APOSTOLAKIS: That was proposed in
22 the mid-80s, right, to use fault tree analysis to
23 identify failure modes? Everybody keeps saying FMEA,
24 and I'm wondering why they leave fault trees out.

25 MR. HILSMEIER: We will be doing the fault

NEAL R. GROSS

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

1 trees during the development of the hardware and
2 software. The purpose of the FMEA is to learn and
3 understand the digital system.

4 CHAIR APOSTOLAKIS: Well, fault tree --

5 MR. HILSMEIER: Right.

6 MR. MARTINEZ-GURIDI: Well, in my mind,
7 also what happens, when you build a fault tree, you
8 already know what failure modes of the system are
9 there, and so you use the fault tree to combine them
10 to reach the top event. But before you build the
11 fault tree, you need to know how each component fails,
12 and what is going to be the impact on the system. So
13 I see FMEA as a preliminary step to the fault tree.

14 CHAIR APOSTOLAKIS: But you don't say
15 fault tree at all.

16 MR. HILSMEIER: But the fault tree is
17 actually a --

18 CHAIR APOSTOLAKIS: Put FMEA, fault trees,
19 all these things help you understand the system.

20 MR. HILSMEIER: Correct. Then task five,
21 six, and seven involves developing a probabilistic
22 failure model for the hardware of the system, with
23 task five involving development of the failure rate
24 database for hardware. And Louis Chu will be
25 discussing this task in detail. And then task six and

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 seven involves developing and quantifying the
2 probabilistic failure model for hardware using a fault
3 tree analysis. And tasks eight and nine involve
4 developing and quantifying a probabilistic failure
5 model for software, realizing that software is system
6 centric. With task 8A, reviewing system failure
7 experience induced by software faults, which Gerardo
8 Martinez and Louis Chu will be presenting in detail
9 today. And task 8A is completed, but is currently
10 being evaluated by NRC. The dynamics group is
11 evaluating our work along with myself. And the rest
12 of tasks eight and nine involve development of the
13 software reliability model, including answering
14 questions, are software failure rates meaningful, and
15 developing a linkage between software and hardware,
16 and quantifying the model.

17 Once we establish the linkage between
18 software and hardware in task ten, we'll combine the
19 two models. Then in task eleven, integrate the
20 digital system probabilistic failure model into the
21 PRA. And the next presentation will be discussing
22 task five.

23 CHAIR APOSTOLAKIS: Is the EPRI report
24 you're referring to the one we discussed at the last
25 meeting?

NEAL R. GROSS

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

1 MR. HILSMIEIER: Yes, it was.

2 CHAIR APOSTOLAKIS: You are still
3 developing a position?

4 MR. HILSMIEIER: No.

5 CHAIR APOSTOLAKIS: It's a year now.

6 MR. HILSMIEIER: Right. We're not still
7 developing a position, but this plan shows everything
8 that we've done. We no longer are studying this
9 guide.

10 CHAIR APOSTOLAKIS: Oh, you're not.

11 MR. HILSMIEIER: No.

12 CHAIR APOSTOLAKIS: So you have a
13 position.

14 MR. HILSMIEIER: Well, we have a position
15 as far as how it's useful to us in the development of
16 the traditional PRA method.

17 CHAIR APOSTOLAKIS: Are you expected to
18 send the formal opinion to EPRI?

19 MR. HILSMIEIER: Steve would have to answer
20 that.

21 MR. ARNDT: The EPRI report was submitted
22 for our review, and I don't want to go into the gory
23 details, but it was determined we would not review it
24 formally for SER at that time, from an agency
25 standpoint. The task he's referring to is learning

NEAL R. GROSS

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

1 from what was proposed in that methodology. At a
2 future time they may resubmit it, and we may decide to
3 write an SER against it. We looked at it from how we
4 can use it to help develop the traditional model.

5 CHAIR APOSTOLAKIS: So the first one -- we
6 have two reports from BNL.

7 MR. HILSMEIER: Correct.

8 CHAIR APOSTOLAKIS: Which one are you
9 presenting first?

10 MR. HILSMEIER: The first one would be
11 development of the failure parameter database.

12 CHAIR APOSTOLAKIS: Neither one has a
13 title.

14 MR. HILSMEIER: Excuse me?

15 CHAIR APOSTOLAKIS: Collection of Failure
16 Data, or a Review of Software Induced Failures?

17 MR. HILSMEIER: Collection of Failure
18 Data.

19 CHAIR APOSTOLAKIS: Okay.

20 MR. HILSMEIER: And the objective of this
21 report is to develop failure parameter database for
22 digital hardware based on currently available data for
23 quantifying digital system reliability models. And
24 the approach analysis will be presented by Louis Chu
25 from Brookhaven National Lab.

NEAL R. GROSS

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

1 MR. CHU: I'm presenting our work,
2 developing hardware failure database for digital
3 systems hardware. The outline will include our
4 objectives, review of available failure rate database,
5 some comments on hardware reliability protection
6 methods, and then I'll talk about use of hierarchical
7 Bayesian analysis to come up with generic estimates of
8 component failure rates, some conclusions, what we've
9 done and some proposed additional data collection.

10 The objective of this task is to develop
11 a generic failure parameter database of digital
12 components based on currently available data in
13 support of developing reliability models, such as
14 fault trees, Markov models of digital systems.

15 CHAIR APOSTOLAKIS: So what failure
16 parameters are you talking about?

17 MR. CHU: Component failure rates.
18 Hardware component failure rates.

19 CHAIR APOSTOLAKIS: Of the computer you
20 mean? Hardware --

21 MR. CHU: Yes, like microprocessors,
22 memories.

23 CHAIR APOSTOLAKIS: Okay. All right.

24 MR. CHU: Okay. The approach we use is
25 review of available methods and database, and then we

NEAL R. GROSS

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

1 came up to the understanding there's not too much out
2 there, and we tried to do what we can with the
3 available data, and we performed this analysis using
4 data extracted out of PRISM.

5 This viewgraph summarizes the review of
6 failure rate databases. The existing nuclear
7 databases do not contain digital component failure
8 rates. For example, IEEE standard, SPAR database, the
9 T-book, the ZEBD, the Swedish database, they don't
10 contain digital component failure rates.

11 CHAIR APOSTOLAKIS: What is the definition
12 of a database? I mean, the IEEE standard is really
13 the judgment of the people they polled, and this is
14 qualified to be called a database? I mean, you could
15 say it's a general term, but when I hear database, I
16 usually have in mind something that has real data in
17 it.

18 MR. CHU: Yes. What we have in mind is
19 something that was estimated based on real data.

20 CHAIR APOSTOLAKIS: So IEEE standard
21 wouldn't qualify.

22 MR. CHU: I thought some of that would --
23 I mean, they don't have digital components, but I
24 thought some of that was based on actual data.

25 CHAIR APOSTOLAKIS: It's really expert

NEAL R. GROSS

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

1 opinion. Now the expert opinion may have been --

2 MR. CHU: Based on some kind of data.

3 CHAIR APOSTOLAKIS: May have included
4 experience with actual failures. And SPAR, SPAR is
5 out kid. Right? We're trying to help them. Anyway,
6 I mean, I'm nitpicking now. AP600, what do these guys
7 say?

8 MR. CHU: It has some high level, I would
9 say crude model of digital systems, and it contains
10 some, you know, I call it scatter data. If you look
11 into their database, they probably have some estimated
12 failure rate of a microprocessor, or maybe a
13 particular circuit board. And if you look more
14 carefully, you try to trace how the failure rates were
15 estimated. Typically, you found it's based on say
16 Westinghouse proprietary data. And it's scattered in
17 the sense that it doesn't cover all the components
18 that you can think of in a digital system. And if you
19 look at papers, you can see some -- some papers
20 collect some data in a particular study, the estimated
21 failure rate of a programmable logic controller. But
22 then our attempt is try to come up with something
23 generic such that when you do a study, if you collect
24 specific component failure rates of the system you are
25 studying, you can possibly use that data to update

NEAL R. GROSS

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

1 this generic failure rate.

2 CHAIR APOSTOLAKIS: Is it correct to say
3 that of all these databases you have there, it's
4 really the LER database that gives you real data?

5 MR. CHU: LER and EPIX gives you nuclear
6 data.

7 CHAIR APOSTOLAKIS: EPIX doesn't have much
8 on digital INC. Right?

9 MR. CHU: Well, even LER, you know, it's
10 required, you're required to have LER. It has some
11 reporting criteria, you have to violate tech spec, or
12 you -- therefore, certain failure may not get
13 reported. And another difficulty with use of LER is
14 that often you see some failure, but then you don't
15 know how many of the same components are being used at
16 a plant, and how long they've been operating.

17 CHAIR APOSTOLAKIS: But they are real
18 data.

19 MR. CHU: Right. And while I call the
20 hardware reliability prediction method that is the
21 military handbook to Telcordia and PRISM, supposedly
22 they developed their model based on actual data, too.
23 But then they came up with empirical formula that you
24 just apply. In case of PRISM, I know, because we
25 looked into the raw data and we extracted the raw data

NEAL R. GROSS

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

1 to do our --

2 CHAIR APOSTOLAKIS: What does PRISM stand
3 for? Do you^v remember?

4 MR. CHU: My understanding is it's not an
5 abbreviation of anything. It's just a name they
6 chose.

7 MR. MARTINEZ-GURIDI: PRISM is a system
8 that was developed by the Reliability Analysis Center,
9 and PRISM is actually software that contains the
10 database developed by this organization, that you can
11 query to get the information.

12 CHAIR APOSTOLAKIS: And this center is
13 military?

14 MR. MARTINEZ-GURIDI: No, it's a company.

15 CHAIR APOSTOLAKIS: Oh.

16 MR. MARTINEZ-GURIDI: They are mainly
17 funded by Department of Defense.

18 MR. CHU: So --

19 CHAIR APOSTOLAKIS: SINTEF?

20 MR. CHU: SINTEF is an organization. I
21 have its name. Let me see.

22 CHAIR APOSTOLAKIS: Yes, I know. It's a
23 Norwegian company, but where did they get their data
24 from?

25 MR. CHU: We haven't looked into it yet.

NEAL R. GROSS

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

1 It just came to us. They came up with a data handbook
2 dated 2006, I believe, so that's another source of
3 information to look into. And the claim is that they
4 have data to support the Markov model described in the
5 IEC standard.

6 A few things on reliability prediction
7 method. They include Handbook 217, Telcordia and
8 PRISM. The problem with this method is that they
9 attempt to capture many causes variability explicitly,
10 and such attempt is too ambitious. That is, they
11 introduce all kinds of high factors to adjust the base
12 failure rates, and they use empirical formula. My
13 speculation is that some of the factors, high factor
14 they estimated based on actual data, but then they
15 extrapolate.

16 CHAIR APOSTOLAKIS: Do you know what kind
17 of review these things get?

18 MR. CHU: I know there's a Professor York
19 Maledon, provide quite critical --

20 CHAIR APOSTOLAKIS: Just a professor?

21 MR. CHU: Yes. He had written several
22 papers criticizing the accuracy of this type of
23 method.

24 CHAIR APOSTOLAKIS: So really, they have
25 not been reviewed --

NEAL R. GROSS

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

1 MR. CHU: And he's only looking at it at
2 the level of the results. And I think what needs to
3 be scrutinized is how those factors were derived.

4 CHAIR APOSTOLAKIS: Oh, sure.

5 MR. CHU: In principle, they have some
6 kind of internal document that's not available to us.
7 But in general, you could say we could ask for those
8 bases studies that came up with it.

9 CHAIR APOSTOLAKIS: They're probably like
10 the pro forma shaping factors in a reliability
11 analysis. You do what you like.

12 MR. CHU: Chances are, say in one case
13 they came up with an estimate, you know, military
14 equivalent is a factor three better than commercial
15 one. And three may be used whenever you need you have
16 a situation, but how accurate is. This is my
17 speculation. Also, it's kind of based on what I know
18 about the current data that they have. I'm going to
19 show you in a later viewgraph. So use of empirical
20 formula is not that accurate.

21 But on the other hand, I guess there isn't
22 much other method out there, or data out there. They
23 essentially add the failure rates of components to get
24 a failure rate of a circuit board. And when it comes
25 to redundancy, then you have to model separately. So

NEAL R. GROSS

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

1 they calculate the failure rate of a circuit board,
2 and treating it as a series system, a system consists
3 of components in series. And then if you have two
4 circuit board, two redundant circuit board, then you
5 have to model separate using something like fault tree
6 or Markov model. So one issue is the accuracy of the
7 empirical formula. And certainly, they didn't look
8 into the uncertainty associated with it. At one
9 point, I asked what about uncertainty? They just said
10 there's so many uncertainties, they cannot account for
11 it.

12 CHAIR APOSTOLAKIS: So large that we don't
13 care about it. Right? So you actually talked to
14 people who are responsible for these databases. You
15 just didn't --

16 MR. CHU: I went to a training session on
17 the PRISM software, and used that opportunity to ask
18 some questions.

19 CHAIR APOSTOLAKIS: Very good.

20 MR. CHU: In looking at those reliability
21 prediction methods, you know, they are software tools
22 that implement the method. They only help you to
23 estimate component failure rates, but they don't give
24 you raw data. PRISM is an exception. It turns out in
25 this database, they included the raw data in the form

NEAL R. GROSS

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

1 of a number of failures, number of hours. So we
2 extracted this kind of raw data and used it in our
3 analysis. The problem with it is there's very large
4 variation in the data that is from different sources,
5 you get very different estimates.

6 This viewgraph shows the data we extracted
7 for one component. I think this is the data for
8 random access memory, and the table shows - the first
9 column is quality, typical, it's commercial or
10 military. Environment GB means ground-based, and GM
11 means ground-mobile. And next two columns are the raw
12 data, the number of failures, the number of hours.
13 And the last column shows a point estimate.
14 Basically, for those sources that have failure, I just
15 do a simple division. In this case, 12 failures in
16 this amount of time, and you get some point estimate.
17 If you look at this last column, you can see the point
18 estimate varies from probably .1 to 10 to the minus 3.
19 There's a lot of --

20 CHAIR APOSTOLAKIS: A million hours.

21 MR. CHU: Yes.

22 MR. HICKEL: You've got to add a six on to
23 those. I just have a simple question. And you're
24 obviously trying to collect data on electronic
25 components, but the thing that is probably most needed

1 by the Agency is the ability to extrapolate that to
2 something that might appear in a digital INC system.
3 To be able to know you can make that extrapolation,
4 don't you also have to know that the mode in which
5 that equipment was used, the way it was
6 environmentally qualified, and run in a power plant
7 environment with tech specs and daily shift checks and
8 all that sort of stuff. How do you know that data
9 from, I don't know, NASA launch facility is equivalent
10 to a control^v system in a power plant? How do you make
11 that equation?

12 MR. CHU: This is why we use the
13 hierarchical Bayesian analysis, that is in this
14 method, we account for the variability from different
15 conditions, different source, like those factors that
16 affect the failure rates.

17 MR. HICKEL: Right.

18 MR. CHU: The factors could be the
19 quality, could be the operating environment, and this
20 population^v variability distribution captures such
21 variability. And then when you do a specific study,
22 you may obtain some failure data. Then you further do
23 a Bayesian updating to specialize the failure rates.

24 CHAIR APOSTOLAKIS: You will talk about
25 that at some point?

NEAL R. GROSS

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

1 MR. HICKEL: Because I'm just betting that
2 somebody from NEI is going to come in and say well,
3 that's very interesting, but that data doesn't reflect
4 anything we're using. I'm just trying to understand
5 how specific this is to a nuclear power plant INC
6 system.

7 CHAIR APOSTOLAKIS: You will tell us how
8 to do that later?

9 MR. CHU: Later we have some suggestions
10 to do additional data work.

11 CHAIR APOSTOLAKIS: No, no, no, the
12 Bayesian hierarchical thing, you're going to talk
13 about that?

14 MR. CHU: Oh, yes. I have two viewgraphs
15 explaining that.

16 CHAIR APOSTOLAKIS: Okay. So let's take
17 one entry here, take the first one, number of failures
18 - 12, 633 million hours?

19 MR. CHU: Yes, million hours.

20 CHAIR APOSTOLAKIS: Million hours. So
21 this was commercial, and this is a particular system,
22 so this is the experience of some organization? You
23 didn't collect each one.

24 MR. CHU: We didn't. When we asked about
25 the source of the data, the kind of information we got

NEAL R. GROSS

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

1 was something like this source of data is warranty
2 repair data from the manufacturer. You don't know
3 what the manufacturer is, just a few words
4 description.

5 CHAIR APOSTOLAKIS: No, but who recorded
6 the 12 failures in 633 million hours?

7 MR. CHU: Manufacturer --

8 CHAIR APOSTOLAKIS: Oh, the manufacturer.

9 MR. CHU: -- of that particular component.

10 CHAIR APOSTOLAKIS: And the manufacturers
11 are different in the different --

12 MR. CHU: It's not identified; therefore,
13 I don't know. It could well be different
14 manufacturers.

15 CHAIR APOSTOLAKIS: So the variability we
16 see in the last column, is this variability due to
17 different manufacturers, due to different
18 environments?

19 MR. CHU: Yes.

20 CHAIR APOSTOLAKIS: Yes, both?

21 MR. CHU: Everything.

22 CHAIR APOSTOLAKIS: Both. Oh.

23 MR. CHU: Yes. And, of course, you can
24 argue maybe you should treat commercial equipment
25 separate from military, but if you look at the data --

NEAL R. GROSS

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

1

2

CHAIR APOSTOLAKIS: The commercial - no, they're almost the same, aren't they?

3

4

5

6

7

8

9

10

11

MR. CHU: It's hard to tell them apart. That's another thing. By just looking at this data, it's hard to say that military equipment are better. Therefore -- and if you group them separately, you may not have enough data to do the analysis. And supposedly, this is the kind of data that PRISM or the Reliability Analysis Center used in coming up with their --

12

13

CHAIR APOSTOLAKIS: Did they have this for all the components of interest to us?

14

15

MR. CHU: We extracted all the data that we were able -- that's in the PRISM database.

16

17

18

CHAIR APOSTOLAKIS: No, but I mean, you were able to find information like this for all the components we're interested in?

19

20

21

22

23

24

25

MR. CHU: I'm not sure, but there were some 30 components as defined in the PRISM tool. They have raw data, so we just extract all of them. We haven't tried to develop our model of the digital system, so when we do that, we'll know. But these components tend to be at a lower level, as you will see. That's kind of what we hope to do, at least do

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 it once, and try to do a detailed analysis, understand
2 the design, and learn from it. And then see how we
3 can possibly -- the method can be simplified, the
4 model can be simplified.

5 CHAIR APOSTOLAKIS: Now what if, let's say
6 again the first row, look at -- we don't know how many
7 components you have. Right? We just know the total
8 number of hours.

9 MR. CHU: Right.

10 CHAIR APOSTOLAKIS: Is it possible that
11 the 12th failure was due to a design error, and that
12 error was not present in the other 11, of course, not
13 also in the ones that operated successfully. So why
14 then -- I mean, just because we have number of hours
15 and number of failures, why are we jumping into a
16 failure rate? How do you know that there is a rate?
17 Maybe one or two of them had a design error and they
18 failed immediately. Do you know that all these 12
19 were components that operated for a certain period,
20 and then failed?

21 MR. CHU: No, we don't have that
22 information.

23 CHAIR APOSTOLAKIS: You don't know.

24 MR. CHU: All we have is what's in these
25 two columns.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: Okay. So then I'm
2 arguing that you're making a pretty serious assumption
3 there, that there is such a thing as a failure rate,
4 because some of them may have had a design flaw and
5 they failed right away. It was not a matter of
6 failure due to random causes, lambda, usually lambda.
7 I think these failure rates are so prevalent here, and
8 very few people are questioning whether they're
9 appropriate. So if you don't know what kinds of
10 failures these are, then it seems to me getting a
11 failure rate is probably not such a great idea.

12 MR. CHU: Well, we just don't have that
13 information. Let me explain a little bit more.

14 CHAIR APOSTOLAKIS: I understand that you
15 don't have it.

16 MR. CHU: The total number of hours
17 actually is the sum over certain reporting periods,
18 different years, so we added them up.

19 CHAIR APOSTOLAKIS: Sure.

20 MR. CHU: So there is a little more
21 detail, information --

22 CHAIR APOSTOLAKIS: Well, let's take
23 pumps, okay? And I start with 10 pumps in my test.
24 I start them, two of them fail right away. They don't
25 work at all, and the other ten fail at some intervals.

NEAL R. GROSS

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

1 Is it reasonable to take the total number of failures
2 and total number of hours they operated, and divide
3 them and get the failure rate? Is that representative
4 of what happened? No, because two of them never
5 worked.

6 MR. HILSMEIER: Would that be kind of just
7 failed to start, for the two that never started?

8 CHAIR APOSTOLAKIS: That's right. And
9 maybe they had a design flaw.

10 MR. HILSMEIER: Right.

11 CHAIR APOSTOLAKIS: So here, I don't know
12 why we're jumping immediately to the principle of
13 failure rate. We don't know. Fine, we don't know,
14 but we are adding more information here which is not
15 based on what the database is telling us. And the
16 reason I'm saying that is because you, yourselves,
17 later will tell us 36 percent of the errors were due
18 to some requirements problem.

19 MR. CHU: Those are software failures.
20 These are hardware failures.

21 CHAIR APOSTOLAKIS: Yes, these are
22 hardware.

23 MR. HILSMEIER: One of the limitations of
24 this data is it's not failure mode specific, so we
25 kind of had -- which you're going to need for fault

NEAL R. GROSS

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

1 trees.

2 CHAIR APOSTOLAKIS: All I'm saying is that
3 most people would look at this table and think it's
4 natural to go to the last column, and I'm not saying
5 that it's natural to do that, because you don't know
6 how they failed. You don't have to assume the failure
7 rate exists automatically. I mean, if there was a
8 design flaw,[^] there was a design flaw. And strictly
9 speaking, they should be accounted for in their
10 unavailability calculation. We just don't know. If
11 it was a failure rate, and this would be a point
12 estimate.

13 MR. HILSMEIER: That's a good comment.
14 We'll look into that.

15 MR. HICKEL: Got to have the pedigree to
16 know how to do the calculation.

17 CHAIR APOSTOLAKIS: Yes. I mean, just
18 taking -- that's why it's important to have a model in
19 your mind when you do the data investigation. And
20 here without really saying so, you assume the model,
21 the exponential failure distribution.

22 MR. CHU: I'll put it this way, that's the
23 only data we were able to find. And I'm glad --

24 CHAIR APOSTOLAKIS: The only data you were
25 able to find is in the first four columns. The fifth

NEAL R. GROSS

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

1 column you created.

2 MR. CHU: Right. It's just providing an
3 indication of a point estimate. We're not using that
4 for other purpose.

5 CHAIR APOSTOLAKIS: I understand, but do
6 you understand what I'm saying?

7 MR. CHU: Yes.

8 CHAIR APOSTOLAKIS: Okay.

9 MR. ELKS: I believe I can add some
10 clarification. Carl Elks, University of Virginia. I
11 used the RAC PRISM database, as well. And when I
12 talked to them about this table, I was concerned much
13 about the same issues as like where did you get this
14 data, is infant mortality rate factored into it or is
15 it not? The answer that I got back from their experts
16 was the infant mortality rate was factored out, so
17 this was stuff that occurred later in time.

18 CHAIR APOSTOLAKIS: They actually operated
19 for a --

20 MR. ELKS: Yes. Now that's off-the-record
21 from one of their vendors. Okay.

22 CHAIR APOSTOLAKIS: If that's the case,
23 then the failure rate estimate makes sense.

24 MR. CHU: So with that column, we
25 performed Bayesian analysis to derive population

NEAL R. GROSS

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

1 variability curves shown in this figure.

2 CHAIR APOSTOLAKIS: This is a two-stage
3 Bayesian, is that what it is?

4 MR. CHU: Yes, but we used what's called
5 hierarchical Bayesian, and it's said to be a more
6 general method. But the underlying model is the same,
7 the difference - the way I see it is only in solving
8 the problem, how you numerically solve the problem.
9 Like the typical two-stage analysis, people just
10 discretize distribution.

11 CHAIR APOSTOLAKIS: Yes.

12 MR. CHU: Hierarchical Bayesian used Monte
13 Carlo simulation in solving it.

14 CHAIR APOSTOLAKIS: Yes, alpha and beta,
15 the parameters of which distribution?

16 MR. CHU: Of the population variability.

17 CHAIR APOSTOLAKIS: I mean, have you
18 assumed the form?

19 MR. CHU: Yes. We made different
20 assumptions, such as uniform exponential, log normal.

21 CHAIR APOSTOLAKIS: If it's exponential,
22 you have only one parameter. Right?

23 MR. CHU: Right. No, on the population
24 variability curve we assume either log normal or
25 gamma.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: Okay.

2 MR. CHU: But on these parameters --

3 CHAIR APOSTOLAKIS: Yes, I understand.

4 MR. CHU: -- they are further distributed.

5 So the underlying model is that we have data from
6 different sources, different plants, or different
7 manufacturer, and this curve is used to characterize
8 that variability. Therefore, the data from different
9 sources has failure rates that are samples from
10 distribution. And with the data from different
11 sources, we go through the statistical analysis to
12 estimate this distribution.

13 CHAIR APOSTOLAKIS: So then the question
14 then that Dr. Hickel asked earlier, this is the
15 answer, that you have a broad curve that represents
16 different manufacturers, different environments, and
17 so on. But then there is another assumption there
18 that the environment and manufacturer of your
19 application in a nuclear plant is part of this
20 ensemble.

21 MR. CHU: Right.

22 CHAIR APOSTOLAKIS: Which is another
23 assumption, because I don't know if those guys have
24 Appendix B. Okay? Or the equivalent, so our
25 environment is probably better controlled, so maybe we

NEAL R. GROSS

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

1 are on the low side. Maybe.

2 MR. CHU: Hopefully, if you have some
3 data, then you further analyze it.

4 CHAIR APOSTOLAKIS: Oh, yes. You start
5 with hopefully, you could say anything you want. But
6 this is a good idea, I mean, trying to get there, and
7 then maybe you can modify the curve to allow for the
8 fact that we have all these controls and so on.

9 MR. CHU: Yes.

10 CHAIR APOSTOLAKIS: That's a funny looking
11 distribution there, Louis. A little more tilted to
12 the left and it would be really a strange beast. In
13 fact, we would be wrong if you did it that way.
14 Almost vertical there, isn't it? Is it freehand or -
15 can't be because it's smooth.

16 MR. CHU: I don't remember how we came up
17 with this.

18 CHAIR APOSTOLAKIS: So what is Mu-I?

19 MR. CHU: Mu-I, it's just lambda times T.
20 This is a notation within the --

21 CHAIR APOSTOLAKIS: Oh, T to the minus
22 lambda T. Okay.

23 MR. CHU: Yes, this is just a notation
24 within the win BUGS, or hierarchical Bayesian method.
25 This method is kind of advocated in the NRC handbook

NEAL R. GROSS

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

1 on parameter estimation.

2 CHAIR APOSTOLAKIS: Parameter estimation,
3 yes.

4 MR. CHU: And we used it, and we recognize
5 there's still some problem with the guidance here.

6 CHAIR APOSTOLAKIS: There's no problem
7 with the method. The problem is what we just
8 discussed. I mean, the assumptions that go behind
9 this, is my environment, are my components part of
10 this ensemble that I get.

11 MR. CHU: Yes.

12 CHAIR APOSTOLAKIS: That's really the
13 fundamental question.

14 MR. CHU: Yes.

15 CHAIR APOSTOLAKIS: Should I stress the
16 distribution on the low side to account for those, and
17 if I decide to do that, how am I going to do it so I
18 can defend it. These are the real issues here,
19 whether you -- I know what this method is. It's okay,
20 theoretically it's okay. Who are the Brookhaven
21 Science Associates, by the way? You?

22 MR. CHU: This is the company that manages
23 Brookhaven Lab.

24 CHAIR APOSTOLAKIS: Okay.

25 MR. CHU: It's formed by people from the

1 universities, and BATEL Lab.

2 CHAIR APOSTOLAKIS: I thought it was a
3 group within Brookhaven, but it's a hierarchical base.
4 Right? It's higher.

5 MR. CHU: I've shown an example of the
6 kind of data, and we extracted data for 30 components.
7 And WinBUGS is the software that we used.

8 CHAIR APOSTOLAKIS: Who developed that?

9 MR. CHU: I'm sorry?

10 CHAIR APOSTOLAKIS: WinBUGS, who developed
11 it?

12 MR. CHU: I think some people --

13 CHAIR APOSTOLAKIS: Oh, it's a commercial

14 -- MR. CHU: Yes, it's available. You go to
15 the website, sign up for it and you can download it.
16 It's some British professor, probably.

17 CHAIR APOSTOLAKIS: Some who?

18 MR. CHU: British professor. I have some
19 reference. I don't recall the --

20 CHAIR APOSTOLAKIS: He spells bayes with
21 a lower a B?

22 MR. CHU: Okay. It solved the model by
23 performing simulation. In our analysis of these data,
24 we assumed failure rates were either log normal and
25 gamma distribution --

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: You mean the failure
2 rate distributions were log normal, not the failure
3 rates.

4 MR. CHU: Right. The distributions, yes.

5 CHAIR APOSTOLAKIS: And the generic
6 distributions.

7 MR. CHU: Yes. And further, the
8 parameters of the distribution --

9 CHAIR APOSTOLAKIS: So let's look at the
10 results. Yes, this is fine, I believe, we believe.

11 MR. CHU: The result is that because the
12 data is very scattered, so --

13 CHAIR APOSTOLAKIS: Don't you have a curve
14 somewhere? No? Okay.

15 MR. CHU: Some results, two viewgraphs of
16 results. The problem appears to be the error factor
17 is --

18 CHAIR APOSTOLAKIS: Wait, wait, wait.
19 What you are showing here is the average curve, isn't
20 it?

21 MR. CHU: Yes.

22 CHAIR APOSTOLAKIS: The average curve, so
23 you have average overall values of alpha and beta?

24 MR. CHU: Right.

25 CHAIR APOSTOLAKIS: And this is the curve

NEAL R. GROSS

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

1 that you are^u showing us. Okay.

2 MR. CHU: Right.

3 MR. HICKEL: Okay. Can I -- this list of
4 components here, this is from LER, PRISM, RAC?

5 MR. CHU: PRISM.

6 MR. HICKEL: PRISM only.

7 CHAIR APOSTOLAKIS: Yes. The kind of data
8 he showed earlier. So what do we learn from this,
9 Louis? I see some error factors that are pretty
10 significant there, 173.

11 MR. CHU: Just too wide.

12 CHAIR APOSTOLAKIS: Oh, I don't know that
13 it's too wide. I mean, maybe that's the reality.
14 Right? I would say that the four point date is too
15 narrow. What is the message from all this?

16 MR. CHU: There's very large variability
17 among different -- the same type of component from
18 different manufacturer or different sources.

19 CHAIR APOSTOLAKIS: But explain the
20 largest error factor, I presume this is not normal,
21 right?

22 MR. CHU: Yes.

23 CHAIR APOSTOLAKIS: Is 173, and on the
24 left you say error. What does that mean?

25 MR. CHU: No.

1 CHAIR APOSTOLAKIS: Component is error?

2 MR. CHU: No, it should continue to error
3 detection or error collections.

4 CHAIR APOSTOLAKIS: Oh. Oh.

5 MR. CHU: That's one component. As to the
6 definition of component, there's uncertainty to what
7 does that mean when it says error
8 detections/collection.

9 CHAIR APOSTOLAKIS: Is that the component?
10 I don't know.

11 MR. CHU: We tried to get some explanation
12 to the component, but these names are strictly
13 extracted from PRISM, and in our report we tried to
14 give some explanation of what the component - what we
15 think the component --

16 CHAIR APOSTOLAKIS: But since you took
17 that course, is it possible to call somebody and find
18 out? I mean, the others seem to be components, but
19 this one I don't know.

20 MR. CHU: Yes, I think it's possible.
21 Yes. This large variation, if you compare this to
22 say what you see in AP600 or in some PRAs --

23 CHAIR APOSTOLAKIS: Is that million hours?

24 MR. CHU: Yes. Next table is the same.
25 I want to back up a little. Let me see. Like 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 point out one problem with assuming gamma
2 distribution. This is based on some recent work by
3 Hover, Bunere, Cook, some of the people working on the
4 PRA project, actually. They look into the two-stage
5 Bayesian analysis, and they recognize the problem with
6 --

7 CHAIR APOSTOLAKIS: Where are these
8 people?

9 MR. CHU: Let me see. A few of them are
10 currently with George Washington University, but I
11 think they're originally from European countries
12 working on - maybe German or --

13 CHAIR APOSTOLAKIS: What's that name
14 again?

15 MR. CHU: Hover.

16 CHAIR APOSTOLAKIS: Oh, I know him, yes.
17 Okay.

18 MR. CHU: So for gamma distribution, it
19 can be shown analytically that the likelihood --
20 function becomes the likelihood of a common incident
21 rate model when the parameters are large. That means,
22 the likelihood is not bounded, it goes to -- it
23 doesn't die as alpha beta goes to infinite. And it's
24 improper, and it has no maximum, and is esoteric of
25 the maximum along a ridge. Basically, is asked when

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 you work with this kind of problem that you truncate,
2 whenever you use computer to implement it, you
3 truncate and you lose information. That would be --

4 CHAIR APOSTOLAKIS: If I use log normal,
5 don't have any problem.

6 MR. CHU: Right.

7 CHAIR APOSTOLAKIS: Good.

8 MR. CHU: Right. Kind of I want to make
9 a remark - we've done this kind of analysis so many
10 years, and all of a sudden we recognize there's a
11 problem, so there are still things to learn.

12 CHAIR APOSTOLAKIS: Well, the papers by
13 Hover have been out also for a number of years, but
14 the question is how many people have read them. But
15 we're using log normal most of the time, so it's okay.

16 MR. CHU: Right.

17 CHAIR APOSTOLAKIS: Ahh, conclusions.

18 MR. CHU: We developed a process for
19 estimating generic failure rates.

20 CHAIR APOSTOLAKIS: So you are saying then
21 that the best we can do it to use PRISM. Is that what
22 you're saying?

23 MR. CHU: That's the only place I guess in
24 the raw data.

25 CHAIR APOSTOLAKIS: You didn't get

NEAL R. GROSS

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

1 anything from LER?

2 MR. CHU: LER, that's the suggested
3 additional work, you try to collect more information
4 from the plant so that you find out how many of the
5 same equipment are being used at the plants, or how
6 long they've been operating.

7 CHAIR APOSTOLAKIS: Well, maybe instead of
8 expecting to get information from LERs that will help
9 you find failure rates, maybe you can get some idea as
10 to how better our components are, and then devise a
11 means of changing the low tail of the distribution you
12 have developed from PRISM to account for nuclear
13 environments. Maybe that would be a way to go,
14 because I don't think these people have the same
15 quality controls that we have. And probably the low
16 tail of the distribution should be further to the
17 left. I don't know. I mean, if you disagree, you
18 disagree, but I think that's an issue here.

19 MR. HICKEL: That's a very good idea.

20 MR. CHU: We did look into some kind of
21 regrouping of the data, but I find it hard because
22 there isn't enough data to do this kind of analysis,
23 when you do a --

24 MR. HICKEL: You know, I really had a
25 problem with one of the conclusions, and this

NEAL R. GROSS

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

1 statement just kind of jogged it into my memory. Your
2 report on page 21 said that when you searched the LER
3 database for failures in digital INC systems, you only
4 got 18 records?

5 MR. CHU: That was probably for a
6 particular type of component. Maybe we searched for
7 microprocessor.

8 MR. HICKEL: Right.

9 MR. CHU: I think. That's the case, we
10 are -- I'm pretty sure that that's the case. Again,
11 LER doesn't necessarily record all the failures.

12 MR. HICKEL: Right. I fully agree. As a
13 matter of fact, I would say that most of the plants
14 that have a device that includes the microprocessor
15 would report in the LER the name of the system, not
16 the fact that it was a microprocessor failure. They
17 report that such and such system failed, and that
18 would give you a low count. But the other thing is,
19 I saw the word you searched. You mean you did an
20 electronic search of the LER database?

21 MR. CHU: Yes.

22 MR. HICKEL: Well, you are aware that on
23 the NRC LER website, they've got the optical imaging
24 going back to 1984. I take it you didn't consider
25 anything that was a paper record that's just been put

NEAL R. GROSS

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

1 on as a PDF.

2 MR. CHU: We did the search of the system
3 being maintained by INEL.

4 MR. HICKEL: Right.

5 MR. CHU: And I think it does go back to
6 like 1984. That's about right.

7 MR. HICKEL: It does, but you can't
8 electronically search it, so when I saw the word that
9 you searched for microprocessor, my immediate reaction
10 was well, that's interesting. How do you search a PDF
11 on a file like that? You can't.

12 MR. MARTINEZ-GURIDI: I believe that the
13 LER search system can be searched electronically. You
14 can specify a certain string of characters, and it --

15
16 MR. HICKEL: Yes, but many of the records
17 going back that old, they're images, they're pictures.

18 MR. MARTINEZ-GURIDI: Not any more. I
19 mean, that was the case a few years ago, but nowadays,
20 they have the electronic version to '84 where you can
21 search electronically.

22 MR. HICKEL: Okay. Because I was going to
23 tell you, I personally had done a search of LERS
24 looking for digital systems, and it happened to be in
25 an area where I knew the names of the plants, I knew

1 roughly when they had changed out, and when they did
2 it. And I worked at CE a long time ago, about 20-30
3 years ago. I searched looking for information about
4 their core protection calculators, and I got about 160
5 something LERs that all involved that system. There
6 were failures all over the place, different kind of
7 combinations and permutations of something in test,
8 and a guy uploaded a new data set without knowing that
9 one of the other channels was bypassed. All that
10 stuff is there. There's MOX failures, there's CPU
11 failures, all of those, and I think that that LER
12 database contains failure experience that's a lot more
13 relevant than what you might find if you're trying to
14 find out what the Air Force is doing with a missile
15 tracking computer or something like that.

16 The reason is, it has to do a little bit
17 with pedigree, and I think George talked about, we
18 talked about it a little bit. It's the mode that the
19 equipment is bought, procured, installed,
20 commissioned, tested, operated with tech specs, and
21 people that have to do certain periodic tests. This
22 is not commercial electronics like your laptop at
23 home. It's a very different variety of stuff, and I
24 think basically, I think there's a lot more in the LER
25 data system than you're considering in this

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 evaluation.

2 MR. CHU: We've only done some kind of
3 trial search of the LER. We knew that we will not
4 have information on how many of the same components
5 are operating, how long they've been operating, so we
6 knew we're not going to be able to use it to come up
7 with some estimates, so what we searched LER was just
8 some trial search, see what we can find. We didn't
9 try to use that to do any kind of --

10 CHAIR APOSTOLAKIS: Do you plan to do this
11 kind of more detailed search?

12 MR. CHU: That's what we're suggesting to
13 do. The last viewgraph talk about it, but I recognize
14 the difficulty. Searching LER is one thing, you have
15 to somehow get information from the plant, that kind
16 of information.

17 CHAIR APOSTOLAKIS: The last bullet,
18 really, I mean did you agonize on it a lot before you
19 put it there? This is a consensus view of the
20 project, that better data should be collected? Yes,
21 Louis, go on. Just say yes. Didn't you learn from
22 Steve? Please identify yourself and speak into the
23 microphone.

24 MR. STONE: I'm Jeff Stone from
25 Constellation Energy. I work PRA. What I was

1 questioning is you're focusing on operational failure
2 rates, per hour failure rates. Are you going to
3 address how we're going to quantify demand failure
4 probabilities in this document?

5 MR. CHU: Not in this document, because
6 all we have is those data from the PRISM tool. Like
7 George pointed out, in some situations the failure
8 could be demand type of failure, but we don't have
9 that kind of data.

10 CHAIR APOSTOLAKIS: How important do you
11 think that is?

12 MR. STONE: I think that's probably much
13 more significant than the operational failure
14 probabilities.

15 CHAIR APOSTOLAKIS: He's right.

16 MR. HICKEL: The issue is you've got some
17 spike where there's a demand, that you need that
18 equipment to work. And in that period, it had better
19 be working in that interval, but that's -- if he's got
20 the hourly failure rate, getting that wouldn't be that
21 difficult.

22 CHAIR APOSTOLAKIS: Well, that's something
23 for you guys to consider. I mean, it's okay that you
24 haven't done it, but it's certainly something that
25 deserves --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STONE: Well, I mean, there are two
2 parts to a demand failure probability. There's a part
3 that it can fail per hour, or is there some shock
4 failure probability when it's actually demanded. So
5 just question that. Thank you.

6 MR. ELKS: Carl Elks, University of
7 Virginia. Just one final comment I had. In my
8 experience working with this PRISM database during the
9 past couple of months, I've done a lot of CIRCA design
10 of these safety critical systems in the past, and the
11 components that are actually in the PRISM database are
12 relatively old. I mean, these are the things that you
13 would see ten years ago in a design, even longer. I
14 mean, if you go back and look at that thing where you
15 see latch counts, comparators and stuff, we don't use
16 those any more, these FPGAs, and PLDs, and things of
17 that nature. And I talked with the PRISM people about
18 this, and I said when are you going to update your
19 database so that we get more contemporary components,
20 and they were going well, as soon as we get the data
21 in. So I don't know if that was your experience or
22 not, that trying to kind of look at it from the point
23 of view of actually what's out in the field, and
24 what's actually in the database, sometimes are not
25 lined up correctly. And that's it.

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. CHU: Well, I guess Reliability
2 Analysis Center at least has some means of collecting
3 data. We didn't even try, but that's what I kind of
4 suggest you do in this last viewgraph. Try to collect
5 data from the manufacturer of the equipment for
6 nuclear plants, I listed some of the names that I'm
7 aware of. And another thing to do is contact the
8 plants so that we can --

9 CHAIR APOSTOLAKIS: It seems to me that
10 both comments really you should add to your future
11 activities. At least think about, these were both
12 very useful comments.

13 MR. CHU: Yes.

14 CHAIR APOSTOLAKIS: Okay. That's it?

15 MR. CHU: Yes.

16 CHAIR APOSTOLAKIS: Now you have an
17 interesting sentence here -- you want to say
18 something?

19 MR. NGUYEN: Yes. My name is Thuy from
20 EPRI EDF. In Europe there had been recently a new
21 directive against the use of lead in soldering, and as
22 a result, we had seen new failure modes, new hardware
23 failure modes that due to the new alloys used to
24 solder the electronic components. Have you heard of
25 that? That the industry has called the whiskers

NEAL R. GROSS

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

1 issue. It's because you have very thin metallic
2 whiskers growing from the solder of soldering pots
3 that create short circuits between the legs of the
4 circuits. And so for us, it's a new kind of hardware
5 failure. And there also this notion of single event
6 upsets, which are the fact that now the electronic
7 circuits are so small, the engraving is so fine that
8 you can have, for example, a stray neutron, a stray
9 particle that can create a temporary error in the
10 circuit, that when you restart the system, everything
11 works correctly.

12 CHAIR APOSTOLAKIS: It's probably a higher
13 order problem. Some useful input here.

14 MR. CHU: Yes, thank you for the input.
15 We don't have -- we are not manufacturers, and we
16 don't have easy access to the plants, so these are the
17 limitations, that I suggest that we try to do
18 something.

19 CHAIR APOSTOLAKIS: On page 28 you have a
20 sentence that I found interesting. "Failure mode,
21 specific failure rates are required in the Markov
22 model. However, no such database exists." Now this
23 morning we heard that you can get those. I don't give
24 up, do I? You say "no such database exists."

25 MR. CHU: When I said that, I'm referring

NEAL R. GROSS

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

1 to the type of analysis that's done using the guidance
2 of IEC standard, where you develop Markov models, you
3 talk about fail safe, fail and safe, safe --

4 CHAIR APOSTOLAKIS: Well, that's what we
5 had this morning, didn't we? There were two states,
6 fail safe, and fail unsafe?

7 MR. CHU: Right. But how do you estimate

8 -- CHAIR APOSTOLAKIS: And there were
9 lambdas.

10 MR. CHU: How do you estimate the split,
11 or how do you estimate the coverage?

12 CHAIR APOSTOLAKIS: Yes. That's my
13 question, too.

14 MR. CHU: Right. That's the difficulty --

15
16 CHAIR APOSTOLAKIS: I really think you
17 guys ought to talk to each other more often, because
18 these are interesting comments coming from the same
19 project. And we were told this morning that this will
20 happen, so it's fine.

21 MR. CHU: Yes. I guess tomorrow we'll
22 have a meeting.

23 CHAIR APOSTOLAKIS: You will talk
24 tomorrow?

25 MR. CHU: Yes.

1 CHAIR APOSTOLAKIS: Okay, Louis. What's
2 next? I see your name again. You name is Gerardo?

3 MR. MARTINEZ-GURIDI: That's right.

4 CHAIR APOSTOLAKIS: It's not Gerardo like
5 you were introduced. It's Gerardo, right?

6 MR. MARTINEZ-GURIDI: That's right. I can
7 use both.

8 CHAIR APOSTOLAKIS: Okay. So now we go to
9 the second report, Review of Software Induced Failure
10 Experience. Is that correct?

11 MR. MARTINEZ-GURIDI: That's correct.

12 CHAIR APOSTOLAKIS: Very interesting
13 report, by the way. Now this is here, 30 slides, 31,
14 geez. You need all of them, Gerardo?

15 MR. MARTINEZ-GURIDI: Yes, we'll go over
16 it. Hi, my name is Gerardo Martinez. I work for
17 Brookhaven National Lab. I will be presenting our
18 review of software failures in different industries.
19 The outline of the presentation is to present the
20 general objectives of the project, our approach to
21 reach these objectives. We also developed a
22 preliminary model of software failures that we would
23 like to have feedback from you. Then we'll present a
24 review of the software-related failures at domestic
25 nuclear power plants. At that point, Louis Chu will

NEAL R. GROSS

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

1 take over to talk about the review of events of
2 software failures at other industries and foreign
3 nuclear plants, the scheme for categorizing software
4 failures, a detailed description of selected events.
5 And as you know, a lot of this work was motivated by
6 some ACRS comments, and we will try to address them.
7 Also, discuss briefly some of the methods available
8 for assessing the reliability of software, and we
9 conclude with some conclusions.

10 The main objectives are to get a better
11 understanding of software failures, to present an
12 approach for collecting these kinds of failures, and
13 to try to address ACRS' comments in light of insights
14 doing this in achieving these two objectives.

15 In general, our approach was to search the
16 LER search system.

17 CHAIR APOSTOLAKIS: By the way, you have
18 to be a little careful. Some of these comments were
19 not ACRS. They were not in a formal letter from the
20 committee, so when you address the comments, you have
21 to make the distinction. You understand what I'm
22 saying? If there is a letter from the committee,
23 signed by the chairman of the committee, that's the
24 ACRS position. If you have at the end added comments
25 by a member, that's the member's comments. You can'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 call them ACRS comments, because other members may
2 disagree.

3 MR. MARTINEZ-GURIDI: All right.

4 CHAIR APOSTOLAKIS: I know this is new to
5 you, but the record will have to be careful, I think.

6 MR. MARTINEZ-GURIDI: Okay. I suspected
7 that, but thank you for the clarification.

8 CHAIR APOSTOLAKIS: Okay.

9 MR. MARTINEZ-GURIDI: We also did a search
10 for events in other industries, and we developed the
11 model I mentioned.

12 CHAIR APOSTOLAKIS: These other
13 industries, everybody keeps saying we look at other
14 industries and learned something. Have we ever
15 learned anything from any other industry? We never
16 learn anything.

17 MR. MARTINEZ-GURIDI: Well, one thing that
18 --

19 CHAIR APOSTOLAKIS: Is that true? Did you
20 learn anything besides they don't know?

21 MR. ARNDT: We learned that they have
22 different approaches.

23 CHAIR APOSTOLAKIS: Yes.

24 MR. ARNDT: Frequently what we learn is
25 that they've looked at things, and they decided it's

NEAL R. GROSS

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

1 too hard, and they're going back to simpler models.
2 Frequently what we've learned, and we'll talk a little
3 bit about this particular study, is that for detailed
4 models you need detailed analysis. So we've learned
5 some new things, but mostly we validated things.

6 MR. MARTINEZ-GURIDI: If I jump ahead of
7 myself a little bit --

8 CHAIR APOSTOLAKIS: Please, do.

9 MR. MARTINEZ-GURIDI: Something that we'll
10 learn from looking at failure events at other
11 industries is that software failures can lead to
12 really catastrophic outcomes.

13 CHAIR APOSTOLAKIS: Oh, yes. Sure. But
14 again, you have to be careful about --

15 MR. MARTINEZ-GURIDI: And the kinds of
16 failure modes that happen in other industries are
17 totally applicable to the nuclear industry, as well,
18 so in that sense --

19 CHAIR APOSTOLAKIS: That's a good point,
20 Gerardo. That's a good point.

21 MR. MARTINEZ-GURIDI: Yes.

22 CHAIR APOSTOLAKIS: So let's go to the
23 meat of this.

24 MR. MARTINEZ-GURIDI: Okay. We developed
25 this preliminary model of software failures to

NEAL R. GROSS

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

1 understand better the causes of these failures, and to
2 understand how they propagate in a complex system.
3 The main objectives were to understand these failures,
4 and to establish a basis for eventually developing a
5 model to quantitatively assess the probability of
6 software failure. And at the very top we classify the
7 causes of internal and external, and I will go into
8 that a little bit as we move on.

9 Software failure there can be propagated
10 to the debate, to the devices controlled by the
11 software directly, such as the valves, for example, as
12 it was mentioned this morning, to the entire system in
13 which the software is embedded, and to the overall
14 plant, or overall complex system. The propagation of
15 the failure will depend on several factors, such as
16 the overall context, the overall state of the plant at
17 the time of the software failure, and the tolerance to
18 the software failure of the software, the devices, the
19 system, and the plant.

20 CHAIR APOSTOLAKIS: And that's where,
21 again, I believe the classification we have requested
22 of applications would be very useful. One of the ACRS
23 comments has been please develop a classification of
24 various applications, actuation systems, feedback and
25 control. Like you have some in passing in your

NEAL R. GROSS

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

1 report, real time digital, non-real time digital
2 system, communication failure, so all this stuff that
3 would be nice[^] to have seen. Okay.

4 MR. MARTINEZ-GURIDI: Yes. Well, to
5 mention something about that, that's a task that we
6 don't currently have at the lab, as far as I know. So
7 I am aware that is something is relevant to our
8 project, and that --

9 CHAIR APOSTOLAKIS: I think it is, because
10 you're classifying failures. It would be nice for us
11 to know which particular systems are subjected to
12 certain kinds of failures.

13 MR. MARTINEZ-GURIDI: Absolutely.

14 CHAIR APOSTOLAKIS: Okay.

15 MR. MARTINEZ-GURIDI: Okay. Something
16 that I think is also very relevant is that the
17 potential for dependent failures, common cause
18 failures are also very -- is a relevant issue for
19 software-driven systems because the redundant trains
20 or channels of a system may use the same or similar
21 software. In general, many times they use exactly the
22 same software. And, therefore, if that is the case,
23 then the failure of the software means that all the
24 trains in that system will fail, failing the entire
25 system. So if these dependent or common cause failure

NEAL R. GROSS

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

1 occurs, then it may cause a failure of all the
2 devices, or the entire system. And this is something
3 that has been observed both in the nuclear industry,
4 as well as in other industries.

5 This is our overall model. What we have
6 at the top is the development of the software, the
7 stages in which software is developed, starting from
8 the system engineering and modeling task, which you
9 define what the software is going to be doing, and how
10 it's going to interact with the surrounding system and
11 the surrounding plant. Then you go to a phase of
12 requirements analysis, in which you establish in a
13 more formal way what the software is supposed to
14 accomplish. Then you start in the design phase to
15 turn those ideas into an architecture of the software.
16 Then you move in to generate the actual code. Then
17 once the code is generated, of course, these are very
18 broad steps, and this is simplified model. This is
19 certainly more involved. Then there is some testing
20 of the software, and eventually it's brought into
21 operation and maintenance, and that's --

22 CHAIR APOSTOLAKIS: Our regulatory review
23 right now is really focused on the top five. Right?

24 MR. KEMPER: Yes, that's true.

25 CHAIR APOSTOLAKIS: And we are trying to

NEAL R. GROSS

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

1 bring the lower part back to inform, or to expand the
2 review. Right? We are really focusing a lot on the
3 five boxes you have up there.

4 MR. KEMPER: As far as process for
5 licensing review and licensing - oh, yes. Absolutely.
6 Yes, the top five are the only areas that we can
7 concentrate for a new application, obviously.

8 CHAIR APOSTOLAKIS: Right.

9 MR. KEMPER: Because all the rest of it is
10 subsequent to that.

11 CHAIR APOSTOLAKIS: Yes.

12 MR. HICKEL: But when the equipment is in
13 operation, isn't it true that that box, that next
14 lowest level, O&M, isn't that historically where there
15 have been most of the failures related to the
16 software, and the constants, and all that?

17 MR. KEMPER: That's been my experience,
18 yes.

19 CHAIR APOSTOLAKIS: But when we're
20 licensing, we look at the top five.

21 MR. HICKEL: Yes, but you're all supposed
22 to be looking in the license at the processes and
23 controls that are going to be used once they get it in
24 the field.

25 CHAIR APOSTOLAKIS: Yes.

NEAL R. GROSS

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

1 MR. HICKEL: Because that's where there's
2 less control, in those boxes on the top.

3 MR. KEMPER: Right. That's a
4 configuration management plan or something along that
5 --

6 CHAIR APOSTOLAKIS: Okay.

7 MR. MARTINEZ-GURIDI: So all these stages
8 are usually known as the software life cycle, and it's
9 often interesting to know, that you may already be
10 aware, is that errors made at earlier stages in the
11 development are just going to propagate into later
12 stages, as you know, and compound with errors that may
13 be made at subsequent stages. And once the software
14 comes into operation and maintenance, there may be
15 some faults there which may not necessarily be
16 manifested, latent faults in the software, and that's
17 what we call internal faults, or that's what we call
18 internal causes. These eventually can be triggered
19 and actually occur into a software failure, which is
20 the next box down, the failure of the software, which
21 would include the common cause failure, as I was
22 mentioning before.

23 The failure of the software also can be
24 due to external causes, which is the box on the right,
25 which we categorize into four main types, which would

NEAL R. GROSS

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

1 be one human error, you know, somebody who operates
2 the software in an incorrect way, failure of support
3 systems, such as the hardware in which it runs, the
4 power supplies, HVAC or any other support system that
5 the software requires.

6 CHAIR APOSTOLAKIS: So is it correct to
7 say that the dynamic methods we've heard this morning
8 deal with the four vertical boxes, failure of software
9 all the way down to maybe status of the complex
10 system, but they don't deal with the external causes,
11 at least in the present case.

12 MR. MARTINEZ-GURIDI: I would like them to
13 answer.

14 MR. ARNDT: They don't explicitly deal
15 with external causes. As related to what the
16 operational profile is, the likelihood of having a
17 input that is unexpected by design, it does look at
18 that, in terms of --

19 CHAIR APOSTOLAKIS: But not human error.

20 MR. ARNDT: But not human error or things
21 like that.

22 CHAIR APOSTOLAKIS: Whatever, high
23 humidity.

24 MR. ARNDT: Right. That's not explicitly

25 --

1 MR. ALDEMIR: Tunc Aldemir, Ohio State.
2 We don't deal with external causes in the sense of
3 human error, cyber security, external events, but
4 supporting systems, there is interconnection between
5 the system we are dealing with and the rest of the
6 system. That's what happens when, for example, you
7 hook it up with PRA, the whole PRA. So not
8 intentionally, but partially covered.

9 CHAIR APOSTOLAKIS: Okay. Very good.
10 Thank you.

11 MR. MARTINEZ-GURIDI: And then if we could
12 move down in this diagram, what we tried to depict,
13 again in a simplified way, is how a software failure
14 is going to propagate with the possibility of creating
15 a major accident. So from failure of the software
16 that you could potentially have, a failure of the
17 devices controlled by the software, then the failure
18 of the entire system containing the software, and then
19 that could propagate to have some impact on the plant.
20 And then you could have some recovery. Of course,
21 recovery can be applied at any of these stages of
22 propagation. You can have recovery at the software
23 level, you can have recovery at the device level, you
24 can recovery at the system level, you can recovery at
25 the plant level. And then if the recovery finally

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 fails, then, of course, you may have an accident,
2 otherwise will be avoided.

3 All of these propagation will also depend
4 on the overall context of the plant, the overall state
5 of the plant at which this happens. If the failure of
6 the software happens to happen when there is some
7 unavailability for equipment, then the propagation
8 will be more likely, or more severe. And, of course,
9 these boxes at the bottom is basically operating
10 environment of the software.

11 So, to summarize, we see that the software
12 - we proposed that the software can be analyzed in
13 terms of these two main types of causes, internal
14 causes resulting from the development of the software,
15 and the external causes, which is the environment of
16 the software. And also, the propagation depending on
17 the overall context. And we also acknowledge that the
18 specific context that is relevant for the software is
19 the so-called error forcing context that has been
20 proposed as a triggering mechanism for the failure of
21 software.

22 CHAIR APOSTOLAKIS: I think the dynamic
23 methods we talked about earlier, and the same, I
24 think, idea applies. As I tried to explain what
25 lambda might mean, it's really the occurrence of the

NEAL R. GROSS

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

1 error forcing context, which may trigger the
2 manifestation of a design flaw some place, so it's
3 time-related. Please.

4 MR. MARTINEZ-GURIDI: Okay. Now I will
5 move on to the actual review of software failures at
6 domestic plants. We did this review to identify and
7 gain insights into the nature of these failures in
8 terms of characteristics, such as the specific causes
9 of failures, the associated error forcing context, and
10 to identify any dependent failure, such as common
11 cause failures.

12 Our approach was to identify these
13 failures by using the licensee event report search
14 system. We searched for basically the entire period
15 available, which is from '84 to the end of last year.
16 All plants, all modes of operation, and what we did
17 was to search for the key word "software" in the
18 abstract of the LER. This, of course, leads to
19 somewhat incomplete set, because it's possible that we
20 missed some LERs, but our objective was not to create
21 a complete database, but just to get a sample of the
22 most significant, hopefully, the most significant
23 events that have happened in the industry.

24 The search was complemented with six
25 additional events from NUREG CR 67.34, which is a new

NEAL R. GROSS

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

1 reg that this was specifically written to address,
2 failures in requirement specification, and they
3 identify some additional events. Some of the ones
4 identified in that NUREG we already identified with
5 LER, but there were six additional that we had not
6 identified. And we were aware of an additional event,
7 which was an interesting event, that we also added.

8 CHAIR APOSTOLAKIS: So why weren't these
9 events in the database? I mean, you say you searched
10 the LERs.

11 MR. MARTINEZ-GURIDI: Yes.

12 CHAIR APOSTOLAKIS: Yet six events are in
13 the NUREG report, and also were aware of one. How
14 come it's not in the database?

15 MR. MARTINEZ-GURIDI: You mean how come it
16 was not identified?

17 CHAIR APOSTOLAKIS: I mean, the additional
18 event that you guys were aware of. How comes it was
19 not there?

20 MR. MARTINEZ-GURIDI: Well, it was in the
21 LER search database, but because we only looked for
22 the key word "software" in the asterisk --

23 CHAIR APOSTOLAKIS: Oh.

24 MR. MARTINEZ-GURIDI: So it is possible
25 that there are some additional LERs that have the

1 software -- maybe, for example, one possibility is
2 that they didn't use the word software. The people
3 who wrote the LER might have used computer code
4 instead of the word "software".

5 CHAIR APOSTOLAKIS: Well, why didn't you
6 use computer code as a key word?

7 MR. MARTINEZ-GURIDI: Well, the problem is
8 that there are many possible words that can be used,
9 so if we use all those we would end up with a very
10 large number of LERs. And we didn't have the
11 resources to go over those --

12 CHAIR APOSTOLAKIS: So on the one hand we
13 complain we don't have sufficient data, and on the
14 other hand you say -- that's okay. Keep going. Now
15 you tell me when to stop for a break. You decide what
16 is a logical place to do this.

17 MR. MARTINEZ-GURIDI: I think that will be
18 when I finish this, before Louis takes over.

19 CHAIR APOSTOLAKIS: Is that within a
20 reasonable amount of time? You're talking about five
21 minutes or so?

22 MR. MARTINEZ-GURIDI: I can stop at any
23 time, of course.

24 CHAIR APOSTOLAKIS: You can stop any time?

25 MR. MARTINEZ-GURIDI: Yes.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: Okay. So it's up to
2 me, then. Okay.

3 MR. MARTINEZ-GURIDI: Okay. Shall I
4 continue?

5 CHAIR APOSTOLAKIS: Yes, please.

6 MR. MARTINEZ-GURIDI: So using this
7 process, each LER that was identified using the search
8 was reviewed individually. And those LERs that
9 actually documented a software failure were selected
10 in the database, so we ended up with 113 LERs that
11 documented some sort of software failure. And these
12 database we characterize these failure events in terms
13 of basically some basics, such as the unit that was
14 involved and so on, but more importantly, we provide
15 a brief description of the software failure, its main
16 causes, its consequences, the error forcing context
17 and whether it was an independent failure.

18 Some means, as we learned, was that 71
19 different nuclear units have at least one event
20 related to software failure during the period that we
21 studied, so software failures have occurred in a
22 significant number of units. And as a conclusion, we
23 see that it's quite likely that any plant that uses
24 software supported systems could experience a software
25 failure.

NEAL R. GROSS

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

1 Out of those 113 LERs, there were 17 that
2 documented two units, so the software failure was
3 applicable not to a single unit, but two units, so
4 overall we found 130 software failures.

5 Then I searched the last 10 years of the
6 software failures we identified, which is comprised of
7 45 LERs, to try to classify them in terms of what was
8 the software failure mode, and the cause of the
9 failure. And what we found was that in 69 percent of
10 the cases, the software failed with a failure mode, it
11 runs but it^v generates a run results which are not
12 necessarily evident.

13 CHAIR APOSTOLAKIS: So this is the fail
14 unsafe mode that we were talking about earlier?

15 MR. MARTINEZ-GURIDI: I would say this is
16 certainly --

17 CHAIR APOSTOLAKIS: I mean, this is the --
18 the guy from Virginia, Carl. This is one minus your
19 coverage.

20 MR. ELKS: Yes, this would have to be
21 definitely --

22 CHAIR APOSTOLAKIS: Yes, one minus the
23 coverage.

24 MR. ELKS: You have to put this in the
25 system. Error detection mechanism didn't --

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: No, no. You have to
2 come here. I'm sorry. Repeat everything you said
3 since this morning.

4 MR. ELKS: Okay. (Laughing.) It won't
5 take long. In the context of our definition of
6 coverage, which we stated this morning, this would be
7 an uncovered fault. Exactly.

8 CHAIR APOSTOLAKIS: That's a pretty high
9 number, isn't it?

10 MR. ELKS: Yes, 31 out of 45 events. We
11 don't know what the total operational time that these
12 things, 20, 30, 40 years, maybe hundreds of years of
13 operational time. Ten years, okay. So it's a fairly
14 high number out of an event, I would say.

15 MR. MARTINEZ-GURIDI: Well, something that
16 I think is very important to take into account is that
17 these failures cover everything, both safety-related
18 and non-safety-related systems. And possibly most of
19 the failures occur --

20 CHAIR APOSTOLAKIS: Well, your
21 classification is important.

22 MR. MARTINEZ-GURIDI: We'll be happy to
23 take it up for you at Brookhaven. My impression is
24 that most of the failures occur in non-safety-related
25 systems, that may not even have any fault tolerant

NEAL R. GROSS

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

1 features, may not have coverage at all, or may have a
2 very low level of coverage.

3 CHAIR APOSTOLAKIS: But, Gerardo, then I
4 would expect you to put a couple of sentences to that
5 effect in the report, because I don't see that
6 anywhere. And all I see is 31 out of 45, and that's
7 kind of --

8 MR. MARTINEZ-GURIDI: In the report it is
9 mentioned that we believe that most of the failures
10 are in non-safety-related systems.

11 CHAIR APOSTOLAKIS: But that's somewhere
12 else. It's not where it should be.

13 MR. MARTINEZ-GURIDI: You mean --

14 CHAIR APOSTOLAKIS: I'm sure in a report
15 of this size it's somewhere, but when I look at the
16 heart of it, conclusion C.1, you're saying "69 percent
17 had the failure mode runs with wrong results that are
18 not evident", and there you don't say anything else.
19 That's pretty scary. You should put these qualifiers
20 there, because a lot of people look at the actual
21 conclusions.

22 MR. MARTINEZ-GURIDI: Thank you for your
23 comment.

24 CHAIR APOSTOLAKIS: You are very welcome.
25 Okay.

1 MR. MARTINEZ-GURIDI: Well, another point
2 is that we think it is maybe a reason for concern to
3 have software that is running, we run this stuff
4 sometimes for pretty long periods of time, and just
5 generating incorrect results.

6 CHAIR APOSTOLAKIS: I'm sorry. You say
7 that later. ↘ It is later in the report.

8 MR. MARTINEZ-GURIDI: Yes, it is there.

9 CHAIR APOSTOLAKIS: Okay. We're going to
10 go to the causes of failure, the main cause was
11 software requirements analysis with 16 hits, about 36
12 percent. As you may already know, the software fails
13 to do its function because it was not designed to
14 perform that function.

15 Another perhaps more surprising result is
16 that operation and maintenance also had a pretty high
17 percentage of failures with 27 percent, and these were
18 events that were -- these were problems, issues
19 introduced while the software was brought operational
20 into the field, and then somebody somehow made some -
21 perhaps with the best intention did some upgrade
22 thinking that they were going to improve the system,
23 and it turned out that perhaps they improved what they
24 were trying to improve, but the software failed for
25 other reason.

↘
NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 In many cases we were able to identify the
2 error forcing context. However, in some cases,
3 perhaps all again due to the fact that systems are
4 non-safety related, the software didn't really perform
5 its function from the start of its operational life.
6 And it may remain hidden for a long time, perhaps
7 several years. And also, what we saw from the
8 operational experience is that the failure may be
9 discovered by indirect means, such as somebody perhaps
10 noticed some problem somewhere else, did some
11 calculation, and in the process of troubleshooting,
12 they found out that there was a problem, and
13 eventually traced it down to software.

14 In a fairly large percentage also, about
15 26 percent, there was some type of dependent failure,
16 including common cause failure. And additional 13
17 LERs potentially also involve dependent failures. We
18 are not sure because we couldn't -- the LER didn't
19 have enough information to find out whether that was
20 actually -- 25 positively where there was actually a
21 dependent failure. So it was clear that the potential
22 of software failures to cause dependent failures is
23 the most rated, and that since dependent failures can
24 be a significant to risk, then software failures also
25 have the potential to be a significant contributor.

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 think I can stop at this time, if you
2 think it's --

3 CHAIR APOSTOLAKIS: Thank you.

4 MR. MARTINEZ-GURIDI: Thank you.

5 CHAIR APOSTOLAKIS: We'll reconvene at
6 2:55.

7 (Whereupon, the proceedings went off the
8 record at 2:39:45 p.m. and went back on the record at
9 2:59:36 p.m.)

10 CHAIR APOSTOLAKIS: Take your positions.
11 Okay, Louis. Tell us what is going on here.

12 MR. CHU: Okay. I'll continue the
13 presentation. I'll start with review of events in
14 other industries and foreign nuclear power plants.
15 Summarize how we search for events, internet search is
16 the most important part of our method for identifying
17 software-induced failures, and I provided some example
18 websites containing descriptions of events, or
19 references to details of the events. Just like other
20 internet searches, they tend to -- one thing lead to
21 another. You identify one -- you look up one event,
22 and then at the same time, you find ten other events,
23 so kind of the number of events you can find grows
24 quickly. But you find from different sources there's
25 significant overlap, also.

NEAL R. GROSS

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

1 We used our judgment to pick certain
2 events that we feel that are interesting, and we did
3 some more detailed analysis. The aviation accident is
4 an area where we did more thorough search; that is,
5 the NTSB Aviation Accident Database was reviewed to
6 identify software-related failures. We also looked at
7 NASA website, which provide description of NASA
8 missions, and some of the missions involve failures,
9 and software failure was the cause.

10 In searching the internet, of course, we
11 come across many news media, newspapers, magazines,
12 and university websites. And information about the
13 events, the level of detail varies a lot. In some
14 cases, it could be two sentences in the form of an
15 email, and then you search more for it, you cannot
16 find anything. In some cases, there are more detailed
17 official reports. These are basically how we search
18 for events in other industries.

19 In terms of foreign nuclear experience, we
20 basically make use of this NEA report that provides
21 descriptions of some digital-related failures.
22 COMPSIS is a database that's being developed, and
23 currently my understanding is that they are still
24 developing guidelines and database structures. From
25 that international operating experience on digital

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 systems will be collected.

2 CHAIR APOSTOLAKIS: Several years ago
3 there was an international corporation that was
4 established to look at common cause failures for
5 hardware, which apparently did very well. Is there
6 any thought to have something like this on digital
7 software?

8 MR. ARNDT: The common cause database is
9 sponsored by the same organization that is sponsoring
10 the COMPSIS database program, so there is some
11 interplay between the people who are working on both
12 the data structures for COMPSIS, as well as the data
13 associated with that. They're both OECD.

14 CHAIR APOSTOLAKIS: But we are
15 participating in this COMPSIS.

16 MR. KEMPER: Yes, definitely. In fact,
17 I'm filling in for the project manager, who just got
18 promoted, right now. Went to a meeting just a couple
19 of months ago in Korea, and we talked about this. And
20 Louis is right, we're right in the middle of
21 developing guidelines, coding guidelines and the user
22 interface at this point, which will ultimately be
23 available to everybody in the agency, hopefully, from
24 a data acquisition point of view. But there's about
25 17 international regulators and research organizations

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 participating in that right now.

2 CHAIR APOSTOLAKIS: Is the industry
3 participating in any of this?

4 MR. KEMPER: Not at this time. We're
5 still kind of kicking around ideas about participation
6 and accessibility of the data. Right now, it's kind
7 of protected, because a lot of -- some organizations
8 across the world, they just don't want to share the
9 failure data within their country, unless there's a
10 reciprocity type of arrangement. But it's going to
11 focus primarily on nuclear installed devices, that's
12 the idea with COMPSIS.

13 MR. CHU: A little bit about screening of
14 the events. Basically, in our search, we found a huge
15 number of software-related failures, and we used
16 judgment to pick some events that we think are
17 interesting. Many of the events selected just based
18 on their severity, the consequence of the failure.
19 Some events were selected because they represent
20 interesting failure modes, the failures associated
21 with communication, or cyber security-related events.
22 Some events were selected, such that we covered some
23 specific industries.

24 In the end, we analyzed 48 events in 10
25 different industries. For each of these events,

1 basically we tried to get detailed description of the
2 event, and write up a description. And then we tried
3 to categorize the failure modes of the software
4 failures, and failure causes, failure consequences of
5 these events, that as we develop, get a duration
6 scheme for software failure mode and failure causes.

7 In addition, we tried to identify the
8 sequence of events that trigger the software failure.
9 In some cases, the precise sequence of events can be
10 identified, in other cases it's just not clear, but
11 it's obvious software error was involved.

12 I'll talk a little bit about how we
13 categorize software failure events based on failure
14 mode and failure causes. In general, it is hard to
15 define, to narrow software failure modes, because
16 failure modes may depend on the function of the
17 software, and also depends on the level of detail at
18 which you are talking about software failure. So in
19 addition to reviewing software-induced events, we also
20 did a literature review of software FMEAs, and see how
21 other people define software failure modes, or if they
22 do causes, and try to make sure the failure modes and
23 failure causes that we have covers all those that
24 others have identified.

25 Often in our review, we've often found

NEAL R. GROSS

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

1 that the terms, the definition of failure causes,
2 failure modes, and failure effect can be easily mixed
3 up; that is, one failure cause may be the failure mode
4 of some other study. A possible reason has to do with
5 the level of detail. In a way, low level failure mode
6 could be the trigger cause of a higher level.

7 By reviewing the events, and reviewing the
8 literature, we came up with our way of categorizing
9 the events. This table shows the high level failure
10 modes we have defined. Essentially, we tried to
11 define the modes in terms of the behavior of the
12 software. And think of software could be a
13 complicated system, consisting of elements, and then
14 the elements can further be broken down into sub-
15 elements, sub-elements can further be broken down, so
16 based on that kind of thought.

17 MEMBER BONACA: I have a question
18 regarding -- I mean, clearly, digital software in
19 nuclear applications has specific requirements, and
20 there are software requirements that are very specific
21 in so far as verification, validation, and so on and
22 so forth. To what levels do these kind of standards
23 apply to the other databases that you looked at?

24 MR. CHU: I'm not sure I understand the
25 question. Could you elaborate on that?

1 MEMBER BONACA: I'm saying in nuclear
2 applications, software is subjected to specific
3 requirements, which include verification, validation,
4 testing, independent verification, a lot of steps to
5 assure the quality of the software that's being
6 implemented, and I'm just wondering about the other
7 software that you looked at; are they subjected to
8 similar requirements?

9 MR. CHU: We didn't specifically look into
10 the specific requirement of other industries. I
11 imagine there's a lot of variations in the industry,
12 or in the military, aerospace, because more safety-
13 critical systems are there. There might be more
14 stringent requirement, but in our look, we didn't. We
15 just looked at how failure occurred, and tried to
16 categorize based on what happened.

17 MEMBER BONACA: Okay. So you don't have
18 a sense of what the requirements may be. They may
19 vary significantly from one application to another.

20 MR. CHU: Right.

21 MEMBER BONACA: All right.

22 MR. CHU: Okay. In this table at the high
23 level, the left column, basically we call it system
24 level failure mode. It's defined based on whether or
25 not the software stopped running, and whether or not

NEAL R. GROSS

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

1 software failure occurred with a clear indication, so
2 this relates to whether or not you can observe the
3 failure, whether or not you're aware that failure
4 occurred.

5 At the element level, we defined five
6 software elements. They are kind of based on the
7 function of the elements, input, output,
8 communication, resource allocation, and processing.
9 And for each of these elements, we have element-
10 specific failure modes that are shown on the next
11 viewgraph. And this viewgraph shows generic failure
12 modes that are generically applicable to all the
13 software elements.

14 This graph shows the element-specific
15 failure modes. For example, communication failure
16 mode could be failed interaction in sub-routine calls
17 or in data communications. Resource allocation could
18 be competing for resources, priority errors. Software
19 failure causes, similarly we define software failure
20 causes. For internal causes, we basically relate
21 those causes to stages in the software life cycle.
22 Essentially, faults were introduced and not detected
23 during the development process, so they are due to
24 errors in the development stages. And for each event,
25 we tried to identify possible stages in 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 development of software where error was introduced.
2 And these software faults are introduced during the
3 development stages, and that is the quality of the
4 software depends on how good a job you've done in
5 developing it in each stage of the life cycle.
6 Therefore, somehow, if we want to develop some
7 quantitative software reliability model, we are going
8 to make use of this kind of information, how good a
9 job have you done in developing the software. So this
10 kind of failure cause categorization can potentially
11 help with that kind of work. This is just some high
12 level failure causes. In our report, we have more
13 detailed examples for each category of failure causes.

14 Some insights, review of software-induced
15 failures in other industries. In general, events that
16 took place in other industries, that ones that we
17 analyzed in detail, tend to be more exciting, or have
18 much more serious consequence, because you're getting
19 events from a wider source from many other industries.
20 And, in general, I would say the same type of failure
21 could happen in the nuclear industry. Of course,
22 keeping in mind that nuclear industry, the safety-
23 related system, there might be better -- but in terms
24 of say developing model, that kind of factor can be
25 taken into consideration.

NEAL R. GROSS

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

1 Some insights - incorrect implementation
2 and omission of function are important failure modes.
3 Error due to requirement analysis stage are the most
4 important failure causes. The occurrence of error
5 forcing context triggering a software failure is a
6 reasonable way of considering software failures; that
7 is, the software failure rate effectively is the rate
8 at which the error forcing context occurred.

9 In some software failure events, we
10 recognize that the failure occurs at the very low
11 level. In one case, a bit stuck at one or zero
12 trigger a sequence event causing a pretty serious
13 accident. And so the implication is that in order to
14 capture this kind of problem, you need to develop a
15 pretty detailed level of model.

16 Some software failures involve softwares
17 that are not application softwares. The operating
18 system, the diagnostic software, communication
19 software, so to capture this kind -- to identify this
20 type of software faults or failures is quite
21 difficult. And in quite a few instances we did find
22 software common cause failures, the fact that
23 identical hardware used identical software.
24 Man/machine interface is a contributor to some of the
25 events.

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 some description, a reasonably
2 detailed description of four events, but they are
3 pretty detailed. I hope that I don't need to explain
4 them, every one in detail, because it's going to be
5 pretty time consuming. But these four events all took
6 place at nuclear power plants. The first three
7 occurred in domestic plants, the fourth one occurs in
8 Bill's Canadian plant. And they all involved software
9 failures. For the three events at domestic plants,
10 they all involve software associated with redundant
11 equipment, like diesel generator sequencers, core
12 power calculators, and regulating voltage regulating
13 transformers. They all have identical hardware
14 running identical software, so in principle, common
15 cause failure could lead to failure of redundant
16 equipment.

17 Maybe I'll try to explain each of these
18 events quickly. Turkey Point diesel generator
19 sequencer - it was during a test that they found that
20 there's a software logic error, such that high
21 pressure injection pump wouldn't start. This was
22 discovered during a test. But my understanding is,
23 before this was discovered, earlier there was another
24 LER reporting pump failed to start event. And at that
25 time, they couldn't tell what was the reason the pump

NEAL R. GROSS

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

1 failed to start. And when they recognized this
2 problem, they went back and identified that this was
3 the cause of that earlier event, so this is
4 interesting.

5 Another thing is, again, my understanding
6 is that it seemed to say it can happen only when you
7 are testing, but if you look at that earlier event, it
8 was actually a real signal. There is a real actuation
9 signal, and the system failed, or the pump failed to
10 start, so this issue might happen with reasonable and
11 high likelihood. Of course, problem - you discover
12 the problem and the bug is removed, and it's no longer
13 a problem.

14 CHAIR APOSTOLAKIS: Let's go back. You
15 say the error forcing context is the test?

16 MR. CHU: During test - okay, the error --

17
18 CHAIR APOSTOLAKIS: That's when they found
19 it. But the first bullet under consequences says that
20 even if it was a real event, you would not have
21 responded properly to an SI signal, and units 3 and 4
22 were operating outside their design basis.

23 MR. MARTINEZ-GURIDI: What happens is the
24 sequencer can operate in different operational modes,
25 and there was some kind of switching where you can

NEAL R. GROSS

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

1 select which[^] operational mode. And usually, it was
2 selected to be in an automatic test mode, so in a way
3 the sequencer was always in this automatic test mode.
4 So should a real signal come, it will most likely find
5 it in a test mode, and, therefore, it will fail to
6 actuate. That's actually what happened in the
7 previous LER that he was describing, that's exactly
8 what happened. And they couldn't find out -- they
9 didn't realize there was this connection of events.
10 But then with the second event, they realized that
11 every time the[^] sequencer was in some kind of test
12 operational mode, it will have this vulnerability,
13 that it will not respond to a real signal.

14 MR. HICKEL: Was the fault unique to a
15 software system, or was it unique to the function that
16 was being implemented?

17 MR. MARTINEZ-GURIDI: Well, it was
18 certainly a software problem.

19 MR. HICKEL: If I took the same function
20 and implemented it using a bunch of AGOSTAT relays, if
21 I could find them on eBay or something like that, I
22 would not have this problem, it was unique to
23 software?

24 MR. MARTINEZ-GURIDI: My understanding is
25 that it was unique to software. The thing is that I

NEAL R. GROSS

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

1 cannot give you a positive answer, because this kind
2 of detailed information, in most cases, was not in the
3 LER itself, so we didn't know, have all the details to
4 tell. But it was clearly stated that the problem was
5 in the software.

6 MR. CHU: This is an example, we're
7 limited to the information that's available in the
8 LER. In some cases, you find some description of the
9 event. They identify some failure, and then they said
10 they sent the circuit board to the manufacturer for
11 diagnosing it, and then we don't know what happened,
12 so there are technical situation, too.

13 CHAIR APOSTOLAKIS: So, Gerardo, you say
14 the problem was that the sequencer was continually on
15 --

16 MR. MARTINEZ-GURIDI: On a test mode.

17 CHAIR APOSTOLAKIS: Test mode. And who
18 did that?

19 MR. MARTINEZ-GURIDI: The plant decided to
20 put it in that mode.

21 CHAIR APOSTOLAKIS: So is it because they
22 did not understand what that meant, or it was just a
23 slip? Because that's really, it seems to me, the
24 error forcing context.

25 MR. HICKEL: That's right.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: Right?

2 MR. HICKEL: Yes.

3 CHAIR APOSTOLAKIS: Not that the sequencer
4 is executing the test, is that somebody put it in that
5 automatic loop where it was self-testing all the time.

6 MR. MARTINEZ-GURIDI: But it was not an
7 error. It's possible that the plant believed that put
8 it in this operational mode was the safest way to have
9 it, so it would be operational - continually being
10 tested.

11 CHAIR APOSTOLAKIS: So the error forcing
12 context then was not understanding what it meant to
13 have it in that mode. That's the error forcing
14 context.

15 MR. MARTINEZ-GURIDI: But, perhaps, that
16 was the mode in which the sequencer should be.

17 CHAIR APOSTOLAKIS: Then there was a
18 design error.

19 MR. HICKEL: I was going to say, it's hard
20 to believe that somebody delivered a sequencer, and
21 they didn't run a test to see that it sequenced the
22 loads on the diesel at least once. So this has to be
23 a mode where it was not the normal standby mode of
24 operation.

25 CHAIR APOSTOLAKIS: But the reason why I'm

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 bringing that up is because it's important to
2 understand what the error forcing context is.

3 MR. MARTINEZ-GURIDI: Yes.

4 CHAIR APOSTOLAKIS: You really have to
5 look for the context that creates this error, so
6 either they didn't understand it, and that's the
7 error, or there was a design error. I don't know.
8 And if they were advised to do this, then whoever
9 advised them did not have all the information as to
10 the behavior of this. You have to look a little more
11 deeply into what is the context within which the
12 software does something wrong.

13 MR. CHU: The next event is an actual
14 common cause failure that took place at Pilgrim. It
15 involved loss of multiple vital AC buses. That
16 happens during a storm, such that there is power
17 transient, a voltage transient. Their regulating
18 transformer was designed to regulate the input voltage
19 within 20 percent of the nominal value, 480 volts.
20 That is, if the voltage goes beyond that range, it
21 just automatically tripped the transformer, and as a
22 result, you would lose the vital AC bus. It happens
23 during that event some of the voltage goes below 350,
24 and indeed, that caused tripping of the transformer,
25 and loss of multiple vital AC buses.

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 Core protection calculator problem at Palo
2 Verde. This appears to be just a software was written
3 not following the requirement specification; that is,
4 the core protection calculators take analog inputs and
5 compare it with some set point and determine if a trip
6 is needed. The design is such that when two input
7 modules are unavailable, core protection calculator
8 should generate a trip signal, but it didn't. It was
9 programmed to use the last known good value of the
10 input, so it seemed to me, it's a simple error of not
11 program following the requirement specification. This
12 type of failure, of course, is a potential common
13 cause failure, too. To trigger its failure, you have
14 to lose the two analog channels, which is probably
15 random, so it's not that likely you'll have redundant
16 failures because of this software failure.

17 Ontario Hydro's refueling accident - this
18 is an accident that involved quite a few independent
19 events; that is, you have combination of four or five
20 events that appear to be independent to trigger the
21 failures. And as a result, there's a small loss of
22 coolant accident. What happened was that the CANDU
23 reactor can perform refueling while the reactor is on-
24 line. They way it's done is that you have a fuel
25 channel. You connect one fuel machine to one end, and

NEAL R. GROSS

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

1 another to the other end, and then you connect the
2 fuel machine to the fuel channel such that it become
3 part of pressure boundary, and you push from one end.
4 You push the old fuel out, and the new fuel in, and
5 then you reseal the ends.

6 During this accident, what happened is one
7 fuel machine was clamped to the fuel channel, and
8 something went wrong with the control, such that a
9 spurious, some stimulate independent event triggered
10 movement of the grade of the bridge, such that when
11 it's clamped and you try to move it, it created a
12 small LOCA. The combination of events that led to
13 this involve, first, there is a software fault in the
14 error handling software; that is, somehow the return
15 address wasn't specified correctly. It was specified
16 such that at the end of this error handling, it will
17 go through the routine that will move the crane. And
18 that's one event.

19 And then, first, you have to have an error
20 on the computer, depend on trigger error handling such
21 that the address will be pointing to the wrong place.
22 And then this machine, this computer actually was not
23 used to control the fuel machine that's already
24 clamped. It's used to control some other things, but
25 it was used to control this machine earlier, but still

NEAL R. GROSS

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

1 it was connected. The control is still connected to
2 the fuel machine, such that when someone using this
3 computer to control some other things, he generated an
4 unrelated error, but it triggers the error handling
5 routine, an error handling routine at the end
6 transferred to the movement of the fuel machine.

7 Another independent event is there should
8 be another protected computer there that should detect
9 this kind of situation, and prevent it from occurring,
10 but that computer was out-of-service at the time, so
11 there are kind of four or five independent events.

12 CHAIR APOSTOLAKIS: Are they allowed to
13 operate with this computer out-of-service? Was this
14 a violation, in other words?

15 MR. CHU: I didn't see description of any
16 violation.

17 MR. HICKEL: It probably had a procedure
18 that said if the computer is out-of-service, you must
19 manually do what the computer was going to do. That's
20 typical.

21 MR. CHU: So these are some of the nuclear
22 events. And then there are many other events in other
23 industry. Some involve much serious accident. The
24 blackout that took place two or three years ago has to
25 do with some rates conditions. It was reported in one

NEAL R. GROSS

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

1 book written by a former CIA employee that CIA planted
2 a virus in software that the Soviet Union bought, and
3 it caused an explosion in a natural gas distribution
4 system, and it was a huge explosion that the satellite
5 actually detected the explosion. At the time, it was
6 during the Cold War period. Initially, we were
7 thinking maybe they are launching a missile. This is
8 reported only in that book. It was discussed in some
9 newspaper articles, but there was no official
10 acknowledgment of the event. So kind of that's
11 interesting.

12 And water treatment system at an
13 Australian location, they have some computer control
14 of their system, and the company, they hired a company
15 to install the system. That company has an employee
16 that for some reason left the company, but decided to
17 cause some trouble, and he set up some wireless
18 control of the water treatment plant, such that in 40
19 instances that he just opened the sewerage, such that
20 it dumped sewerage into the river, or into a park.
21 Eventually, he was caught when the police saw him
22 doing something with a computer at the site boundary.

23 CHAIR APOSTOLAKIS: Again, I think these
24 incidents would make much more sense within the
25 classification system that classifies 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 applications.

2 MR. CHU: Yes. I guess, like one example
3 about virus is the Davis-Besse event, where there's a
4 virus that was introduced to the plant network,
5 because they allowed some consultant access to the
6 internet of the plant. So that's another virus-
7 related event.

8 CHAIR APOSTOLAKIS: Okay, Louis.

9 MR. CHU: Let's move on.

10 CHAIR APOSTOLAKIS: What else? By the
11 way, this classification of failure modes, on page C-
12 33 of the Reliability Modeling Report, there is a
13 classification scheme, which I'm not sure is
14 consistent with what you are doing. So that's
15 something you guys want to look into.

16 MR. CHU: Yes.

17 CHAIR APOSTOLAKIS: Okay. So where are
18 you now, discussion of ACRS comments?

19 MR. CHU: Yes. This viewgraph, basically
20 this task was carried out --

21 CHAIR APOSTOLAKIS: What was the comment?
22 You are telling us what you did, but what was the
23 comment?

24 MR. CHU: I guess it's a comment from one
25 ACRS member.

1 CHAIR APOSTOLAKIS: No, no, no. What was
2 the comment, not whose comment it was, what was the
3 comment?

4 MR. CHU: One is looking at failure
5 experience to identify --

6 CHAIR APOSTOLAKIS: Okay, yes.

7 MR. CHU: -- the failure mode frequencies.
8 So we did this task in response to that comment. We
9 developed a preliminary model of software failure,
10 basically it give us high level picture, how we see
11 software failure occurs. And we viewed operating
12 experiences, and we developed a way of categorizing
13 events. And regarding modeling of software failures,
14 we feel it's reasonable to model it probabilistically,
15 because the frequency is the same as the frequency of
16 the triggering event. The question is how you
17 estimate such frequency, but conceptually, I don't see
18 a problem.

19 CHAIR APOSTOLAKIS: Are you talking about
20 the fourth bullet now?

21 MR. CHU: Yes.

22 CHAIR APOSTOLAKIS: Well, I don't know how
23 the statement of the constant failure is a reasonable
24 assumption follows from what you've told us. Let's
25 take the Turkey Point incident. I mean, I don't see

NEAL R. GROSS

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

1 where a failure rate could play a role there. The
2 thing was useless, because it was constantly self-
3 testing, so what is the failure rate? I mean, that
4 was an error introduced from the beginning, and as you
5 say in your slide, they were actually operating
6 outside their design basis. I don't think that your
7 statement there is supported by the evidence you have
8 collected.

9 MR. CHU: The failure rate in that case
10 would be the frequency that you have --

11 CHAIR APOSTOLAKIS: SI?

12 MR. CHU: Right. You have a demand.

13 CHAIR APOSTOLAKIS: No, because in a PRA,
14 you would, under certain conditions, have the safety
15 injection signal. Right? And then the next question
16 is, what happens, is it executed correctly and so on,
17 so you will need the probability there. The signal
18 will come anyway, so the probability now is one that
19 the sequencer will not respond correctly.

20 MR. CHU: Yes. It depends on where you
21 start your calculation. There is a sequence of events
22 that led to this SI signal.

23 CHAIR APOSTOLAKIS: Right.

24 MR. CHU: So the frequency of that
25 sequence of events effectively is the frequency of

NEAL R. GROSS

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

1 this failure.

2 CHAIR APOSTOLAKIS: Yes, but this is
3 because you know that the thing will not respond. But
4 when I do the PRA, I'm doing a prospective analysis,
5 so now the signal comes, and I know it has to be
6 processed by software. What am I going to say?
7 You're saying that in that particular case, it
8 happened that the conditional probability was one, but
9 that does not justify a constant failure rate.

10 I would say your first statement, the
11 frequency of the EFC occurs, makes sense in some
12 cases. In other words, the software operates, and
13 then a set of conditions occurs, for which it was not
14 designed, for example. Then the frequency of failure
15 is the frequency of those conditions occurring.
16 Right?

17 MR. CHU: Right.

18 CHAIR APOSTOLAKIS: It makes sense to have
19 a rate there, but not in the Turkey Point case . It
20 was useless. Any frequency that demanded operation
21 from the sequencers was bound to -- I mean, would lead
22 to a failure. There is a subtle difference, I think.
23 Put yourself in the situation where you're actually
24 trying to do a PRA, and now you have, in this new
25 world, you have to consider the digital system as part

NEAL R. GROSS

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

1 of the system, the whole system, the response of the
2 plant. Digital system is useless in this case.

3 MR. CHU: Right.

4 CHAIR APOSTOLAKIS: And it's not because
5 of the context. The context is not something that
6 applies to everything. I mean, based on what you have
7 found, it seems to me that it's not something that is
8 useful in general. In some instances, it is. Like,
9 the classic example where airplane, the pilot tried to
10 lift the landing gear when the plane was on the
11 ground. I mean, there you can say yes, the software
12 has nothing to do with this. It was used in a context
13 for which it was not designed, although you might say
14 the designer should have predicted that. Okay? So it
15 depends on how you look at it. But in this case with
16 the sequencer, it seems to me the context has nothing
17 to do with anything. It was just an error.

18 MR. CHU: It is the sequencer event that
19 led to the SI signal. But in case of PRA modeling, I
20 agree that we need to look at, maybe instead of the
21 model that in terms of probability.

22 CHAIR APOSTOLAKIS: Well, as we were
23 discussing earlier, if the error forcing context was
24 the misunderstanding of what the self-testing mode
25 meant, then you might say the frequency of 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 misunderstanding is a rate, but I think we're
2 stretching it a little bit.

3 MR. MARTINEZ-GURIDI: I think that
4 something that is very important is that, as we
5 discussed previously, there are some instances in
6 which basically the software failure is already, is
7 there all the time, basically since they installed the
8 software. ↘

9 CHAIR APOSTOLAKIS: Right.

10 MR. MARTINEZ-GURIDI: In that case,
11 there's been no sense -- much sense in the failure
12 rate. I believe that's what you mean to say. And the
13 other case in which you have a software failure which
14 is latent, and some error forcing context comes later,
15 and then it triggers the thing.

16 CHAIR APOSTOLAKIS: Exactly. And I'm very
17 pleased, actually, that we're having this discussion,
18 because I think we're really getting to understand
19 much better what is going on, and what we want to
20 model. We have to be very careful what we mean by
21 error forcing context, and what is the rate. So under
22 certain conditions, I agree, there is a latent error,
23 and under certain conditions it becomes real. Maybe
24 the rate of occurrence of these conditions then makes
25 sense to use, but in other cases, maybe it doesn'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 So that's something for future thinking.

2 MR. CHU: Yes, we have a next test to look
3 at this kind of issue.

4 CHAIR APOSTOLAKIS: Yes, and that's great.

5 MR. CHU: Your comment certainly will be
6 helpful. We'll try to account for all this.

7 MR. MARTINEZ-GURIDI: Yes, but I think the
8 discussion also illustrates that it's sometimes, or
9 many times it's very difficult to identify in advance
10 when we try to do a PRA, what is going to be the error
11 forcing context that are out there.

12 CHAIR APOSTOLAKIS: Absolutely.

13 MR. MARTINEZ-GURIDI: I mean, there are so
14 many possibilities, that it's a humongously difficult
15 thing --

16 CHAIR APOSTOLAKIS: You can talk to the
17 HRA guys how they do it. In fact, tomorrow we'll
18 discuss it. They start with a basic scenario, they
19 consider deviations from the scenario, and then they
20 ask themselves how likely are these things, they rely
21 on expert opinion a lot. And I'm not saying you should
22 do that, but that's one input to the process, because
23 those guys have spent a lot of --

24 MR. MARTINEZ-GURIDI: I --

25 CHAIR APOSTOLAKIS: Of course, when you

NEAL R. GROSS

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

1 deal with humans, it's a different situation. It's
2 not --

3 MR. MARTINEZ-GURIDI: Yes, it appears to
4 me that for software, it's even a more complicated
5 issue, because software operates --

6 CHAIR APOSTOLAKIS: More complicated
7 than human behavior? I don't know. I don't know.

8 MR. MARTINEZ-GURIDI: Because it operates
9 at an even lower level. It takes inputs at the very
10 lower level, it just takes data, so it's just a
11 humongously difficult problem.

12 CHAIR APOSTOLAKIS: Anyway, I disagree
13 with that second sentence in the fourth bullet. I
14 think it needs more thinking, so let's go on to 27.

15 MR. CHU: Identification of error forcing
16 context is difficult, in general.

17 CHAIR APOSTOLAKIS: It's difficult, sure.

18 MR. CHU: So there's always some faults
19 remaining in the software. On the issue of system
20 centric versus software centric viewpoints, system
21 centric viewpoint includes interactions of the
22 software with the rest of the plant. Conceptually, by
23 considering the interaction, it is possible to
24 identify many of the error forcing context. But a
25 general issue still, I think, is difficult to, or is

NEAL R. GROSS

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

1 impossible to claim that one can find all the error
2 forcing context, all the faults in the software.

3 CHAIR APOSTOLAKIS: But so what? I mean,
4 that's why we have this research project. Right? I
5 mean, if it was easy, it would have been done.

6 MR. CHU: Right.

7 CHAIR APOSTOLAKIS: The thing is, I don't
8 understand your last bullet.

9 MR. CHU: Okay.

10 CHAIR APOSTOLAKIS: There is no
11 contradiction. I mean, it's not a matter of
12 contradiction, it's a matter of what makes sense to
13 do. And go back to Turkey Point again, if I gave you
14 just the software, and I told you this is the self-
15 testing mode, you wouldn't find any problem with that.
16 Right? You can't really say whether it's safe or
17 unsafe, or what. It depends on where it is used. I
18 mean, the software was doing what it was designed to
19 do. And actually, I think the whole rest of the work
20 that was presented today is really system centric, as
21 I think it should be. Now there may be some
22 instances, I mean, sometimes you use word and it
23 freezes. I don't know whether that has to do with
24 anything with another system, or with me, or whatever,
25 maybe it's part of the -- but this is a limiting case,

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 I don't know that the word "contradiction" is the
2 right one to use. It's what is useful and appropriate
3 for us to do, and what we're dealing with is a nuclear
4 power plant that's supposed to respond to certain
5 emergencies in the right way, so that's the context
6 within which we have to analyze these things.

7 MR. MARTINEZ-GURIDI: Yes. I think what
8 we mean to say, what is exactly the meaning of
9 software centric? I mean, if software centric means
10 that we are only going to look at the software in
11 isolation, then we are --

12 CHAIR APOSTOLAKIS: Yes, maybe as a
13 separate component.

14 MR. MARTINEZ-GURIDI: Then we agree that
15 that's not a proper way to approach it. However, what
16 we see is that really software is never really treated
17 in isolation, because --

18 CHAIR APOSTOLAKIS: In real life.

19 MR. MARTINEZ-GURIDI: In real life,
20 because even when you design it, you are taking into
21 account all this interaction, so you should take into
22 account all these interactions with the plant.

23 CHAIR APOSTOLAKIS: Okay. So naturally,
24 it should be system centric. That's what you're
25 saying.

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. MARTINEZ-GURIDI: If that definition
2 includes that, yes.

3 CHAIR APOSTOLAKIS: Okay. That's what it
4 is. You know, as you come to the fault tree the way
5 we do it now, and then add an extra component, say
6 digital system, you have to embed it in the fault tree
7 and see how the components feed into it, they are
8 commanded to do things. That's what -- it can't be
9 just one additional component.

10 MR. CHU: Yes, I agree.

11 MR. NGUYEN: May I make a small comment,
12 please?

13 CHAIR APOSTOLAKIS: Yes.

14 MR. NGUYEN: My name is Thuy, again. On
15 this discussion of software centric viewpoints, there
16 are a number of faults that we call intrinsic faults,
17 that you can recognize as faults independently of the
18 functionality of your system. For example, if you see
19 a division by zero, or the use of uninitialized
20 variables, or so on --

21 CHAIR APOSTOLAKIS: These are limiting
22 cases that are not -- yes, sure. You should divide by
23 zero. That's true.

24 MR. NGUYEN: Yes. But there are tools now
25 that identify these type of faults automatically.

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: That's good. That's
2 not my main concern. My main concern is, if I have a
3 LOCA, am I going to mitigate it. That's really my
4 concern. Now if you divide by zero someplace, then
5 we're in trouble then.

6 MR. NGUYEN: Yes.

7 CHAIR APOSTOLAKIS: That's not my main
8 concern. Okay?

9 MR. NGUYEN: Well, that's still a case.

10 CHAIR APOSTOLAKIS: How often do you
11 divide by zero? I don't do that often.

12 MR. NGUYEN: Well, division by zero is
13 only one --

14 CHAIR APOSTOLAKIS: I understand what
15 you're saying. I mean, this is a limiting case, but
16 that's not what should be our focus.

17 MR. NGUYEN: We made a number of analysis
18 of safety software that has been in operation for
19 quite a long time, and we did find --

20 CHAIR APOSTOLAKIS: But another argument
21 I will make is that if you follow the system centric
22 approach, eventually you will find these things. And
23 we did that at MIT, a colleague of mine had designed
24 control software for a mission that they were going to
25 send to space and all that.

NEAL R. GROSS

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

1 MR. NGUYEN: You may not have found it.

2 CHAIR APOSTOLAKIS: We found it using DFM,
3 by trying to develop the decision tables, the student
4 went there and he said oh, what is he doing here?
5 He's dividing by zero. So it was found without really
6 focusing just on the software, but trying to develop
7 the -- but, anyway, your point is well-taken, but I
8 don't think it's strong enough argument to abandon it.

9 MR. NGUYEN: No, no. It's just to say
10 that there is no contradiction.

11 CHAIR APOSTOLAKIS: You can't talk to me
12 from there. You have to come to the microphone.

13 MR. NGUYEN: It's just to say that the
14 last bullet says there is no contradiction --

15 CHAIR APOSTOLAKIS: I understand. Thank
16 you. Are you done, Louis?

17 MR. CHU: Almost. Another ACRS comment
18 was to look at software reliability methods, and
19 review them critically, so we did some review, and in
20 our report we documented --

21 CHAIR APOSTOLAKIS: But it was not a
22 critical review, because you say you will do a
23 critical review later.

24 MR. CHU: Right. Our next task, we'll try
25 to -- we'll get --

NEAL R. GROSS

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

1 CHAIR APOSTOLAKIS: You're going to come
2 out and say this method --

3 MR. CHU: But I think all the foundation
4 has been done.

5 CHAIR APOSTOLAKIS: You're going to come
6 out and say this method is no good. Can you say that?
7 Can we see those definitive statements at some point?

8 MR. CHU: We'll try to be more critical.

9 CHAIR APOSTOLAKIS: No, that's not what I
10 asked. I didn't ask you to be more critical. I'm
11 asking you to be truthful, because people usually are
12 reluctant to say that, unless their own method is
13 attacked, then everybody else is wrong, but that's
14 different. I expect an objective assessment, Louis.

15 MR. CHU: Okay. We'll try. We'll try.

16 CHAIR APOSTOLAKIS: Formal methods, have
17 you contacted the Canadians at all? I understand they
18 have done something like this. Not exactly formal
19 methods, but they borrowed from formal methods, and I
20 don't know what they did, they formulated certain
21 things using lesson learned from there, and they were
22 very pleased with that. Ontario Hydro, have you
23 talked to anybody there?

24 MR. CHU: No, no. We'll try to. It looks
25 like formal method is a reasonable thing to try, even

NEAL R. GROSS

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

1 in terms of finding software faults. You use
2 mathematical language to model your requirement
3 specification, such that you can check. When you
4 develop such a model, you think more systematically so
5 it's not likely you'll make mistakes in specifying
6 requirements, and the tools will automatically check
7 for some kind of inconsistencies, completeness issues.
8 And Nancy Levenson had done that in the Traffic
9 Collision Avionic Systems successfully.

10 CHAIR APOSTOLAKIS: Well, SRI, I think, is
11 doing -- SRI in California.

12 MR. ARNDT: George, the Germans and the
13 Indians actually have also done work in this area.

14 CHAIR APOSTOLAKIS: Yes. It would be
15 useful to see. Because eventually you may want to
16 have a combination of approaches.

17 MR. ARNDT: Yes.

18 CHAIR APOSTOLAKIS: If this 36 percent of
19 errors are due to requirements, you might say gee, my
20 dynamic methodology doesn't quite fit that, but look
21 what I do before I apply it. I do some formal thing
22 to minimize it, I do something else, so the
23 combination eventually probably will be -- they have
24 different objectives.

25 MR. ARNDT: Yes. The big issue with

NEAL R. GROSS

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

1 formal methods is that, at least as it's been applied
2 in the nuclear industry so far, is that it's really
3 more an error detection and error reduction
4 methodology, as opposed to a modeling methodology.
5 It's useful in other aspects of the digital research
6 program plan, less so in the reliability part of it.

7 CHAIR APOSTOLAKIS: Yes, but if you tell
8 me that I'm doing my reliability analysis using this
9 method, assuming that I have already done these other
10 things, then maybe that will give it a little more
11 substance.

12 MR. ARNDT: That really gets to something
13 that the U.S. industries also put forth as part of the
14 EPRI methodology. The mechanisms by which you can,
15 like formal methods, and redundancies, and fault
16 tolerant techniques --

17 CHAIR APOSTOLAKIS: Okay.

18 MR. ARNDT: -- give you a higher
19 likelihood that you're not going to have problems.

20 MR. CHU: And the method I think was
21 recommended by the National Research Council, too.

22 CHAIR APOSTOLAKIS: Which method?

23 MR. CHU: The formal method.

24 CHAIR APOSTOLAKIS: As one of the methods
25 that are available. Right?

NEAL R. GROSS

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

1 MR. CHU: Right. Since we are trying to
2 develop Markov type of model for digital system, and
3 quantification of software failure rates or failure
4 probability will be an important part of the model
5 development. Currently, we're thinking about using
6 Bayesian belief network method. Some European
7 countries have tried it. It is a tool for performing
8 quantitative analysis of decision making, and in our
9 application, we will develop some kind of network, and
10 one of the nodes will be say software failure
11 probability, the quality of the software. And then we
12 identify different things that affect the quality of
13 the software, the failure rate, or failure probability
14 of the software. And express the relationship in
15 terms of some kind of conditional probability tables,
16 and such tables certainly will have to be derived
17 probably based on judgment, based on expert
18 elicitation. In general, this seemed to be a
19 reasonable way for quantifying software failure rates
20 or probabilities.

21 Conclusion - software failures occur many
22 different ways. Experiencing other industry is, in
23 general, applicable to the nuclear industry. Some
24 failure took place in such a way that implies very
25 detailed modeling would be required. Some failures

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 involve non-application software, that implies the
2 type of software analysis needed to identify those
3 problems. It's reasonable to model software failures
4 in --

5 CHAIR APOSTOLAKIS: And that's where I am
6 not sure that's correct.

7 MR. CHU: Yes.

8 CHAIR APOSTOLAKIS: And we need to
9 investigate this idea of context and all that more
10 carefully.

11 MR. CHU: Yes.

12 CHAIR APOSTOLAKIS: Remember, this is a
13 subcommittee meeting that's supposed to be helpful.
14 Right? I mean, it's not a final review of the
15 project.

16 MR. CHU: We had a high level model for
17 software failure. That part can be further developed,
18 trying to look into this kind of issue.

19 CHAIR APOSTOLAKIS: Absolutely.
20 Absolutely. Conclusion two.

21 MR. CHU: In terms of identifying software
22 faults, it looks like there are many different
23 methods. Each method, they have advantages and
24 weaknesses. In general, you kind of want to use
25 combination of them. But still in the end, most

NEAL R. GROSS

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

1 likely, you cannot assume there's no faults in the
2 software.

3 CHAIR APOSTOLAKIS: The biggest problem
4 here is not really finding faults, in the context of
5 reliability, is what can you say about the probability
6 of performance in the future, given that you have
7 found faults, and you have fixed them?

8 MR. CHU: Right.

9 MR. HICKEL: The problem, George, is that
10 I believe that there's -- just the data, I'd say the
11 data right now shows that the rate of introduction of
12 faults after its been turned over and is in use, is
13 very high.

14 CHAIR APOSTOLAKIS: Yes, I agree.

15 MR. HICKEL: They include things like the
16 vendor supplying the wrong set points, and that's not
17 unique to digital, but it also includes all these --
18 there is a lot of experience about things getting
19 changed in the field.

20 CHAIR APOSTOLAKIS: And the question is
21 how do you model it?

22 MR. HICKEL: Probably your HRA is more
23 associated with this than the digital software
24 reliability.

25 CHAIR APOSTOLAKIS: We inject errors into

NEAL R. GROSS

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

1 the operators?

2 MR. HICKEL: No, they inject it into the
3 equipment. Most of the time, the equipment catches
4 it, and that's when you get an LER, thank God.

5 CHAIR APOSTOLAKIS: The common saying that
6 you shouldn't fly an airplane right after its
7 maintenance. Okay. I guess that's it.

8 MR. CHU: Yes. The things on the list we
9 have has already been discussed.

10 CHAIR APOSTOLAKIS: Very good. Any
11 comments for these gentlemen from anyone? Thank you
12 very much. Very nice. And the next subject is the
13 Regulatory Guide. I understand the presentation is
14 not too long, but we are going to take a few minutes,
15 so let's come back at 10 minutes after, unless the
16 members disagree. You want 15 minutes?

17 (Whereupon, the proceedings went off the
18 record at 4:02:39 p.m. and went back on the record at
19 4:16:55 p.m.)

20 CHAIR APOSTOLAKIS: Okay. Now we are
21 talking about the Development of Regulatory Guidance.
22 Mr. Arndt.

23 MR. ARNDT: Yes.

24 CHAIR APOSTOLAKIS: Have we seen this
25 diagram before?

NEAL R. GROSS

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

1 MR. ARNDT: Yes. I just wanted to mention
2 a couple of things real quick before I go on. Two
3 quick things, to fix it in the Committee's mind,
4 because it's been an issue before. We're obviously
5 going to be talking about this element here, the
6 development of regulatory guidance, and this has
7 inputs both from what our stakeholders were talking
8 about, and what they're interested in, and the issues
9 they have, but also the information we learned from
10 the rest of the program.

11 Also, before we get out of here, I want to
12 make a couple of quick comments to remind you who's
13 doing what so you can get it straight in your head.
14 The overall program plan, all the different areas, is
15 being managed out of the INC Group, and I'm the
16 overall Program Coordinator for that. The traditional
17 methods that we talked about most recently, is being
18 managed out of our PRA Group, Todd Hilsmeier is the
19 NRC Program Manager for that part of it, and BNL is
20 the prime contractor. The dynamic models, I also wear
21 that hat as the Program Manager for that area. The
22 prime is Ohio State University, Tunc Aldemir and his
23 group, and he has a couple of subs, one looking at DFM
24 modeling methodology at ASCA, and also the UVA that is
25 working both on the development of actual interface

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 with the system that we're working on, but also
2 working on the modeling of the coverage space and
3 things like that. So this is basically what the
4 structure of the program is, so --

5 CHAIR APOSTOLAKIS: Are you getting any
6 input from NRR?

7 MR. ARNDT: Yes. And as we move toward
8 the regulatory guidance development, that involvement
9 is going to expand.

10 Now as I pull this other one up, I want to
11 also mention, we appreciate the opportunity to come
12 and work with you. One of the things I just want to
13 mention is at the last meeting, you really emphasized
14 your desire to work with us, and work on intermediate
15 results, so some of this has been watching sausage
16 being made, to some extent. But we appreciate your
17 comments and your review, and we hope to continue
18 working with you in that area. And we can talk about
19 that later after the end of the last presentation.

20 This is going to be some general ideas on
21 what we think the structure and content of the
22 regulatory guidance is going to be. As I mentioned
23 earlier, this is a process by which we're trying to
24 develop the ideas, get input, and work with the
25 stakeholders before we send it out, the first draft

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 out for public comment.

2 As we mentioned earlier, as part of the
3 overall research program plan, we're developing the
4 needed regulatory guidance to support risk-informed
5 digital system reviews. To do that, we're taking the
6 information that we're gaining from the other parts of
7 this program, understanding the failure data,
8 assessing the model, what models can be used,
9 determining what systems need to be modeled at what
10 level of detail, developing acceptable methods and
11 acceptance criteria associated with that.

12 A little bit of reiteration. Industry has
13 expressed interest in this area. We want to both
14 develop regulatory guidance for regulatory
15 applications of this method, but also to continually
16 update the actual PRAs so they're consistent across
17 the board, and model the digital systems.

18 MR. HICKEL: Steve, could I ask a question
19 back on that last slide.

20 MR. ARNDT: Sure.

21 MR. HICKEL: You're saying as the
22 licensees replace analog system with digital systems,
23 their current PRAs are not keeping up with these
24 changes. Now are you -- you're not expecting, or the
25 staff, or NRR doesn't expect the licensees to modify

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 their PRAs for non-safety-related control systems.

2 MR. ARNDT: We do not.

3 MR. HICKEL: You do not. Okay.

4 MR. ARNDT: And if you look at the way we
5 implement risk-informed regulation, there's an
6 evaluation as to whether or not the models that are
7 being used for the particular risk-informed
8 application are sufficient quality, completeness, and
9 other things, to support that particular application.
10 This simply is highlighting the fact that if you want
11 to do something that happens to touch a system that
12 happens to be a digital system, then you're going to
13 have some challenges, if you haven't updated that
14 piece, as well. If you don't need to do that, we
15 don't need to evaluate it, and you don't need to have
16 that application. But we're starting to see in a few
17 very selected applications where that's starting to
18 touch these kinds of issues.

19 MR. HICKEL: Okay. Examples being things
20 like sequencers and --

21 MR. ARNDT: Examples being, for example,
22 risk-informed tech specs. If you want to do risk-
23 informed tech specs for various systems, and one of
24 them happens to have control and protection systems,
25 that's fine, so long as the modeling for that

NEAL R. GROSS

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

1 particular system is accurate to what's currently in
2 the plant, and accurate to the level of detail that it
3 models all the important aspects of the systems. If
4 you want to exclude that particular system from your
5 risk-informed tech spec, that's fine. But if you want
6 to include it, then we need to establish some criteria
7 as to what is a regulatorily acceptable digital system
8 model for that application.

9 MR. HICKEL: Well, the main reason
10 somebody might want to get relief is he's going to put
11 in a system that's automatically tested to replace one
12 that he used to have to go do surveillance on.

13 MR. ARNDT: That would be one example,
14 yes.

15 MR. HICKEL: Okay.

16 MEMBER BONACA: A question I had, Steve,
17 was a number of these replacements, I believe have
18 occurred under 05.59.

19 MR. ARNDT: Correct.

20 MEMBER BONACA: And I would expect that
21 industry will still try to use 50.59 to perform
22 changes without having formal approval.

23 MR. ARNDT: There will be a number of
24 situations where that will be the case, yes.

25 MEMBER BONACA: Okay. Now I'm wondering

NEAL R. GROSS

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

1 about bullet number two, where I see that the industry
2 has expressed interest in using risk-informed
3 regulation, Regulatory Guide 1.174, as an alternate
4 method for licensing the systems. And so I'm trying
5 to understand --

6 MR. ARNDT: Some systems we have
7 specifically stated we expect the licensees to bring
8 them in for regulatory review.

9 MEMBER BONACA: Okay. There has been the
10 clarification.

11 MR. ARNDT: Reg Guide 1.174 provides
12 guidance on how to do risk-informed decision making.
13 But as we've talked about, it doesn't provide specific
14 criteria for digital systems. Now does it necessarily
15 need to? Well, as we work this out, we'll find out
16 what additional guidance, if any, is necessary. As
17 you know, there's a series of guides to specific risk-
18 informed applications, risk-informing the Q List,
19 risk-informing the tech specs, et cetera. We believe
20 the unique aspects of digital systems means you need
21 some additional guidance.

22 Because of that, we want to look at issues
23 associated with digital system modeling, as well as
24 the other aspects of regulatory review that you need
25 to do for risk-informed guidance; that is to say, how

NEAL R. GROSS

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

1 does the requirements in 174 for maintaining
2 sufficient safety margin meeting the current
3 regulations defense-in-depth philosophy, and
4 performance measurement strategies apply when you do
5 a digital system upgrade based on the risk-informed
6 application.

7 This is basically a reiteration of what
8 I've said a couple of times already today, our
9 strategy for the development. Development and
10 understanding of the characteristics, what are the
11 things that might be necessary to model to have a
12 sufficiently good model for these applications? Some
13 of those were articulated in Reg Guide CFR 69.01 and
14 various other work that's been published, and will be
15 published. Is this a complete list, is it a list that
16 has to be satisfied by every model? No. That goes
17 back to the categorization issue that we've talked to,
18 and I'll talk to a little bit later in this
19 presentation.

20 Identify methodologies for modeling the
21 systems. We've done that, and we're going to continue
22 to do that. Develop an understanding of the data
23 issues - that's a very large issue. Develop draft
24 regulatory guidance or a draft regulatory approach -
25 this is the guide that we're going to use. It's

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 tentatively DG-1151, an approach to plant-specific
2 risk-informed decision making for digital systems.
3 We're going to have, as we mentioned earlier, a public
4 meeting or a workshop to discuss our strategies for
5 putting this together, and we hope to publish the
6 comment - the draft for public comment in December of
7 this year.

8 This is a very rough first guess at a
9 structure for what the reg guide would include.
10 There's a discussion of the modeling requirements,
11 discussion of the issues associated with integration
12 of digital system models into the full PRA model
13 methodology, discussion of the data requirements. I
14 expanded out and will highlight the uncertainty
15 analysis issue here, primarily because 174 doesn't
16 talk to it in great detail, and this is an area, as we
17 discussed earlier, there's a lot of uncertainty
18 associated with the data, with the models, with the
19 context or operational profile that are going to
20 assume that we want to have some explicit guidance
21 associated with this.

22 The acceptance criteria - is the Delta CDF
23 and Delta LERF appropriate, and if so, are additional
24 guidance necessary? And then, how do you interpret
25 the other issues that you need to look at for 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 informing performance measures, maintaining sufficient
2 margin, defense-in-depth, diversity, those issues.

3 Here are some of the modeling requirements
4 we are looking at, including - now to some extent this
5 is motherhood. We want to model everything as best
6 you can, but from these criteria, we want to focus in
7 on what we care about when we are going to review one
8 of these models. The model must account for
9 important, relative features of the system under
10 consideration. Model must make valid, plausible
11 assumptions about the system characteristics, and
12 justify these. Model must be able to quantitatively
13 describe the dependencies between failure events,
14 support systems, common mode failures, dynamic
15 interactions, and if the model - if you choose not to
16 model some of these things, demonstrate why they're
17 not important. In very simple actuation systems, it
18 probably is very easy to demonstrate why they're not
19 important. In more complex systems, probably not.

20 Be able to differentiate between permanent
21 and intermediate failures, distinction between
22 multiple and single failures, issues associated with
23 the complexity of the system. If the system is not
24 very complex, then you discuss why it's not important,
25 and why the model doesn't need to include it. If it

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 is complex and you still choose not to model it, then
2 we have a much more detailed requirement for
3 understanding how you're going to deal with that.
4 Understand the model must be able to provide the kinds
5 of information that you need for inclusion in a PRA,
6 cut sets, probability failure, uncertainty.

7 There's nothing to say that this can't be
8 a multi-stage analysis, a stand-alone model that is
9 then integrated with the PRA. But if you're going to
10 do that, you've got to go back to how does that meet
11 the criteria above for characteristics, and
12 interfaces, and system dependencies, and things like
13 that. Methodology must be able to incorporate the
14 various accident sequences, and have enough detail so
15 that if there's interactions with non-INC systems,
16 that that's included.

17 Level of modeling detail - same kind of
18 concepts; that is to say, not saying you have to use
19 DFM, or you have to use Markov, or whatever, it's
20 saying you have to use modeling detail sufficient to
21 capture the important aspects of the digital system.
22 The digital systems RNL issues, issue you brought up
23 earlier, George, unique failure modes, if there are
24 unique failure modes, unique characteristics of
25 software failures and tests, some of the stuff 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 Louis mentioned earlier.

2 If you want to look at simplified models,
3 we would ask that you verify that the unique system
4 characteristics that are not modeled in your
5 simplified models aren't important. We want you to
6 look at understanding how the data fits the model. If
7 you data doesn't fit the model, or you're not
8 capturing the unique characteristics of the potential
9 failure modes in the data, we want to understand how
10 you're doing that, and why you're doing it that way.
11 Common mode failure issues, system interaction issues,
12 and the last bullet there gets to the issue that we
13 talked about earlier in the day - validate the events
14 that have happened in historical record can be modeled
15 by the level of abstraction that you have.

16 We hope to have some examples to
17 illustrate what we really mean by these things. We'll
18 probably inform that by our categorization issues that
19 we've talked about today.

20 If it's an implicit integration, if you're
21 going to do a fault tree/event tree-type model, this
22 is less important. If you're going to do something
23 more sophisticated, this is more important, in the
24 same way that you would, say, do a seismic analysis,
25 or some other kinds of analysis that is embedded in

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 current generation PRAs. You need to include all the
2 important interactions and dependencies, and include
3 systems that would impact or would be impacted by the
4 digital system changes.

5 Data requirements - this is going to be
6 challenging for everybody, but we want to look at what
7 data is being extracted, both in generic databases,
8 the plant-specific or system-specific databases,
9 particularly if we're going to use databases from
10 vendors or parts manufacturers that may not be
11 publicly available information, or may not have had
12 public peer review, and what the limitations and
13 biases, if any, are for those systems. Then look at
14 if some of the data is being supported by test
15 methodologies, be it reliability growth modeling for
16 software, or some of the factor acceptance testing,
17 site acceptance testing data, or specific data,
18 specific testing methodologies to develop specific
19 data like the fault injection methodology, understand
20 what those are telling us, and how applicable they are
21 to the particular delivered product, as well as how
22 much of the system are they really covering.

23 In terms of review of the database, these
24 are some of the issues we want to understand. The
25 data collection hasn't been done in a systematic way.

NEAL R. GROSS

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

1 Is it a good structure database, can we interrogate
2 it, is there good configuration management for the
3 measures, is the root cause analysis for the database
4 entries appropriate.

5 One of the biggest challenges with LER
6 database, for example, is you frequently only get very
7 high level causes, the module failed. Modeling at the
8 module level, and that is sufficient, that's great.
9 If you're modeling at a lower level, or a higher
10 level, you need to understand how that has been
11 generated, so that's going to be an issue that we're
12 going to look at.

13 Now some of this is the same kind of stuff
14 that you would see in any PRA analysis. However,
15 there are some unique aspects of digital systems, so
16 we won't look at them in a unique way. We talked
17 about model uncertainty earlier, look at model
18 uncertainty, look at operational profile uncertainty,
19 or context uncertainty, if you prefer, the knowledge
20 of the possible input space, and the probability
21 distributions associated with it, and data
22 uncertainty.

23 Additional requirements - as I mentioned
24 earlier, this is acceptance criteria explicitly laid
25 out in Reg Guide 1.174. There may need to be some

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 additional acceptance criteria for the digital
2 systems. We need to look at how we meet the current
3 regulations and defense-in-depth philosophy as
4 embodied in 10 CFR 50.55 a(h), the various reg guides,
5 603, and the interpretation of how our regulatory
6 structure currently exists.

7 One of the issues associated with risk-
8 informed upgrade or risk-informed evaluations is a
9 specific look at how the performance measurement
10 strategies are going to be applied. In the case of a
11 risk-informed digital system, that might include long-
12 term validation of the data used, monitoring of
13 industry-wide events to assure the assumptions
14 continue to be valid. As the technology associated
15 with digital systems changes, we want to make sure
16 that the assumptions that was used in the digital
17 reliability modeling also continue to be valid.

18 So, again, these are first thoughts of
19 things that need to be included in a structure that
20 would, I think, both give the NRC a relatively good
21 assurance that the modeling is being done
22 appropriately, at the same time giving sufficient
23 flexibility to the industry to propose alternative
24 methodologies.

25 The research into the current state-of-

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 the-art methods is being used to help inform this
2 regulatory guidance development, looking at a large
3 number of potentially viable methods, developing
4 acceptable methods. And as I just mentioned, we plan
5 on making this a performance-based; that is to say,
6 not prescriptive to a particular modeling methodology,
7 but rather, defining acceptable characteristics of a
8 modeling methodology.

9 The point of giving you some general ideas
10 here is to see whether or not you seem to think this
11 is a reasonable first approach for developing the
12 guidance, and also to look at issues that the
13 committee may think need to be included that we have
14 not thought of at this point. Any comments along
15 those lines would be much appreciated.

16 CHAIR APOSTOLAKIS: This is a pretty high
17 level description, so it's hard to, at least for me,
18 to come up with any substantive comments, unless my
19 colleagues have something to say. Is the subcommittee
20 going to review this guide as it is being developed,
21 subcommittee meeting?

22 MR. ARNDT: The standard procedure, as you
23 know, is once the draft is developed, it will be sent
24 to the ACRS to either be reviewed before public
25 comment, or waive review until after public comment.

1 You, of course, have the option to review it before
2 it's sent out for public comment, if you choose.

3 Additionally, of course, as we go forward,
4 we plan on having additional informational briefings
5 to the subcommittee.

6 CHAIR APOSTOLAKIS: That's what I was
7 asking. I mean, you do plan after you have some,
8 let's say it's 40 percent complete, maybe have an
9 information meeting and see what the reaction of the
10 subcommittee would be?

11 MR. ARNDT: It depends on scheduling, and
12 sequencing, but we could do that. Well, for example,
13 we're going to have internal review of the rough
14 draft, we're going to have the workshop that's going
15 to talk about this in more detail because it'll be
16 further along at that point. We'll get feedback from
17 the stakeholders. At some point between then and the
18 time we actually send it to the ACRS for review, we
19 could have a subcommittee meeting to discuss that,
20 among other things.

21 CHAIR APOSTOLAKIS: I think that would be
22 advisable. So you think the next time we'll see this
23 will be when it's really a draft of a regulatory
24 guide, not before. Well, maybe -- if we have a
25 subcommittee meeting to discuss other issues, maybe we

NEAL R. GROSS

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

1 can find a couple of hours to also discuss the --

2 MR. ARNDT: That would be very useful.

3 CHAIR APOSTOLAKIS: Yes.

4 MR. KEMPER: This is Bill Kemper. I think
5 that's a good idea, George, because we wanted to try
6 to discuss the software metrics project that just
7 didn't work out for us, so we do want to get back with
8 you in the next few months to talk about that, so
9 maybe we can combine this at the same time.

10 CHAIR APOSTOLAKIS: That would be a great

11 -- MR. KEMPER: I'm very much interested in
12 getting all of your insight into this draft reg guide
13 before we actually send it out for public comment.

14 CHAIR APOSTOLAKIS: Very good.

15 MR. KEMPER: Probably, I'm guessing,
16 probably around October-ish time frame is what we'd be
17 looking at from a calendar perspective.

18 MR. ARNDT: We'll work it out with the
19 staff.

20 MR. GAERTNER: I'm John Gaertner from the
21 Electric Power Research Institute. First of all, it's
22 been a very interesting day. I really enjoyed
23 learning these things, and the exciting things you
24 have underway. And as you know, we, and our
25 representation, the industry group, we support 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 risk-informing of this decision making for digital
2 INC, and we support the use of the PRA. But a few
3 things, Steve, that you said in this last talk leave
4 me a little concerned, so I just wanted to point them
5 out.

6 First of all, there seems to be a strong
7 desire to incorporate the INC modeling deeply into the
8 existing PRA as part of this effort, and I think that
9 could be a mistake. It's appropriate, I think, to use
10 the PRA to determine the acceptability of the digital
11 INC from a risk perspective, but a lot of the
12 assessments you're going to do are going to be
13 bounding, and that'll be acceptable to show the safety
14 of the INC system, but you don't want those bounding
15 assumptions put back into your PRA permanently. And
16 also, there'll be considerably uncertain, as we saw
17 from the data analysis that we saw. And we have
18 issues with aggregation - when we put things together
19 in PRA, and some things are highly uncertain and some
20 things aren't, or highly conservative and aren't, we
21 don't like to aggregate them. So I think it may be in
22 the best interest to keep the two separate, to a large
23 extent, and not insist that the detailed modeling be
24 incorporated into the PRA, necessarily. That's my one
25 comment.

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 My second one has to do with defense-in-
2 depth. I'm still concerned that it looks like we may
3 be still expecting to have a high level of
4 deterministic defense-in-depth, in addition to the
5 risk-informed, and that would make some sense, even in
6 Reg Guide 1.174, because where there's a lot of
7 uncertainty in risk analysis, one asks for defense-in-
8 depth. So I want to make sure that we're not just
9 compounding, that we're not adding this risk-informed
10 as an additional requirement on what we already have,
11 so for that reason, I think we need to reconsider the
12 current defense-in-depth requirements in light of the
13 risk-informed approach that we're using. So I hope
14 you'll do that in your reg guide. Thank you.

15 CHAIR APOSTOLAKIS: Okay. Thank you,
16 Steve. The industry has requested time, Mr. Marion.

17 MR. MARION: Good afternoon. My name is
18 Alex Marion, I'm Executive Director of Nuclear
19 Operations and Engineering at NEI. And I do have a
20 couple of comments I'd like to make relative to
21 successful application of digital technology in
22 today's nuclear plants, as well as in tomorrow's
23 nuclear plants. But before I get into that, I would
24 like to make a couple of comments about the last
25 presentation from Steve on the reg guide. And I

NEAL R. GROSS

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

1 accept the fact that this is very preliminary thinking
2 on the part of the staff, but this is extremely
3 important. If it's not done properly, it will be a
4 barrier to progress, and what I mean by that is, the
5 regulatory process associated with applying digital
6 technology will be so onerous that it will not be
7 applied. And that's a disservice to just about
8 everyone involved, including the NRC.

9 Based on what I heard today from the
10 research activities, and it's all kind of interesting,
11 it appears that the NRC is creating a situation where
12 they're going to impose on the licensees through this
13 regulatory guide to develop answers to some of the
14 questions that were raised today. And these are
15 questions that the NRC ostensibly is hoping to address
16 through this research program, so we have to be sure
17 as we go forward, if you take it to that level of
18 detail in this document, that we understand, together
19 understand what the expectations are, but more
20 importantly, how to satisfy those expectations in a
21 reasonable manner. And that's going to be the
22 greatest challenge in this effort.

23 And to get back to John Gaertner's comment
24 about risk-informing the process, we do support that,
25 but we do want to make sure as we go through that

NEAL R. GROSS

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

1 process and document it in the regulatory guide and
2 license amendments that will follow, hopefully, that
3 it allows us to prioritize and identify those areas
4 that are risk-significant that warrant attention. And
5 I submit that everything we talked about today in
6 terms of the research activities are not necessarily
7 risk-significant.

8 We do want to engage the staff as we go
9 forward, which includes the Office of Research and
10 NRR, this is a very important activity for us, and we
11 want to make sure it's successful. Within NEI, we
12 agree that we need to make this as successful as we
13 possibly can, and so the only way we can do it is work
14 with the NRC hand-in-hand, identify the issues,
15 prioritize them from the standpoint of risk, identify
16 options on addressing those issues, et cetera, and
17 moving the ball forward, if you will.

18 Timeliness of this is a concern on our
19 part, especially with regard to new plant activities.
20 Currently, the vendors are designing systems. We have
21 systems that have been installed in other countries.
22 There's an opportunity to start collecting data. I
23 submit that in the presentation earlier this afternoon
24 where four operating events were identified, it
25 doesn't make sense, to me, that we worry about a 15 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 20 year experience with digital technology, given the
2 pace of technology and its development. Okay? Just
3 think about what's happened in computer science over
4 the last five years. Okay? And the processes that we
5 have in place at nuclear power plant, as you well
6 know, is where there's an event where there's a
7 problem, there's a root cause evaluation, and
8 corrective action taken, so the relevance of these old
9 events just doesn't seem to make sense to me.

10 Let's see. Conventional PRA methods, at
11 this point, appear to be satisfactory if software,
12 common cause failure, and fault tolerant design
13 features are modeled in a conservative way. And we
14 provided a document to the NRC that was developed by
15 EPRI on defense-in-depth and diversity, and we're
16 hoping that the review of that document can proceed
17 in light of what we heard earlier today, and the
18 comments on it. We need to establish some confidence
19 in applying PRA technology, and I was pleased to hear
20 that the research program includes benchmarking.
21 That's extremely important. We think that is one of
22 the key elements of making this entire process
23 successful, because that gives us a reasonable time
24 frame to start developing some data, and we support
25 that.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 And what I'd like to do is propose an
2 integrated approach. We'll be thinking about, after
3 we all debrief next week, we'll be thinking about
4 sending in a letter to the NRC offering an integrated
5 action plan of things that we think need to be
6 addressed in order to make this process successful.
7 There are analyses and designs that are currently
8 ongoing for new plant construction. I know that
9 Oconee withdrew their submittal for their upgrade, but
10 I suspect that there are other utilities, well, I know
11 there are other utilities seriously thinking about a
12 submittal, so there are things that we need to
13 identify, that we need to address now within the next
14 six months. Otherwise, all of this activity is in
15 jeopardy.

16 The draft reg guide and the August
17 workshop schedules are extremely ambitious in light of
18 what we heard today, but I still think there are some
19 opportunities for addressing the low-hanging fruit,
20 and get the process moving.

21 The industry would like to be a peer in
22 the review of the research projects. It's kind of
23 awkward to be sitting here at a discussion, where the
24 committee members are commenting about a draft report
25 that they have, but that report wasn't made publicly

NEAL R. GROSS

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

1 available. We could have offered some input and
2 comments, and insights on that, as well. So at the
3 appropriate time, we would respectfully request to be
4 part of that peer review, because this is extremely
5 important to the industry in a number of ways.

6 We are also interested in looking for
7 opportunities for collaborative research. We have the
8 NRC's research plan, we'll look at that, and hopefully
9 in the not too distant future, schedule a meeting
10 where we can talk about such opportunities and try to
11 figure out how we can work together on answering those
12 questions.

13 I mentioned the EPRI topical report that
14 was submitted. I'd like to see that review progress.
15 We did receive comments from NRR. Those comments, I
16 think we can respond to. We generally agree with the
17 basic thrust of those comments. I don't know if we
18 should expect similar comments from the Office of
19 Research. I don't know if the Office of Research was
20 involved in putting those comments together or not.
21 All right.

22 Over the long term, NUREG CR 69.01 was
23 published, identify methods. There are a couple of
24 things we want to say about that approach. As we go
25 through evaluating digital systems and how to model

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 them, we need to keep in mind a couple of things. One
2 is, there are applications that deal with a specific
3 threshold, digital applications under these conditions
4 you open a valve. All right? Under these conditions
5 you respond to a particular pressure reading on an
6 instrument, et cetera, relatively straightforward and
7 fundamental. Others are more dynamic with a feedback
8 loop process, and we need to make sure that those two
9 kinds of applications have to be dealt with in
10 different manners. And I think you acknowledge that,
11 at least based upon what I heard today. But the NUREG
12 CR 69.01 doesn't differentiate between those two forms
13 of applications, or two types of applications.

14 We've looked at all the experience with
15 digital systems, specifically some of the software
16 issues, or the software-related experiences, and we
17 characterize a great majority of them as being basic
18 configuration management. Make sure that the
19 application meets the intended service it's going to
20 see in the field, et cetera, and you make sure it's
21 compatible with the design features of the system that
22 you're applying it to, et cetera. That's
23 configuration management, straightforward.

24 As we go through this process, we'll
25 consider whether or not any specific guidance or

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 encouragement is needed from NEI in reinforcing that
2 message, but that seems to be extremely fundamental
3 that we need to agree on, and I think ultimately the
4 staff will agree on that, as well.

5 We need to differentiate, as you go
6 through these evaluations of software failures, it
7 would be helpful if you could differentiate between
8 operating system failures and application failures.
9 That's extremely important. I mentioned the point
10 about relevance of aged experience. One other thing,
11 and the committee knows from presentations I've made
12 before, that I really focus on the process. If we can
13 understand the process, we know how to get from Point
14 A to Point B.

15 We want to be careful that we don't use,
16 or we don't set up an environment or situation where
17 the license amendment process by utilities wanting to
18 submit these applications for NRC review, becomes the
19 way that the NRC regulates digital applications in the
20 future. And I don't mean that in a negative, critical
21 manner. What's important, I think, and the way to
22 avoid getting into that trap is to focus on the risk-
23 informed decision making associated with these
24 applications, and I think that that ought to be the
25 first principle that we all agree on. All 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 We've had experiences with risk-informed
2 applications that have been successful, and let's see
3 if we can translate that, or transfer that to
4 applications in digital technology, and that's where
5 I think it's fundamentally important to stay focused
6 so we don't lose sight of that.

7 That completes my comments. I'll be more
8 than happy to answer any questions. Some of our
9 industry team is here. I don't know if they want to
10 add any additional comments, or any clarifications.

11 CHAIR APOSTOLAKIS: I was thinking about
12 it also today, not only today, and I'm glad you
13 mentioned that you would be willing to have some sort
14 of collaborative research going on with the NRC. And,
15 of course, as we all know, the fire modeling effort
16 was a very successful effort. In the past, we've had
17 common cause failure, common project, joint project.
18 I think it will be very, very useful to try to do
19 that. I think we have to be a little careful about
20 the timing of it, so that the industry and the staff
21 will have maybe some ideas that will evolve and then
22 come together. But I would be all in favor for that,
23 because I think this is a way to develop something
24 that's practical, stakeholder views come into the
25 picture early, and I can't think of any downside,

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 really. So I, personally, would be very supportive,
2 but I think the committee would be also very
3 supportive based on what we have seen so far, so I
4 would encourage you to pursue this. And I don't know
5 now when it would be an appropriate -- and I also
6 think the suggestion from Mr. Marion of having
7 industry reviewers of these documents is not a bad
8 idea. I mean, I don't know what the law says about
9 issuing draft reports before they are draft, and so
10 on, but if you can accommodate that, it seems to me,
11 Steve, you're going to benefit a lot. And, again, it
12 will be in the same spirit we're having these
13 subcommittee meetings; you are getting input early in
14 the process, so you have a chance to respond, or at
15 least you know what's coming down.

16 MR. HICKEL: It would seem they're members
17 of the public, also, NEI.

18 CHAIR APOSTOLAKIS: No, but if you treat
19 them as members of the public, then you have to wait
20 until the time comes for members of the public to see
21 -- I'm talking about the peer review that's happening
22 now.

23 MR. MARION: We've been involved in peer
24 review of other documents, and so the precedent has
25 been set, so I'm just offering that we're still

NEAL R. GROSS

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

1 available to help out.

2 CHAIR APOSTOLAKIS: I think that --

3 MR. KEMPER: Yes, if I could just add my
4 two cents. It's certainly a priority and a goal of
5 the Office of Research to collaborate with industry
6 whenever possible, and so I welcome that.

7 CHAIR APOSTOLAKIS: So it seems to me
8 there is no --

9 MR. KEMPER: It's just a matter of us
10 getting together and working out the details, the
11 logistics. All right?

12 CHAIR APOSTOLAKIS: Okay. Good.

13 MR. KEMPER: Peer review, also timing is
14 perfect for that, because that's also another
15 initiative by our office, is to assure quality of our
16 documents to get as good a peer review as we can, so
17 if we could maybe work out some protocol here about
18 who would be the person, as opposed to sending it out
19 to the entire industry. I don't know if that would be
20 the best solution or not, so we can work that.

21 CHAIR APOSTOLAKIS: You can work out these
22 things.

23 MEMBER BONACA: I'm disappointed to hear
24 about Ocone withdrawing the application.

25 MR. MARION: Yes.

NEAL R. GROSS

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

1 MEMBER BONACA: I didn't know that.

2 MR. MARION: Yes, just a decision they
3 made about two weeks ago or so. I don't know. Tony
4 Harris probably knows -- obviously, knows more about
5 it than I. Are they going to reconsider submitting
6 it, or can someone --

7 MR. HARRIS: No. This is Tony Harris with
8 NEI. I was at the last meeting with the staff, and I
9 think, Bill, you were there, too. Duke was
10 contemplating at that time whether or not they would
11 withdraw. I know they are -- I can't fully speak for
12 them. I do know they are working out the plan under
13 which they would resubmit the application, but they
14 have sent in a withdrawal letter.

15 MEMBER BONACA: I think to have on the
16 table an application, it will be very useful, I think,
17 for progress, I mean, on this plan, because it'll be
18 ideas, and the perspectives I think that, hopefully
19 there is -- somebody else will do that.

20 MR. HICKEL: Mario, or George and Mario,
21 there have been a number of people that were
22 contemplating digital upgrades to protection and ESFAS
23 logic, and there were announcements I think that jobs
24 were sold. And then subsequently they seemed to have
25 gotten off track. Is there any input from NEI, 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 this being caused by lack of guidance, or what is the
2 cause that these things are kind of falling by the
3 wayside? Is it complexity?

4 MR. HARRIS: This is Tony Harris with NEI,
5 again. We did meet with the NRC staff. We had an
6 EPRI/NEI co-sponsored workshop in March, and we
7 started looking through it, because you're exactly
8 right; there are a lot of folks. And the concern with
9 the industry is the length of time on some reviews -
10 now whether it's caused by issues on our end in terms
11 of quality, or some of the issues that you see in
12 terms of unresolved technical issues, some of these
13 things that take a long time. The process itself does
14 take a long time, and it may be that it will take some
15 period of time, but folks are very concerned about the
16 length of time, and the uncertainty in licensing these
17 digital application in RPS and ESFAS.

18 Now to that end, from an industry
19 perspective, we have developed a working group.
20 That's the next highest level you can have at NEI from
21 an industry perspective, and headed by a Vice
22 President of Engineering Technical Services, Amir
23 Sharkarami at Exelon. And we look forward to working
24 with the staff on moving forward all these various
25 issues. We identified I think it was five priority

NEAL R. GROSS

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

1 issues, one of which was research with the staff at
2 that March workshop, so we want to take that list and
3 start knocking it off and move forward, because there
4 are a lot of folks out there that would like to move
5 forward with digital applications, RPS and ESFAS.
6 Most of them say that I'll move forward right now to
7 the extent possible with the controlling sides, with
8 the non-safety related sides and the controlling
9 sides. And wait until things get a little more
10 stabilized in the regulatory front until we know more
11 of what we really have to do. What do we really have
12 to do to have a quality submittal, and have a good
13 timeliness in that application, but we're going to
14 work on that with the staff.

15 CHAIR APOSTOLAKIS: Good. Thank you. Any
16 other comments?

17 MR. KEMPER: Yes. And just to reinforce,
18 just give of a good segue way, we're listening and
19 taking serious exactly what the industry is telling
20 us. I just received a user need to accelerate
21 research in the area of diversity and defense-in-
22 depth, and also advanced control room design issues,
23 which is primarily prompted from that meeting that
24 Tony just spoke to a couple of months ago.

25 CHAIR APOSTOLAKIS: Very good. Thank you,

NEAL R. GROSS

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

1 Alex. Let's close by going around the table and see
2 what impression people got today. You want to start,
3 Tom.

4 MEMBER KRESS: Sure. Well, I believe I
5 saw a lot of progress since our last meeting. And I
6 think the program is on the right track. Early on I
7 was very skeptical that we could ever develop software
8 reliability failure rates, but now I'm more hopeful.
9 I think I see progress in this area. I'd like to
10 second your comment, George, that it would be nice to
11 have some early on judgments as to which systems
12 actually need to be modeled, and what process one
13 would use to model those particular ones. And I think
14 risk-importance measures would be very useful there.
15 No use to waste time on things that are not really
16 risk-significant. And even though we don't have
17 failure rates, I think you have to develop risk-
18 importance measures for systems.

19 One area that kind of bothered me a little
20 is when testing revealed no failures over a range of
21 coverage, I think there should be a statistical
22 technique to estimate the probability of having a
23 given number of failures, and that has to depend on
24 the amount of the degree of coverage, so I thought
25 that needed a little more work.

NEAL R. GROSS

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

1 I was a little skeptical of having the
2 ability to incorporate time-dependent failure rates
3 into PRAs. I think we need to figure out how to work
4 around that, or avoid it. That sounds like a real
5 problem to me. At some point in our subcommittee
6 meetings, I'd like to have a more detailed discussion
7 on how the lambdas are developed from the 1 minus Cs.
8 I'm not sure how that's done.

9 I appreciated the industry's comment that
10 failures per demand would be more interesting than
11 failures per hours of operation. I think that's an
12 area that needs to be thought about. I don't know, it
13 seems to me that replacing analogs with digital almost
14 automatically decreases risk. I don't know if we could
15 make such a blanket determination or not, but that's
16 just a thought.

17 I would like to support, add my support to
18 the industry's comments that on several areas. One,
19 re-evaluating what we mean by defense-in-depth in
20 digital INC areas. And I really like Alex Marion's
21 suggestions on the industry peer review, and
22 cooperative research. I'm glad to hear that that looks
23 like a possibility.

24 Eventually, I think we'll need to have
25 reviews of digital INC installations in new plants,

NEAL R. GROSS

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

1 which may not be LWRs, and I don't think the
2 acceptance criteria will be the same as are in Reg
3 Guide 1.174, and I think somewhere along - I don't
4 know if these guy's role to do that now, but somewhere
5 along the line, we'll have to think about how to deal
6 with them in the newer plants.

7 All in all, I see lots of progress. I'm
8 hopeful that this -- to me, clearly there's a need to
9 incorporate digital INC reliability into the PRAs, so
10 I'm glad to see this work.

11 CHAIR APOSTOLAKIS: Thank you. Mario.

12 MEMBER BONACA: Yes. I voice most of the
13 comments that Tom made. I mean, I see a lot of
14 progress. And, in fact, more than I thought we would
15 see by this stage. The area of determination of which
16 digital system need to be modeled and what level of
17 detail, that's an area, of course, of interest to all
18 of us. But I think it's also important because it
19 will define somewhat where you need to have dynamic
20 modeling, and where you can stay with traditional
21 methods.

22 I would be responsive to Mr. Gaertner's
23 recommendation of not forcing incorporation of digital
24 INC modeling in PRA. I mean, there may be other ways
25 to do that. I would view the approach the NRC 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 choosing as one that they are choosing for their own
2 independent validation and verification, but it is not
3 the only way to go about that. And really, I believe
4 there should be collaboration with industry very much
5 at this stage. I think a collaborative effort can
6 only be helpful.

7 I still believe there is a lot of
8 technology out there available, at least some of it we
9 saw ourselves when we went to Germany, and so there is
10 a lot of experience that can be brought to bear, and
11 from which we can really derive benefit, both from a
12 regulatory standpoint, and from an industry
13 standpoint.

14 Regarding Reg Guide 1.174, I mean, I'm --
15 I can see as work in progress so, of course, all of
16 us have high expectations of that reg guide, because
17 we are all supporting risk-informed regulation in this
18 area, too. So that's pretty much my comments.

19 CHAIR APOSTOLAKIS: John.

20 MR. HICKEL: Well, this was my first foray
21 into what your subcommittee had been doing, and I did
22 appreciate the two letters I think you've shown me
23 what they have done in the past. So I guess my
24 perspective is really of maybe just a fresh set of
25 eyes looking at what you've been doing already.

NEAL R. GROSS

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

1 My immediate thoughts are that needs to be
2 a more focused prioritization of where the staff is
3 trying to develop modeling, and analysis capability.
4 I don't know why the focus was on digital feedwater
5 control systems. I would hope that there is some
6 opportunity to get from the people in NRR that are
7 maybe the users of the research efforts and the reg
8 guides, like a picture, in the next six months we're
9 going to have to review this, in the next two years
10 we're going to have to review that, and five years out
11 we've got advanced reactors, or evolutionary plants
12 where we're going to have to take a position.

13 I would think that there is a need to have
14 more ability to project and evaluate trip systems and
15 ESFAS logic systems than was discussed here today. I
16 think that's my first comment. My second comment is
17 that I think that the data mining efforts that are
18 going on right now on the Brookhaven research project,
19 they appear to be more evolutionary. There's clearly
20 a lot more data out there. I think there are better
21 ways of getting it, but I think one of the things that
22 I see that's out there is issues of configuration
23 control afterwards, because these are the failures
24 that clearly are occurring. Somebody gets a bad data
25 set and they put it into all channels of the trip

NEAL R. GROSS

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

1 system, and that's not digital. You can do the same
2 darned thing in an analog, an old analog system, but
3 it's out there, and trying to understand those kind of
4 controls, I don't think we're focusing on that.

5 There is a lot of experience that people
6 have done that. There's a lot of experience out there
7 from the LER system that there have been problems in
8 calibration that result in people putting the wrong
9 numbers into all channels, and they're assisted and
10 guided by computer programs that are doing that for
11 them.

12 Those kind of things are happening. This
13 is not a highly complicated software reliability
14 issue. This is just that people are following
15 procedures, and on some occasions don't follow the
16 procedures, and they put in wrong numbers into
17 everything. And that issue is probably more likely to
18 occur than some very highly unusual common cause
19 hidden software failure. I'm thinking that the LER
20 database can give you better estimates of that thing
21 versus some unknown, undetected common cause failure
22 of software.

23 I think the numbers can be extracted, and
24 I do believe they will help better focus the efforts
25 towards coming up with regulatory guidance that will

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 be traceable back to history, and numbers, and be
2 better focused. And I think those are the two main
3 comments I'd have.

4 CHAIR APOSTOLAKIS: Okay. Thank you. I
5 think I was pretty vocal all day. I still -- I just
6 want to repeat that this issue of transition rates is
7 something that I really have to understand better,
8 what is the basis, and what do they really mean. And
9 I think we're making a lot of progress, as I said
10 earlier. Now we're discussing context, we're getting
11 into it more deeply, what does it mean, and all that,
12 and I'm confident we'll get some good answers soon.
13 The issue of zero failures, I mean, we're fixing them
14 all the time, and this paper, by the way, that was
15 cited in the report from the IEEE transitions, was a
16 pretty powerful mathematical analysis of what you do
17 in those cases. I'm not saying we should do that, the
18 mathematics is there.

19 So I'm very pleased myself with the
20 progress that has been made, and I'm also happy that
21 you guys are so willing to come and talk to us about
22 things that are still evolving, but that's the whole
23 idea of these meetings. We've tried it with 1.174
24 several years ago, it was pretty successful, so we're
25 doing this now. And I also am very pleased that the

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 industry decided to come and voice their concerns and
2 ideas, because this is really what will lead us to
3 something useful eventually. So with that, unless
4 somebody has something to say, from the staff, the
5 public? Thank you all very much. This meeting is
6 adjourned.

7 (Whereupon, the proceedings went off the
8 record at 5:16:33 p.m.)
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CERTIFICATE

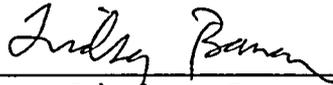
This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission in the matter of:

Name of Proceeding: Advisory Committee on
Reactor Safeguards
Subcommittee on Digital
Instrumentation and Control
Systems 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.



Lindsey Barnes
Official Reporter
Neal R. Gross & Co., Inc.

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



OVERVIEW OF DIGITAL SYSTEM RISK RESEARCH PROGRAM

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 27, 2006

Steven A. Arndt

Instrumentation and Electrical Engineering Branch
Division of Fuel, Engineering & Radiological Research
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)



OVERVIEW(1/2)

- Research will investigate potential procedures and methods for inclusion of reliability models for digital systems into current generation nuclear power plant PRA, develop these methods to the point they can be integrative into current agency tools, and develop needed regulatory guidance
 - Assessing what modeling methods might be usable
 - Determining which systems need to be modeled and at what level of detail
 - Developing and testing methods
 - Developing regulatory acceptance criteria



OVERVIEW (2/2)

- Issues facing NRC
 - Licensees are replacing analog systems with digital systems
 - Licensing these digital systems presents challenges to NRC
 - Industry has expressed interest in using risk-informed regulation (Regulatory Guide 1.174) as an alternate method for licensing these systems
 - Research into the limitations of digital systems reliability modeling does not currently support expanded use of risk information in licensing digital systems
 - As the NRC licensees replace analog systems with digital systems the current PRA's are not keeping up with these changes
 - NRC risk analysis tools and data (SAPHIRE and SPAR models) do not provide an independent means of assessing licensee analyses at present



Meeting with ACRS in June 2006

- ACRS Digital Instrumentation and Control Systems Subcommittee was briefed on the program plan
 - Wished to be consulted as the program progressed
 - Encouraged the review of software-induced failures, and recommended that lessons learned be feedback into the research conclusions
 - Encouraged the staff to critically review methods for assessment of reliability of systems
 - Encouraged the staff to view digital systems from a system standpoint, while acknowledging there may be some systems that can be treated as decoupled systems of components.

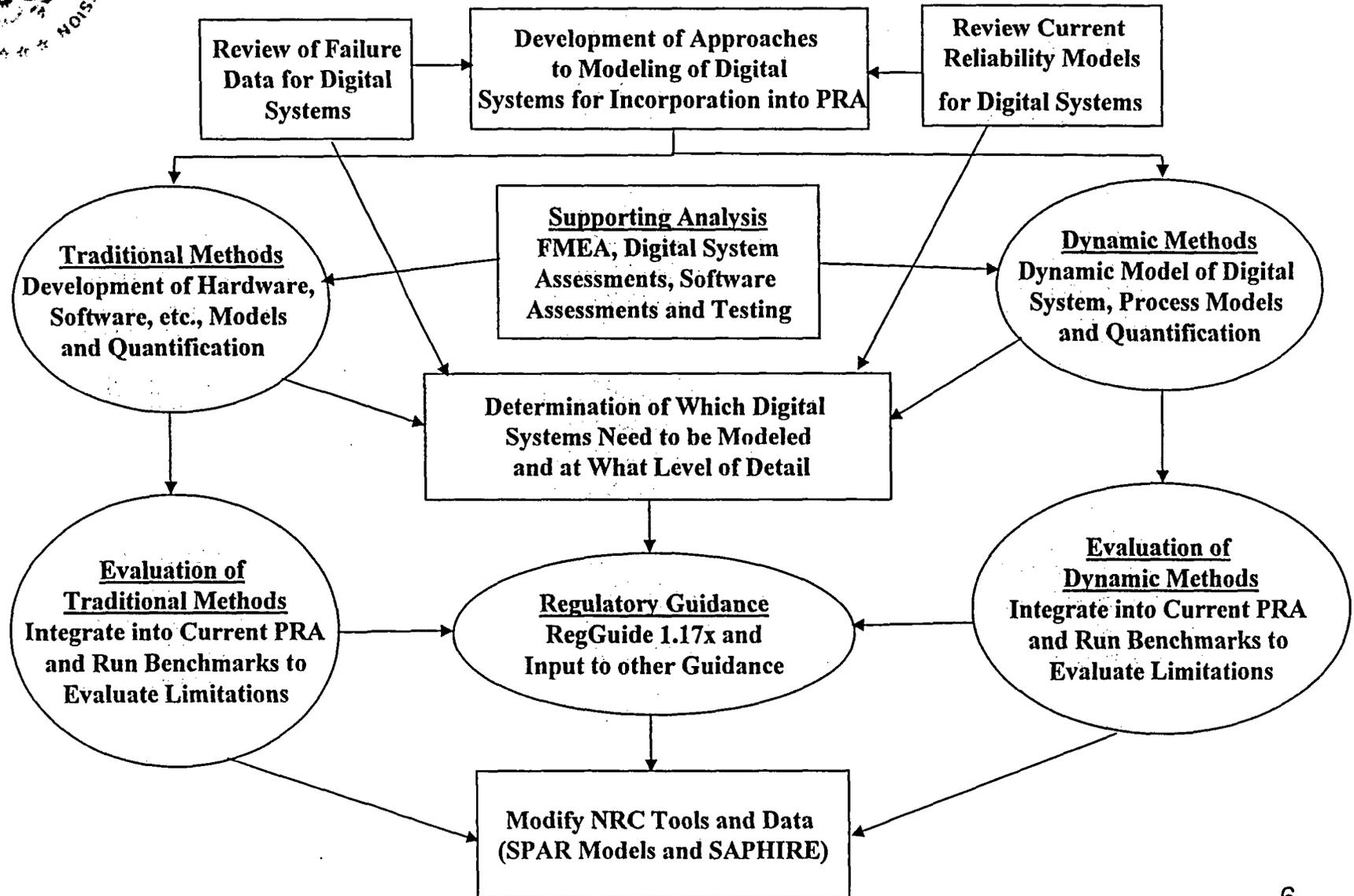


Digital System Risk Program

- **New methods for integrating current digital system models into PRAs are being developed**
 - **Pilot methods using both traditional methods and dynamic methods using models**
 - **Benchmarks of the capabilities of several methods will be completed**
 - **Uses and limitations of methods will be explored**
- **Guidance for regulatory applications involving digital systems reliability**
 - **acceptance criteria**
 - **limitations**
 - **evaluation methods**
 - **reliability data**



NRC Digital System Risk Program





RESEARCH FOCUS

- Structured to support three major outcomes
 - Determining what systems need to be modeled, at what level of detail, and what level of accuracy
 - Developing new capability to support independent analysis of digital systems
 - New or modified versions of current NRC PRA tools and data
 - Developing acceptance criteria for application of risk-informed approaches
- Broad-based research, focusing on review of possible methods, and data to support reliability analysis and acceptance criteria



SUMMARY

- This research will provide data, analysis methods, and acceptance criteria to support the use of risk-informed regulatory methods for the review of digital systems
- RES is looking forward to working closely with the ACRS as this program is implemented
 - Review of progress
 - Advise on best available methods
 - Review and endorsement of proposed methods
 - Review and endorsement of Regulatory Guidance



RELIABILITY MODELING OF DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS FOR NUCLEAR REACTOR PROBABILISTIC RISK ASSESSMENTS

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee
June 27, 2006

Steven A. Arndt

Division of Fuel, Engineering & Radiological Research
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)

Tunc Aldemir

Nuclear Engineering Program
The Ohio State University
(614-292-4627, aldemir.1@osu.edu)

1



Presentation Organization

- Background
- Benchmark System
- Failure Data Generation
- Example PRA Model
- Dynamic Flowgraph Methodology
- Markov Methodology
- Incorporating DFM and Markov Models into the PRA
- Interfacing with SAPHIRE
- Procedures and the Requirements for the Reliability Modeling of Digital I&C
- Conclusion to Date and Next Steps

2



Background (1/2)

- U.S. NRC policy encourages the use of PRA and associated analyses to the extent supported by the state-of-the-art and data
- NRC is in the process of developing methods for estimating failure probabilities for digital systems and modeling methods needed to support risk-informed regulation of these systems
- 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

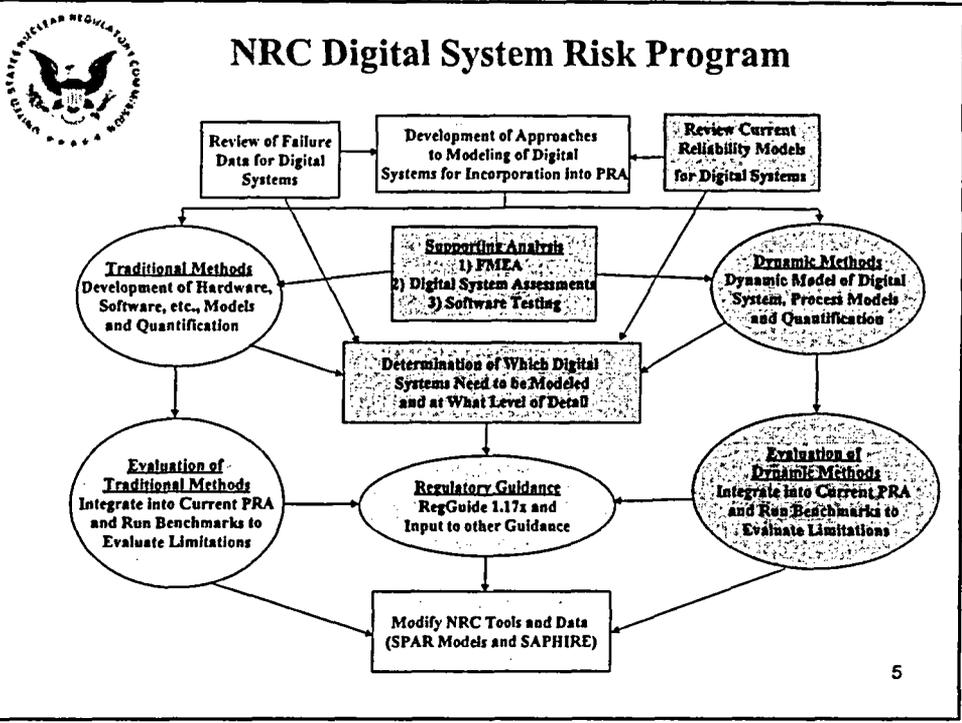
3



Background (2/2)

- From a reliability modeling perspective, this implies 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 and Δ LERF due to proposed change in the I&C system vs. existing system meet an acceptance criteria

4




Objectives

Develop both procedures 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 supporting analysis and data needed to develop Δ CDF and Δ LERF to support risk-informed regulation of nuclear power plant instrumentation and control criteria



Overall Approach

1. Investigate the applicability of the current static event tree/fault tree (ET/FT) approach to digital I&C systems
2. Review the advantages and limitations of available dynamic methodologies as they pertain to digital I&C systems relevant to reactor protection and control
3. Review other industries for practices in the reliability modeling of digital I&C systems
4. Review the existing regulatory framework with regard to requirements that a digital I&C control system must meet
5. Identify the minimum requirements a digital system model must meet for successful incorporation into an existing PRA
6. Identify available methodologies that meet these requirements
7. Demonstrate the methodologies identified in Step 6 using relevant benchmark systems

7



Progress to Date

- Steps 1 through 6 have been completed and the findings have been published in NUREG/CR-6901
- NUREG/CR-6901 has identified the Markov methodology and the dynamic flowgraph methodology (DFM) as methodologies that rank as the top two with most positive features and least negative or uncertain features when evaluated against the requirements for the reliability modeling of digital I&C systems.
- NUREG/CR-6901 also concluded that benchmark systems should be defined to allow assessment of the methodologies proposed for the reliability modeling of digital I&C systems using a common set of hardware/ software/ firmware states and state transition data.

8



Benchmark System

- The benchmark system specification is based on the digital feedwater control system for an operating PWR.
- It has been generalized to be more representative of this type of digital systems.
- The feedwater system serves two steam generators (SGs).
- The purpose of the feedwater controller is to maintain the water level inside each of the SGs optimally within ± 2 inches (with respect to some reference point) of the setpoint level (defined at 0 inches).

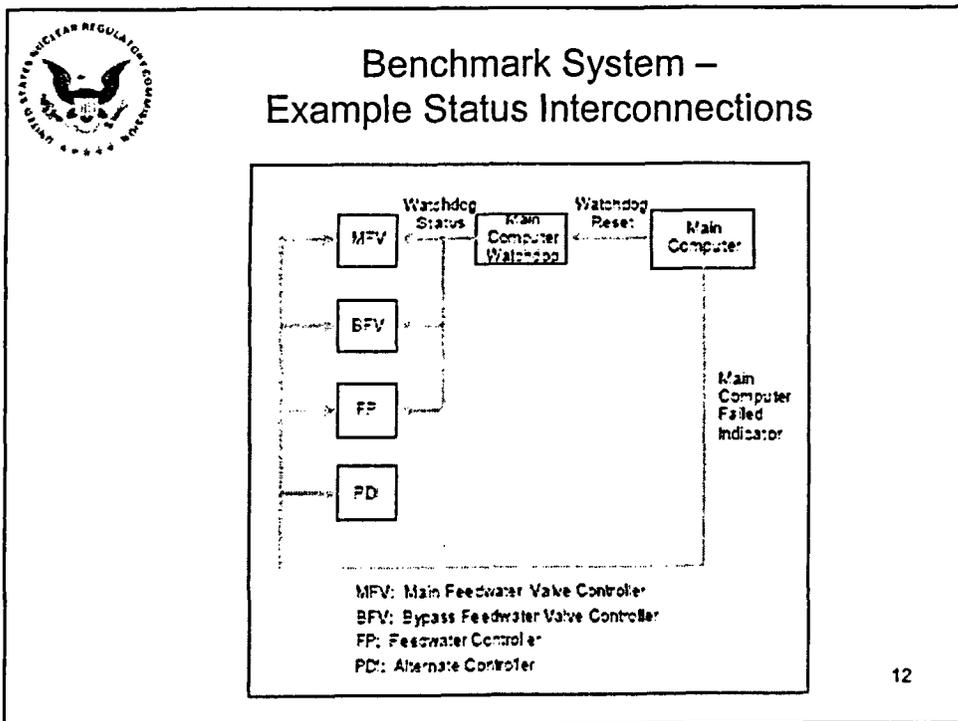
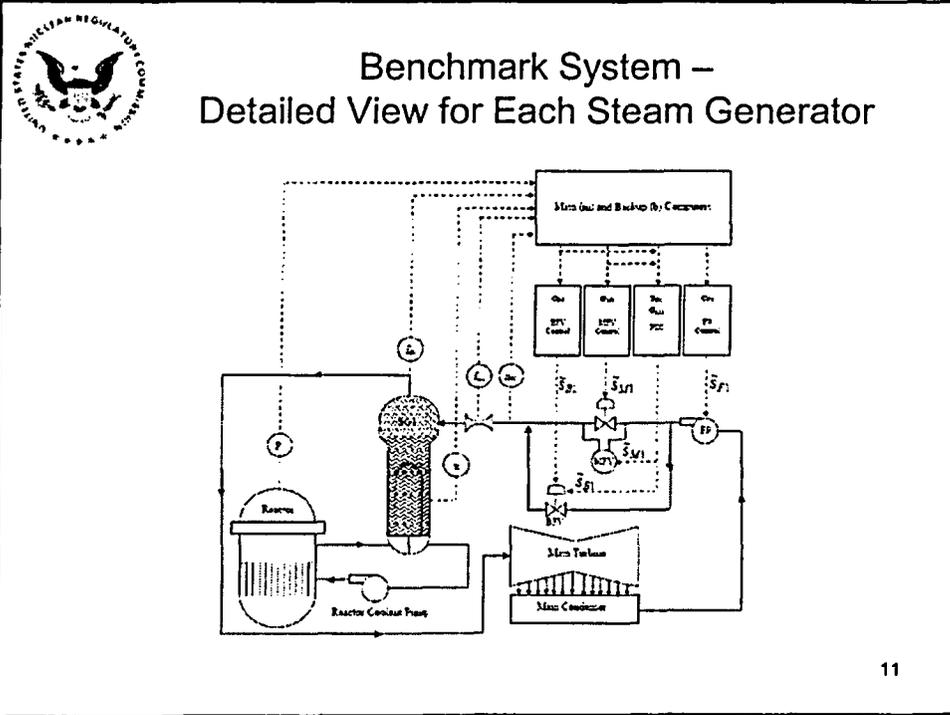
9



Benchmark System

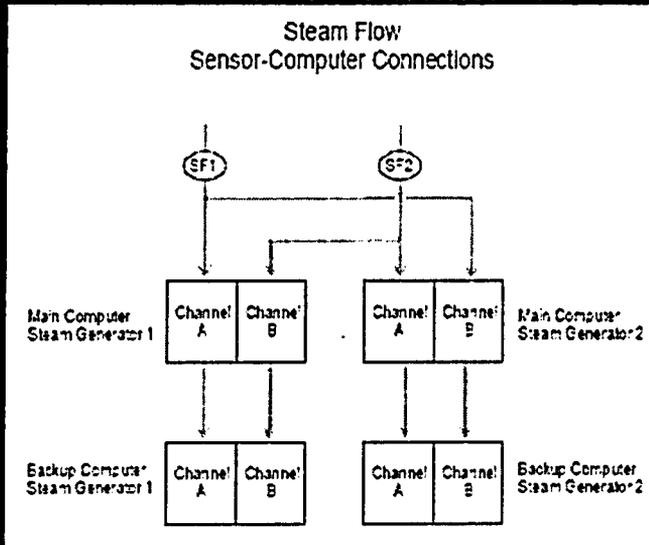
- The controller is regarded failed if water level in a SG rises above +30 and falls below -24 inches.
- Each digital feedwater controller is connected to a feedwater pump (FP), a main feedwater regulating valve (MFV), and a bypass feedwater regulating valve (BFV).
- The controller:
 - regulates the flow of feedwater to the steam generators to maintain a constant water level in the steam generators,
 - provides a means for raising the temperature of the condensate received by the feed pumps, and,
 - provides a means for injecting chemicals into the steam generators from the chemical addition system.

10





Benchmark System - Example Sensor Signals



Benchmark System - Control Laws (1/2)

Rate of level change:

$$\frac{dh_c}{dt} = A(h_c - f_c)$$

Flow Demand:

$$C_w(t) = \beta_c \cdot (f_c) \cdot dh_c - C_w(t) + F_w(t) - \lambda_w \cdot (h_c - f_c)$$

Compensated Water Level:

$$\tau_c \frac{dh_c}{dt} + h_c = \tau_c \frac{dh_c}{dt} + h_c$$

Compensated Flow Error:

$$\tau_c \frac{d(f_c - C_w)}{dt} + (f_c - C_w) = \tau_c \left[\frac{d(f_c)}{dt} - \frac{d(C_w)}{dt} \right]$$

BFV Demand:

$$C_w(t) = \lambda_w \cdot (h_c - f_c) + \beta_c \cdot (f_c) \cdot dh_c - C_w(t) - \lambda_w \cdot (h_c - f_c)$$

Compensated Power:

$$\tau_p \frac{d(C_w)}{dt} + C_w = \tau_p \frac{d(C_w)}{dt} + C_w$$

FP Demand

$$\sigma_{fp}(t) = \begin{cases} \sigma_{fp} & \text{If High Power Operation} \\ \sigma_{fp}(\max(\sigma_{fp}, \sigma_{fp}^*(C_w))) & \text{If Low Power Operation} \end{cases}$$

MFV Demand

$$\sigma_{mfv}(t) = \begin{cases} \sigma_{mfv}(C_w) & \text{If High Power Operation} \\ 0 & \text{If Low Power Operation} \end{cases}$$

BFV Demand

$$\sigma_{bfv}(t) = \begin{cases} 0 & \text{If High Power Operation} \\ C_w(t) & \text{If Low Power Operation} \end{cases}$$

FP Speed:

$$\dot{S}_{fp} = \begin{cases} \sigma_{fp} & \text{Main CPU Operational} \\ \sigma_{fp} & \text{Main CPU Failed, Backup CPU Operational} \\ \eta_{fp} & \text{Main CPU Failed, Backup CPU Failed} \end{cases}$$

MFV Position:

$$\dot{S}_{mfv} = \begin{cases} \sigma_{mfv} & \text{Main CPU Operational} \\ \sigma_{mfv} & \text{Main CPU Failed, Backup CPU Operational} \\ \eta_{mfv} & \text{Main CPU Failed, Backup CPU Failed} \end{cases}$$

BFV Position:

$$\dot{S}_{bfv} = \begin{cases} \sigma_{bfv} & \text{Main CPU Operational} \\ \sigma_{bfv} & \text{Main CPU Failed, Backup CPU Operational} \\ \eta_{bfv} & \text{Main CPU Failed, Backup CPU Failed} \end{cases}$$

PDI Decision:

$$\dot{S}_{pdi} = \begin{cases} 0 & \dot{S}_{bfv} \geq 0 \\ \eta_{pdi} & \text{Otherwise} \end{cases}$$



Benchmark System - Control Laws (2/2)

- The water inflow rate f_{wn} , steam flowrate f_{sn} , heat flux from the primary to the secondary side, level x_n , feedwater temperature for SGn are determined from the 2-volume SGn simulator package modeling the mass and energy transfer in SGn
- The control system provides feedpump speed, main flow valve position and bypass valve position to the simulator package
- The dynamic gain $\beta_{Fn}(f_{sn})$ and $\lambda_{Fn}(\sigma_{Bn})$ are obtained from table lookups
- η_{Fn} , η_{Mn} and η_{Bn} denote history data for the FP, MFV and BFV positions, respectively. If both MC and BC are failed, these data are used to determine the FP, MFV and BFV positions.

15



Benchmark System - Fault Tolerant Features

- Since the MFV, BFV, FP controllers forward the control signals to the corresponding control points, they provide a level of fault tolerance if both computers fail by allowing the operators time to intervene by holding the outputs of each to a previously valid value.
- The computers, MFV and BFV and FP, and PDI controllers are each connected to an independent power source wired to a separate bus. A single power source failure can only affect one computer, all of the MFV/BFV/FP controllers, or the PDI controller at one time.
- The computers are able to process the sensor inputs and perform the control algorithms within one third of the needed response frequency of the physical process. A failure in either computer can be detected and the fail over to a healthy component can occur with enough time to meet the response requirements of the process.

16



Benchmark System - Fault Tolerant Features

- The water level setpoint is taken from a switch connected to the MFV and is propagated to all computers. If the setpoint signal goes out of range, then the computers fall back on a preprogrammed setpoint value.
- Each computer is connected to a watchdog timer.
- Each computer verifies and validates its inputs, checking for out range and excessive rate changes in the inputs that would indicate errors in the sensor readings or problems with the analog to digital conversion of the values. Each computer will ignore input that fails these checks if the other inputs are still valid.
- The values of the inputs are averaged across redundant sensors.
- Deviation between the two sensors is detected and, if the deviation is large enough, the computer can signal a deviation error to the MFV, BFV, and FP controllers so they may switch to another computer.

17



Benchmark System - Fault Tolerant Features

- The PDI controller provides one more level of fault tolerance, in that it holds the MFV to a needed position if the MFV controller does not produce output. The MFV, BFV and FP controllers also check their inputs for range and rate of change checks; providing the ability to detect failures in the main and backup computers as well as the sensor data propagated to them.

18



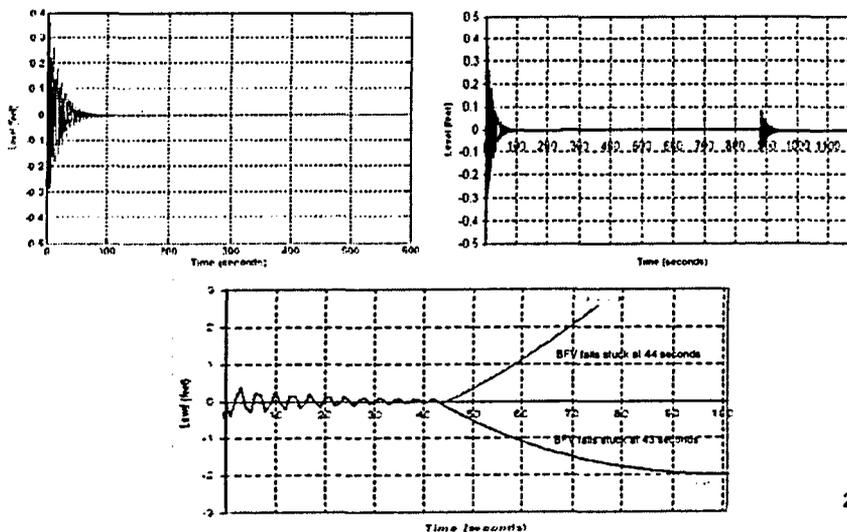
Benchmark System - Other Relevant Features

- Incorporates all of the properties of loosely-control coupled systems and most of the properties of tightly-control coupled systems.
- Properties of tightly-control coupled systems that are not represented are not relevant to instrumentation and control systems currently used in nuclear reactors (e.g. networking, shared external resources)
- Incorporates system history dependent control laws.
- Can lead to artifact generation under certain circumstances.
- System failure mode may depend on the exact timing of failure events.

19



Benchmark System - Operation Following a Turbine Trip with Main Computer Failed



20



Data Generation – Modeling Philosophy

- Define or choose metrics that allow models to be solved accurately.
- Choose models that are supported by observable, credible, measurable data.
- Choose models that are supported by plausible assumptions.
- All parameters of the model that cannot be deduced from the logical system design requirements must be measured.
- All such parameters must be measurable within a feasible amount of time.
- Uncertainties in the models should be accounted.
- *Critical Parameters in the model must be statistically estimated with a confidence bound that is commensurate with overall system reliability.*

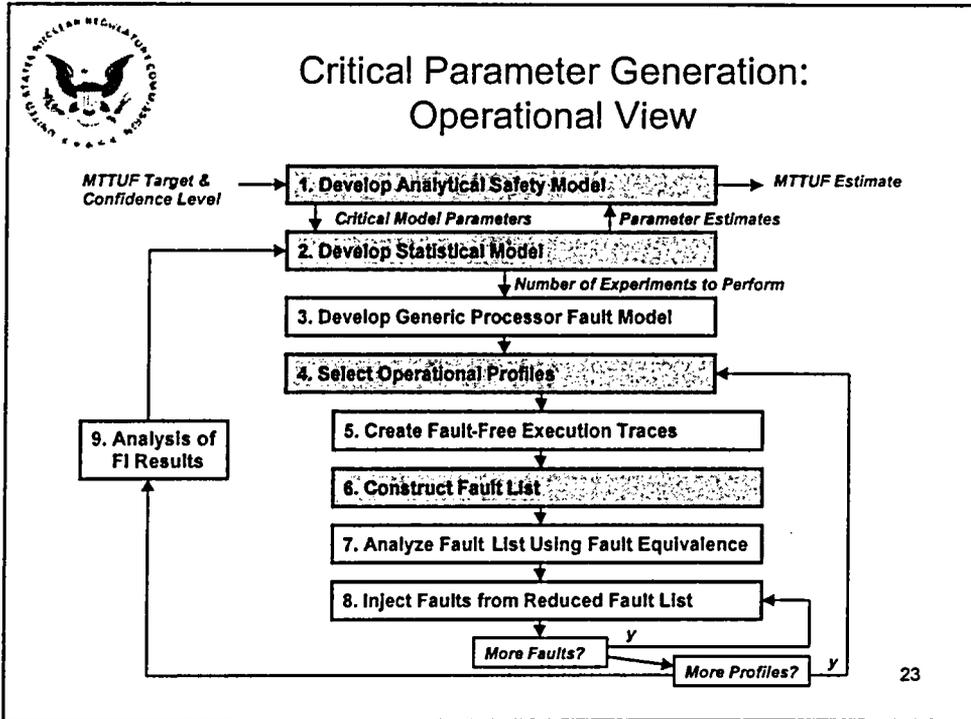
21



Development of Safety/Reliability Models

- Choose models that are supported by observable, credible, measurable data.
- Markov Models and DFM models need:
 - DFWCS component failure rates: Plant Historical data and RAC Prism database.
 - DFWCS Repair times: Plant Historical data.
 - System testing is used to develop additional needed data
 - Failure rates and fault or diagnostic coverage are experimentally determined through Fault Injection campaigns.
- Coverage is used to determine the likelihood for a undetected failure mode

22



23

Fault Injection Data Generation – How it works

- A fault injection experiment begins by selecting a set of faults from the fault library.
- Using the “bit flip injection method” we corrupt registers, memory locations where vital data is stored or processed. These faults induce the system into failure mode (say disrupting the feedback loop).
- For example and without loss of generality, say we inject 100 faults into the register files of the processor that store critical gain feedback parameters. Corruption of these parameters would de-stabilize the loop.
- Most of the time the system detects the injected errors, and correctly reconfigures the system to isolate the faulty processor. However, depending on the timing and duration of the fault we can get erroneous responses that were not detected by the system. These non-detected responses are the non-coverage (1-C) parameter for the models.
- This establishes a likelihood for a undetected unsafe failure mode. Non-Coverage 1-C.
- A detected failure is covered, and represented by the conditional probability C.

24



Operational Profiles

- Any testing or assessment process is sensitive to the input profile.
- Operational (Input/Output) profile data is collected from the *Cliff_time* plant monitoring data archive files.
 - Three years of data collected. Sampled every minute for 24 hours/day, every day.
- Contains plant data from various operational modes: Low power, high power, transitional, outage, testing, automatic, manual, failed components.
 - Log files will be used to synthesize accurate operational profiles for the Fault Injection experiments.
- Operational profiles (system inputs) are under the control of the assessor.

25



Safety and Reliability Models: Modular Markov Chain Modeling (UVA)

- Traditional Markov and Semi-Markov Models: Very general, make few assumptions, capable of modeling many different types of system behaviors and interactions.
- Disadvantages:
 - Computational State explosion
 - Model complexity impedes understanding and model validation (from a visual point of view)
- *Modular Markov Modeling:*
- A formal methodology that allows markov models to be composed in a modular way.
 - Addresses the issue of visual model complexity.
 - More closely tied to the functional architecture of the system.
 - A formal calculus of decomposition and composition
- Safety and reliability computed from the same model.
- Formally composes modules by their potential failure mode state.

26



Data Generation – Example Failure Parameters

Component NO	Component Name	Failure Rate	Example Parameter (per hour)	Coverage	Example Parameter
Component 1.1(A/B)	Power Level Sensor	λ_{11}	1×10^{-6}	C_{11}	0.99
Component 1.2(A/B)	Steam Flow Sensor	λ_{12}	1×10^{-6}	C_{12}	0.99
Component 1.3(A/B)	Water Flow Sensor	λ_{13}	1.5×10^{-6}	C_{13}	0.99
Component 1.4(A/B)	Water Temp Sensor	λ_{14}	1×10^{-6}	C_{14}	0.99
Component 1.5	Water Level Sensor	λ_{15}	1×10^{-6}	C_{15}	0.99
Component 2	Main Controller	λ_2	3.65×10^{-3}	C_2	0.995
Component 3	Backup Controller	λ_3	3.65×10^{-3}	C_3	0.995
Component 4	Main Flow Valve PID	λ_4	1×10^{-3}	C_4	0.995
Component 5	Bypass Flow Valve P.D	λ_5	1×10^{-3}	C_5	0.995
Component 6	Spare P.D	λ_6	1×10^{-3}	C_6	0.995
Component 7	Main Flow Valve	λ_7	1.2×10^{-3}	C_7	0.99
Component 8	Bypass Flow Valve	λ_8	1×10^{-3}	C_8	0.99
Component 9	Feed-Water Pump P.D	λ_9	1×10^{-3}	C_9	0.995
Component 10	Feed-Water Pump	λ_{10}	1×10^{-3}	C_{10}	0.99

29



Example PRA Model

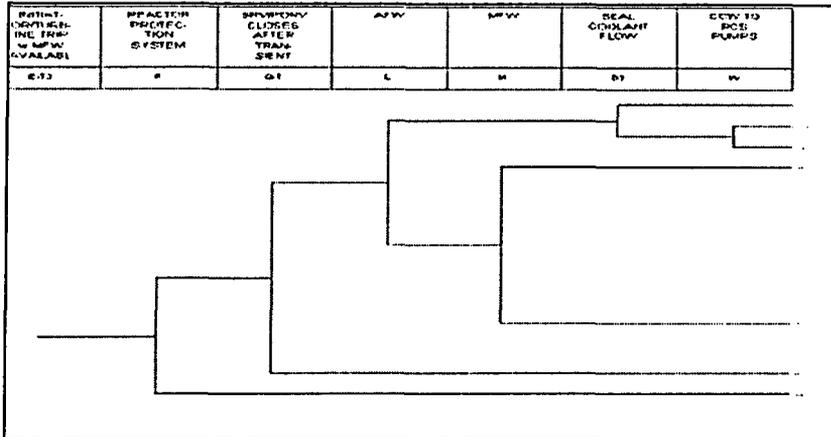
- A 3-loop design with each unit rated at 2441 MW_{th} or 788 MW_e
- The PRA model used is based on NUREG-1150 and constructed using SAPHIRE.
- The benchmark system is assumed to be applicable to each loop.*

*While the benchmark system is based on a 2-loop design, this assumption is necessitated by: a) availability of a documentation on digital feedwater control systems, and, b) accessibility of available PRA models

30



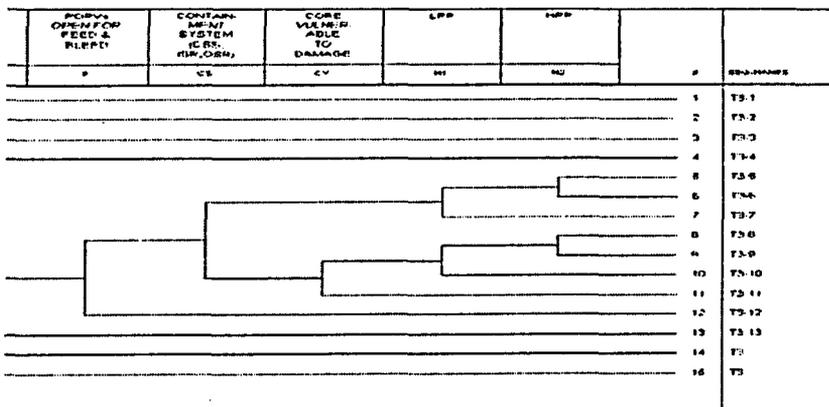
Example PRA Model – Turbine Trip Event Tree (1/2)



31



Example PRA Model – Turbine Trip Event Tree (2/2)



32



DFM - Background

- Developed by ASCA, Inc. in the 1990s as a software tool to support Probabilistic Risk Assessment (PRA)
- Software was used in the safety analysis of several software controlled systems. The results validated DFM's ability to handle software & hardware interactions and to perform dynamic analysis
 - Digital feedwater control system in an advanced Pressurized Water Reactor (NUREG/CR 6465 – April 1996)
 - Control system for the Combustion Module-1 System (NASA Glenn Research Center Shuttle Experiment)

33



DFM – Features (1/2)

- Graphic modeling environment and automated analysis engine that can handle
 - cause-effect relationships
 - time-dependent relationships
 - feedback loops
- Discretized state-vectors represent key process parameters
- Mapping between the discretized state-vectors governed by multi-valued logic rules
 - decision tables
 - transfer-boxes
 - transition-boxes

34



DFM - Features (2/2)

- A DFM model can be analyzed
 - inductively (i.e., in forward-tracking / discrete-event-simulation mode) to verify intended behavior and/or to track the effects of possible combinations of component failures on overall system operation / behavior
 - deductively to determine all possible combinations of basic causes leading to any system event which can be represented in terms of the modeled process variables. This is equivalent to developing dynamic fault trees
- The single system DFM model can be interrogated in many ways:
 - Deductively to analyze a large number of top events
 - Inductively to simulate the sequences from many different initial conditions
- In the deductive mode, current software identifies the prime implicants. Prime implicants are the multi-valued logic equivalent of minimal cut sets in fault tree analysis

35



DFM - Quantification

- In a deductive analysis, the top event can be quantified from the probabilities of the basic events that make up the prime implicants
- The set of prime implicants is first converted to a logically equivalent set of mutually exclusive implicants
 - This process is the multi-valued logic equivalent of the Binary Decision Diagram (BDD) procedure for solving fault-trees
- The top event probability is obtained as the sum of the probabilities of the mutually exclusively implicants
- The quantification results are compatible with standard PRA software formats (e.g., SAPHIRE)
 - The top event probability and/or the set of mutually exclusive implicants (with probabilities) can be exported onto SAPHIRE event-tree and/or fault-tree structures

36



Basic Steps in a Typical DFM Analysis

- Step 1: Model construction
 - Construct DFM model of system of interest
 - Representing the system behavior and flow of causality
 - Model is a network of nodes, transfer-boxes, transition-boxes and associated arc connections
- Step 2: System Analysis
 - Use DFM inductive and deductive engines to:
 - Verify specified system behavior (can be done on system "design model"), and/or,
 - Systematically identify causal links between system failure modes and basic component failure modes (Automated FMEA and/or identification of prime implicants for system failure "Top-Events" of interest), and/or,
 - Define test sequences specifically suited to identify and isolate various classes of possible faults. This feature is especially useful for generating input vectors for testing software based systems 37



Uses of DFM Analyses

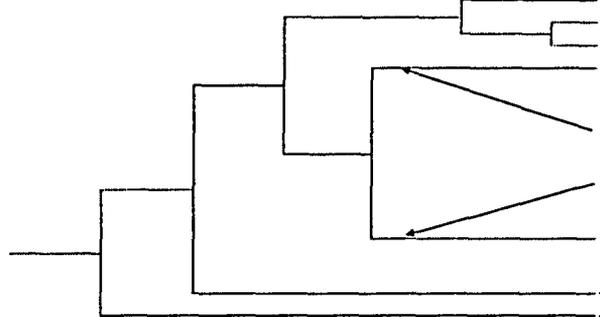
- Deductive and inductive procedures can be combined to carry out 3 types of analyses.
 - System Verification
 - Using mostly the inductive procedure, check that the system will behave as it is supposed to under different initial and boundary conditions
 - Failure and Fault Analysis
 - Automated Failure Modes and Effects Analysis (FMEA)
 - Use inductive analysis to propagate of basic component failure combinations to identify consequences at the system level
 - Prime Implicants
 - Use deductive analysis to identify combinations of component failure modes and software conditions that could cause an undesirable system event to occur
 - Test Sequences
 - Identify test patterns to prove or disprove the presence of specific types of faults in the actual software modules
 - An extension of the procedure used in testing of binary circuits



Example of DFM Supported Risk Assessment

From the Event Tree model in the master PRA, identify the pivotal event that needs to be analyzed by DFM

INITIAL CAUSE/ PRE-TOP EVENT AVAILABILITY	REACTOR PROTEC- TION SYSTEM	SP/POPUP CLOSES AFTER TOP- EVENT	AFW	MFW	SCAL COOLANT FLOW	CCW TO RCS PUMPS
E-13	Y	G-7	L	W	W	W



Analyze the digital feedwater control system with DFM to find the prime implicants for these 2 branches

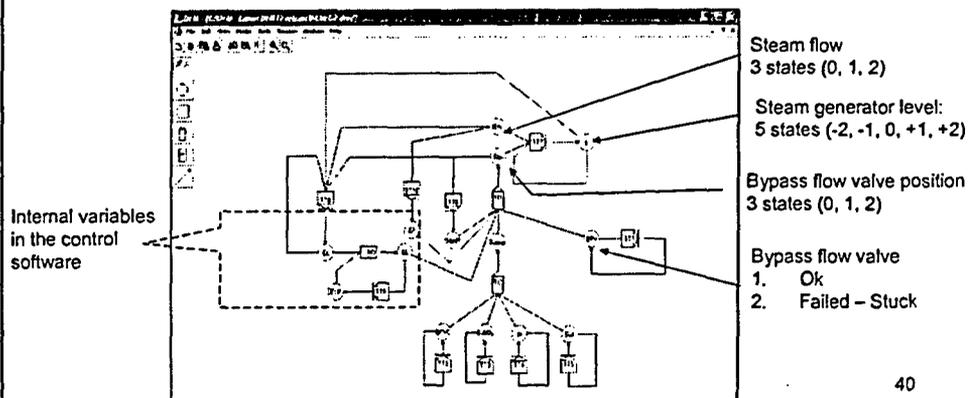
39



Example Initiating Event DFM Model

Construct a DFM model to represent the causality flow of the example initiating event:

- Discretized DFM nodes represent key process parameters.
- Transfer functions between nodes expressed as decision tables.



40



Example Initiating Event DFM Analysis

- Use DFM to determine the prime implicants for the top events:
 - Steam generator high level
 - Steam generator low level
- The Top Events were defined as a conjunction of the node states at different time steps.
 - The SG high level top event was defined as:

$L = 2 @ t = 0 \wedge$
 $L = 1 @ t = -1 \wedge$
 $L = 0 @ t = -2 \wedge$
 $ELP = 0 @ t = -2 \wedge$
 $CL = 0 @ t = -2$

41



DFM - Prime Implicants for SG High Level (1/2)

- The SG high level top event was analyzed deductively for 2 time steps
- 11 prime implicants were identified
- The "BFV fails stuck at 44 s condition that leads to high SG level" is a subset of the initial condition identified in Prime Implicant #5

1	$L = 0 @ t = -2 \wedge$ $ELP = 0 @ t = -2 \wedge$ $CL = 0 @ t = -2 \wedge$ $SbsP = 2 @ t = -2 \wedge$ $SN = 1 @ t = -2 \wedge$ $Out = Loss @ t = -2$	$Level\ is\ normal @ t = -2$ $Level\ error\ is\ normal @ t = -2$ $Compensated\ level\ normal @ t = -2$ $Feed\ for\ Steam\ for @ t = -2$ $Loss\ of\ feed @ t = -2$
2	$L = 0 @ t = -2 \wedge$ $ELP = 0 @ t = -2 \wedge$ $CL = 0 @ t = -2 \wedge$ $SbsP = 2 @ t = -2 \wedge$ $SN = 1 @ t = -2 \wedge$ $BFVC = Failed @ t = -2$	$Level\ is\ normal @ t = -2$ $Level\ error\ is\ normal @ t = -2$ $Compensated\ level\ normal @ t = -2$ $Feed\ for\ Steam\ for @ t = -2$ $Breaker\ for\ valve\ stuck\ at @ t = -2$
3	$L = 0 @ t = -2 \wedge$ $ELP = 0 @ t = -2 \wedge$ $CL = 0 @ t = -2 \wedge$ $SbsP = 2 @ t = -2 \wedge$ $SN = 1 @ t = -2 \wedge$ $SbkUp = Down @ t = -2$	$Level\ is\ normal @ t = -2$ $Level\ error\ is\ normal @ t = -2$ $Compensated\ level\ normal @ t = -2$ $Feed\ for\ Steam\ for @ t = -2$ $Breaker\ computer\ is @ t = -2$
4	$L = 0 @ t = -2 \wedge$ $ELP = 0 @ t = -2 \wedge$ $CL = 0 @ t = -2 \wedge$ $SbsP = 1 @ t = -2 \wedge$ $SN = 1 @ t = -2 \wedge$ $In = Loss @ t = -2$	$Level\ is\ normal @ t = -2$ $Level\ error\ is\ normal @ t = -2$ $Compensated\ level\ normal @ t = -2$ $Feed\ for\ Steam\ for @ t = -2$ $Loss\ of\ feed @ t = -2$
5	$L = 0 @ t = -2 \wedge$ $ELP = 0 @ t = -2 \wedge$ $CL = 0 @ t = -2 \wedge$ $SbsP = 2 @ t = -2 \wedge$ $SN = 1 @ t = -2 \wedge$ $BFV = F-3 @ t = -2$	$Level\ is\ normal @ t = -2$ $Level\ error\ is\ normal @ t = -2$ $Compensated\ level\ normal @ t = -2$ $Feed\ for\ Steam\ for @ t = -2$ $Breaker\ for\ valve\ stuck @ t = -2$

42



DFM - Prime Implicants for SG High Level (2/2)

6	L = 0 @ 1 = -2 A ELP = 0 @ 1 = -2 A CL = 0 @ 1 = -2 A SbrP = 1 @ 1 = -2 A SN = 0 @ 1 = -2 A Out = Loss @ 1 = -2	Level is normal @ 1 = -2 Level error is nominal @ 1 = -2 Compensated level is nominal @ 1 = -2 Feed flow > Steam flow @ 1 = -2 Loss of outputs @ 1 = -2
7	L = 0 @ 1 = -2 A ELP = 0 @ 1 = -2 A CL = 0 @ 1 = -2 A SbrP = 1 @ 1 = -2 A SN = 0 @ 1 = -2 A BFVC = Failed @ 1 = -2	Level is normal @ 1 = -2 Level error is nominal @ 1 = -2 Compensated level is nominal @ 1 = -2 Feed flow > Steam flow @ 1 = -2 Bypass flow valve controller failed @ 1 = -2
8	L = 0 @ 1 = -2 A ELP = 0 @ 1 = -2 A CL = 0 @ 1 = -2 A SbrP = 1 @ 1 = -2 A SN = 0 @ 1 = -2 A BkUp = Down @ 1 = -2	Level is normal @ 1 = -2 Level error is nominal @ 1 = -2 Compensated level is nominal @ 1 = -2 Feed flow > Steam flow @ 1 = -2 Backup computer is down @ 1 = -2
9	L = 0 @ 1 = -2 A ELP = 0 @ 1 = -2 A CL = 0 @ 1 = -2 A SbrP = 1 @ 1 = -2 A SN = 0 @ 1 = -2 A In = Loss @ 1 = -2	Level is normal @ 1 = -2 Level error is nominal @ 1 = -2 Compensated level is nominal @ 1 = -2 Feed flow > Steam flow @ 1 = -2 Loss of inputs @ 1 = -2
10	L = 0 @ 1 = -2 A ELP = 0 @ 1 = -2 A CL = 0 @ 1 = -2 A SbrP = 1 @ 1 = -2 A SN = 0 @ 1 = -2 A BFV = FS @ 1 = -2	Level is normal @ 1 = -2 Level error is nominal @ 1 = -2 Compensated level is nominal @ 1 = -2 Feed flow > Steam flow @ 1 = -2 Bypass flow valve failed stuck @ 1 = -2
11	L = 0 @ 1 = -2 A ELP = 0 @ 1 = -2 A CL = 0 @ 1 = -2 A SbrP = 2 @ 1 = -2 A SN = 0 @ 1 = -2 A BkUp = OK @ 1 = -2 A In = OK @ 1 = -2 A BFVC = OK @ 1 = -2 A Out = OK @ 1 = -2 A BFV = FS @ 1 = -2	Level is normal @ 1 = -2 Level error is nominal @ 1 = -2 Compensated level is nominal @ 1 = -2 Feed flow > Steam flow @ 1 = -2 Backup computer is OK @ 1 = -2 Inputs are OK @ 1 = -2 Bypass flow valve controller is OK @ 1 = -2 Outputs are OK @ 1 = -2 Bypass flow valve is OK @ 1 = -2

43



DFM - Prime Implicants for SG Low Level

- The SG low level top event was analyzed deductively for 2 time steps
- 11 prime implicants were identified
 - 10 prime implicants correspond to steam flow > feed flow and the one of the following failures:
 - Loss of outputs, OR
 - Bypass flow valve controller failure, OR
 - Backup computer failure, OR
 - Loss of inputs, OR
 - Bypass flow valve failed stuck
 - The "BFV fails stuck at 43 s condition that leads to low SG level" is a subset of the initial condition identified in this Prime Implicant
 - 1 prime implicant corresponds to steam flow >> feed flow such that the controller is not able to correct the mismatch fast enough the prevent the SG level from dropping to the very low level

44



Markov Methodology

1. Define Top Events
2. Partition the state space or the controlled variable state space (CVSS) into computational cells
3. Determine the system hardware/software/ firmware configurations
4. Determine the cell-to-cell transition probabilities
5. Determine the component state transition probabilities
6. Determine the pdf and Cdf for the Top Events and s-importance of component state configurations to the Top Events

45



Markov Methodology – Step 1

The controller is regarded as failed if water level in SGn rises above +30 inches and falls below -24 inches. Subsequently, there are two Top Events:

1. $x_n < -24$ inches (Low Level), and,
2. $x_n > +30$ inches (High Level).

46



Markov Methodology – Step 2 (for an example turbine trip with main computer failed)

The relevant system equations are

$$\frac{d\tilde{E}_1}{dt} = \frac{0.001\tilde{E}_1 - 1.268\tilde{E}_2 - 1.201\tilde{E}_3 - 0.064 \cdot 21022}{109} \cdot \frac{1}{10-t} - 1$$

$$r_2 \frac{d\tilde{E}_2}{dt} = C_{L2} - 3.06(t-1) + 0.0014\tilde{E}_1 - 1.268\tilde{E}_2 - 1.201\tilde{E}_3 - 1.2019$$

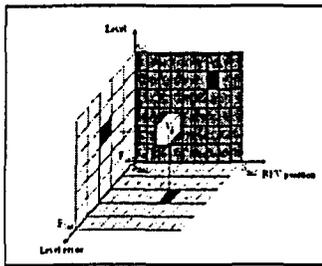
$$\frac{0.065 \cdot 35.05 r_1}{(10-t)^{0.2}}$$

$$- r_3 \frac{d\tilde{E}_3}{dt} = C_{L3}$$

$$\tilde{E}_2(t) = 1 + \int_0^t \left\{ 0.065 \cdot 1500 e^{-r_2 t'} - 0.065 \cdot 1500 \frac{(1-r_2 t')}{r_2} \right\} dt' \cdot \frac{e^{-r_2(t-t')}}{(10-t)^{0.2}}$$

$$- 1200 \tilde{E}_3(t) \cdot 54$$

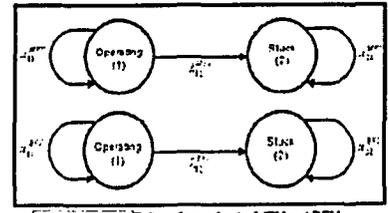
A corresponding CVSS partitioning scheme is



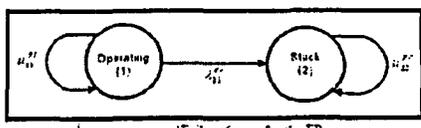
47



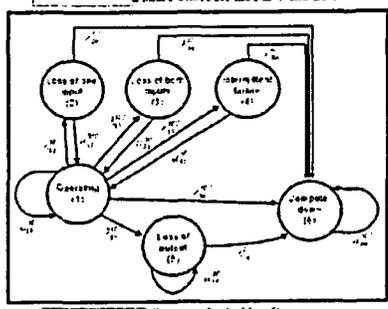
Markov Methodology – Step 3 (1/2) (for some benchmark system example components)



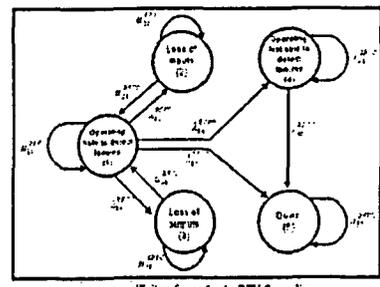
Failure States for the MFV and BFV



Failure States for the FP



Failure state for the Main Computer

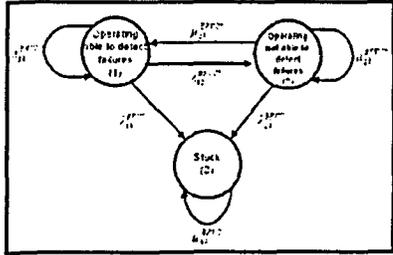


Failure States for the BFV Controller

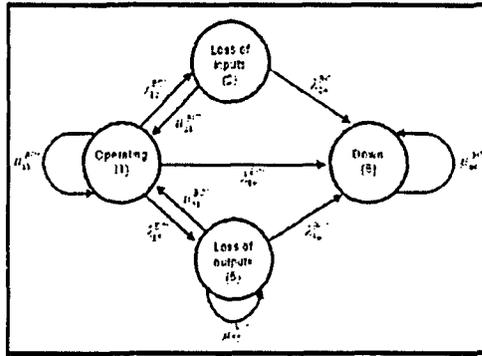
48



Markov Methodology – Step 3 (2/2) (for an example turbine trip with main computer failed)



Combined BFV and Controller



Backup Computer

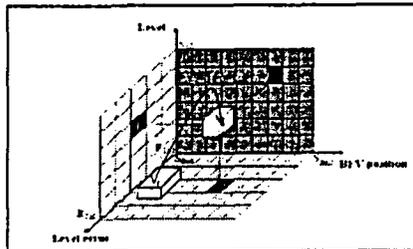


Markov Methodology – Step 4 (1/2)

Transition probability from cell j' to j for system configuration n' can be found from

$$g(j | j', n', k) = \frac{1}{V_{j'} V_j} \int dx e_j[\tilde{x}(x', n', k)]$$

$$e_j(y) = \begin{cases} 1 & \text{if } y \in V_j \\ 0 & \text{otherwise} \end{cases}$$





Markov Methodology – Step 4 (2/2)

Level
 Level Error
 Compensated Level
 BFV Aperture

BFV	CPU	Frame	1-1-1	1-1-2	1-1-3	1-1-4	1-1-5	1-1-6	1-1-7	1-1-8	1-1-9	1-1-10	1-1-11	1-1-12	1-1-13	1-1-14
OK/ABLE	OK	0-0-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-0-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-0-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	0-1-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-1-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-1-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	0-2-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-2-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-2-0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	0-0-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-0-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-0-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	0-1-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-1-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-1-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	0-2-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-2-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-2-1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	0-0-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-0-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-0-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	0-1-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-1-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-1-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	0-2-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	1-2-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
OK/ABLE	OK	2-2-2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

A small portion of the overall matrix which contains the elements $g(n',j',k)$ for an example turbine trip with main computer failed. The first two columns define the components state combination n' while the third one defines the cell V_j . Each cell V_j and V_j' is represented as an array of four elements corresponding to level, level error, compensated level and BFV position, respectively.

51



Markov Methodology – Step 5

Transition probability $h(n|n',j' \rightarrow j, \Delta t)$ from configuration n' to n given that the controlled variables move from cell j' to j can be found from the control laws and component failure modes. Table below shows the $h(n|n',j' \rightarrow j, \Delta t)$ for an example turbine trip with main computer failed

$n' n$	1	2	3	4	5	6	7	8	9	10	11	12
1	$\mu_{11} \Delta t$	$\lambda_{12} \Delta t$	$\lambda_{13} \Delta t$	$\lambda_{14} \Delta t$	$\lambda_{15} \Delta t$	$\lambda_{16} \Delta t$	$\lambda_{17} \Delta t$	$\lambda_{18} \Delta t$	$\lambda_{19} \Delta t$	$\lambda_{110} \Delta t$	$\lambda_{111} \Delta t$	$\lambda_{112} \Delta t$
2	$\lambda_{21} \Delta t$	0	0	$\lambda_{24} \Delta t$	$\lambda_{25} \Delta t$	C	0	$\lambda_{28} \Delta t$	$\lambda_{29} \Delta t$	0	0	$\lambda_{212} \Delta t$
3	0	0	0	0	C	C	0	0	$\lambda_{39} \Delta t$	0	$\lambda_{311} \Delta t$	$\lambda_{312} \Delta t$
4	0	0	0	0	C	C	0	0	0	0	0	$\lambda_{412} \Delta t$
5	$\lambda_{51} \Delta t$	$\lambda_{52} \Delta t$	$\lambda_{53} \Delta t$	$\lambda_{54} \Delta t$	$\lambda_{55} \Delta t$	$\lambda_{56} \Delta t$	$\lambda_{57} \Delta t$	$\lambda_{58} \Delta t$	$\lambda_{59} \Delta t$	$\lambda_{510} \Delta t$	$\lambda_{511} \Delta t$	$\lambda_{512} \Delta t$
6	$\lambda_{61} \Delta t$	0	0	$\lambda_{64} \Delta t$	$\lambda_{65} \Delta t$	C	0	$\lambda_{68} \Delta t$	$\lambda_{69} \Delta t$	0	0	$\lambda_{612} \Delta t$
7	$\lambda_{71} \Delta t$	0	$\lambda_{73} \Delta t$	$\lambda_{74} \Delta t$	$\lambda_{75} \Delta t$	C	$\lambda_{77} \Delta t$	$\lambda_{78} \Delta t$	$\lambda_{79} \Delta t$	0	$\lambda_{711} \Delta t$	$\lambda_{712} \Delta t$
8	0	0	0	$\lambda_{84} \Delta t$	C	C	0	$\lambda_{88} \Delta t$	0	0	0	$\lambda_{812} \Delta t$
9	0	0	0	0	C	C	0	0	$\mu_{99} \Delta t$	$\lambda_{910} \Delta t$	$\lambda_{911} \Delta t$	$\lambda_{912} \Delta t$
10	0	0	0	0	C	C	0	0	$\lambda_{109} \Delta t$	0	0	$\lambda_{1012} \Delta t$
11	0	0	0	0	C	C	0	0	$\lambda_{119} \Delta t$	0	$\mu_{1111} \Delta t$	$\lambda_{1112} \Delta t$
12	0	0	0	0	C	C	0	0	0	0	0	$\mu_{1212} \Delta t$

BFV'	BF	n
OK able	OK	1
OK able	Loss of input	2
OK able	Loss of output	3
OK able	Down	4
OK not able	OK	5
OK not able	Loss of input	6
OK not able	Loss of output	7
OK not able	Down	8
Stuck	OK	9
Stuck	Loss of input	10
Stuck	Loss of output	11
Stuck	Down	12

Component State Combinations

52



Markov Methodology – Step 6

$$p_{n,j}[(k+1)\Delta t] = \sum_{j'} \sum_{n'} g(j | j', n', k) h(n \rightarrow m | j' \rightarrow j) p_{n',j'}(k\Delta t)$$

$$F_y(k) = \sum_{n=1}^N p_{n,y}(k) \quad \equiv \text{Cdf for Top Event } y$$

$$w_{n,y}(k) = \frac{1}{\Delta t} [F_{n,y}(k+1) - F_{n,y}(k)] \quad \equiv \text{pdf for Top Event } y$$

$$(Im)_{n,y}(k) = \frac{\sum_{n=1}^N w_{n,y}(k)}{\sum_{n=1}^N w_{n,y}(k)} \quad \equiv s\text{-importance of configuration } n \text{ to Top Event } y$$

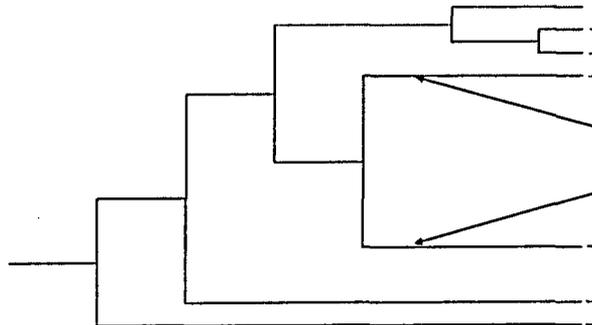
53



Incorporation of the DFM and Markov Models into PRA – DFM

The outputs from the analysis of the MFW DFM model are integrated back to the Event Tree model of the master PRA.

REBAT. DFM/IMP. INE. INE. w/ MFW AVAILAB.	REACTOR PROTECTION SYSTEM	SYMPOHY CLOSURE AFTER TRANS. SENT	M/W	M/W	SEAL. COOLANT FLOW	DCW TO RCS PUMPS
013	E	01	L	#	00	W



DFM prime implicants are integrated back into the Master PRA

54



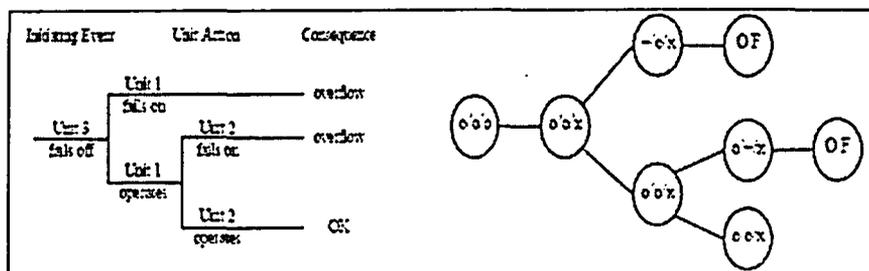
Incorporation of the DFM and Markov Models into PRA – Markov Model (1/5)

- The basic idea of this approach is to use the transition matrix of the Markov model of the system as a graph representation of a finite state machine
- With this representation and standard search algorithms it is possible to explore all possible paths to failure (scenarios) with associated probabilities and to construct dynamic event trees (DETs) of arbitrary depth.
- The DET is represented by a tree data structure. A tree data structure is composed of "nodes" –where information is stored–and "links" that connect the nodes. The nodes in the tree data structure correspond to the branching points in the DET and the links represent the branches.
- The DETs can then be incorporated into an existing PRA model through the regular features of the software that created it (e.g. SAPHIRE)

55



Incorporation of the DFM and Markov Models into PRA – Markov Model (2/5)



56



Incorporation of the DFM and Markov Models into PRA – Markov Model (3/5)

```
initialise DET root node to initial state and probability 1
add DET root node to queue Q of nodes to process
while Q is not empty
  remove next node N = (S,P) from Q
  if S is not a sink state
    for each possible state S'
      if Prob[S,S'] > 0
        compute probability P' for this branch as Prob[S,S'] * P
        if P' > epsilon
          create new node N' = (S',P')
          add N' to the list of children of N in the DET
          add N' to queue Q of nodes to process
        end if
      end if
    end for each
  end if
end while
```

Algorithm 1 to Generate DETs from Markov Model

57



Incorporation of the DFM and Markov Models into PRA – Markov Model (4/5)

```
initialise DET root node to initial state(s) and probability 1
add DET root node to queue Q of nodes to process
while Q is not empty
  remove node N = <(S1,P1),..., (Sk,Pk)> from Q
  initialise A: array [1..number of configurations] of nodes
  for each pair (S,P) in the list of pairs in N
    if S is not a sink state
      for each possible state S'
        if Prob[S,S'] > 0
          compute probability P' for this branch as Prob[S,S'] * P
          if P' > epsilon
            if S' is not in the list of states in node A[Conf(S')]
              add (S',P') to the list of states in node A[Conf(S')]
            else
              add P' to the current probability value associated with S'
              in the list of states in node A[Conf(S')]
            end if
          end if
        end if
      end for each
    end if
  end for each
  add all the nodes in A that contain at least one pair
  to the list of children of N in the DET and to queue Q
end while
```

Algorithm 2 to Generate DETs from Markov Model

58



Incorporation of the DFM and Markov Models into PRA – Markov Model (5/5)

EventTreeDisplay

Timer: 5 seconds

State	Configuration	Process	Probability
1680	BPV: STUCK PWC OK	$-2.00 \leq x_{1a} \leq -1.00$ $-1,000.00 \leq C_{1a} \leq -1.00$ $-500.00 \leq C_{2a} \leq -100.00$ $0.00 \leq S_{2a} \leq 5.00$	2.882E-7
1685	BPV: STUCK BUC OK	$x_{2a} < -2.00$ (LOW) $-1,000.00 \leq C_{1a} \leq -1.00$ $-500.00 \leq C_{2a} \leq -100.00$ $0.00 \leq S_{2a} \leq 5.00$	1.818E-6
1736	BPV: STUCK BUC OK	$-2.00 \leq x_{2a} \leq -1.00$ $-1,000.00 \leq C_{1a} \leq -1.00$ $-100.00 \leq C_{2a} \leq 100.00$ $0.00 \leq S_{2a} \leq 5.00$	5.244E-7
1741	BPV: STUCK BUC OK	$x_{2a} < -2.00$ (LOW) $-1,000.00 \leq C_{1a} \leq -1.00$ $-100.00 \leq C_{2a} \leq 100.00$ $0.00 \leq S_{2a} \leq 5.00$	1.563E-6
1715	BPV: STUCK BUC OK	$-2.00 \leq x_{2a} \leq -1.00$ $4.00 \leq C_{1a} \leq 100.00$ $-500.00 \leq C_{2a} \leq -100.00$ $0.00 \leq S_{2a} \leq 5.00$ $x_{2a} < -2.00$ (LOW)	4.241E-6

Graphical Interface for the Standalone Analysis of DETs

59



Interfacing with SAPHIRE - General

- SAPHIRE (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations) been developed at INL with U.S. N.R.C support.
- The code was first developed by INL in the 1980's in order to create a software PRA code for personal computers.
- The first version was known IRRAS (Integrated Risk and Reliability Analysis System).
- Several modules were written to compliment IRRAS and were all integrated into a single package forming the SAPHIRE code.
- SAPHIRE uses both graphical and logic editors to construct and modify ETs and FTs

60



Interfacing with SAPHIRE - Input

Time	System Configuration	Process State	Explanation
t=0	BFV: OKABLE BC: OK	$-0.17 \leq x_1 \leq 0.17$ $-1.00 \leq E_{11} \leq 1.00$ $-100.00 \leq C_{11} \leq 100.00$ $0.00 \leq S_{11} \leq 30.00$	Both BFV and BC are in their operational state, and all process variables are in their normal range.
t=1	BFV: OKABLE BC: OK	$-1.05 \leq x_1 \leq -0.17$ $2.00 \leq E_{11} \leq 3.00$ $-100.00 \leq C_{11} \leq 100.00$ $0.00 \leq S_{11} \leq 30.00$	Level is low, BFV opens more.
t=2	BFV: OK/UNABLE BC: LOSS-OUT	$-1.05 \leq x_1 \leq -0.17$ $-1000.00 \leq E_{11} \leq -1.00$ $-100.00 \leq C_{11} \leq 100.00$ $0.00 \leq S_{11} \leq 3.00$	BFV becomes unable to recognize process with BC and BC experiences a loss of output, which goes undetected by BFV but results in BFV closing.
t=3	BFV: OK/UNABLE BC: LOSS-OUT	$-2.00 \leq x_1 \leq -1.00$ $-1000.00 \leq E_{11} \leq -1.00$ $-100.00 \leq C_{11} \leq 100.00$ $0.00 \leq S_{11} \leq 3.00$	Level is lower, BC experiences loss of output again, but now BFV recognizes the problem and switches to STUCK.
t=4	BFV: STUCK BC: OK	$-2.00 \leq x_1 \leq -1.00$ $-1000.00 \leq E_{11} \leq -1.00$ $-100.00 \leq C_{11} \leq 100.00$ $0.00 \leq S_{11} \leq 3.00$	BC recovers its output slightly, but it's not new.
t=5	BFV: STUCK BC: OK	$x_1 \leq -2.00$ (LOW) $-1000.00 \leq E_{11} \leq -1.00$ $-100.00 \leq C_{11} \leq 100.00$ $0.00 \leq S_{11} \leq 3.00$	The level falls below the LOW setpoint and the system fails.

XXXX-DEMO, DET-D0 =
 DET-D0 AND /BFV-OK-UNABLE-T0 /BC-LOSS-OUT-T0
 CONT /BFV-OK-UNABLE-T1 /BC-LOSS-OUT-T1
 CONT BFV-OK-UNABLE-T2 BC-LOSS-OUT-T2
 CONT /BFV-OK-UNABLE-T3 BC-LOSS-OUT-T3
 OUT-T4 CONT BFV-STUCK-T4 /BC-LOSS-OUT-T5
 CONT BFV-STUCK-T5 /BC-LOSS-OUT-T5

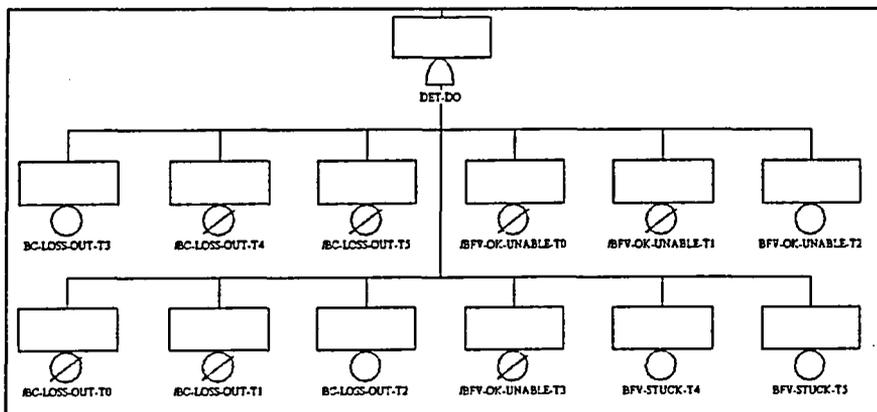
SAPHIRE Input for the Example DET

Event Sequence from an Example DET

61



Interfacing with SAPHIRE - Output



SAPHIRE Output for the Example DET

62



Interfacing with SAPHIRE – Post-Processing

1. Select the MAR-D feature under Utilities
2. Extract the desired fault tree, end state, or sequence cut sets to be exported.
3. This process will create a text file with a .FTC extension (.ESC for event tree end state cut sets, or .SQC for sequence cut sets).
4. Edit the text file to remove time inconsistencies.
5. Re-import cut sets back into SAPHIRE and then quantify using appropriate failure data.

63



Proposed Benchmark, Procedures and the Requirements for the Reliability Modeling of Digital Instrumentation and Control Systems – Benchmark Requirements*

Loosely-Control Coupled Benchmark System Requirements

1. Provides a digital system with a clock
 1. Provides information about a physical process through sampling
 2. Provides a digital system that uses the clock to perform measurements
 3. Provides a system that has roundoff
 4. Provides a system that has truncation
2. Provides explicit representation of the power requirements that are needed for the digital systems
 1. Includes loss of power
 2. Includes low power
 3. Includes power spikes
3. Provides digital systems in which there are real-time constraints
4. Provides a polling-based digital system
 1. Events can occur in between polls
 2. Sensors that are being polled can fail to report value
5. Provides an interrupt-driven digital system
 1. Interrupts can occur simultaneously
 2. Interrupts can occur at an excessive rate
 3. There are unused interrupts that may be activated
6. Provides long term storage for a digital system
 1. Includes failures that can occur in the retrieval of information
 2. Include failures that can occur in the saving of information
 3. Include Loosely-Coupled Requirement 3
 4. Include Loosely-Coupled Requirement 2
7. Provides a digital system that computes values based on the process physics
8. Provides a self-diagnostic system
 1. Contradictory data can be delivered to the system
 2. Events can occur while in self-diagnostic mode
9. Provides a watchdog timer
 1. Instances in which there is no safe state
 2. Instances in which the watchdog timer fails

Tightly-Control Coupled Benchmark System Requirements

1. Includes Loosely-Control Coupled Requirements
2. Provides digital systems networked together
 1. Includes failures in the networked systems
 2. Includes failures in connecting components (wires, routers, etc.)
 3. Include failures of any protocol used
 4. Include failures as a result of the network topology
 5. Includes transient failures in the network
3. Provides an analog backups to digital systems that include failures in which either the digital or analog system has failed
4. Provides digital systems that share memory
 1. Includes failures which involve data races
 2. Include failures which involves both deadlocks and starvation
5. Provides digital systems that share external resources
 1. Includes failures which involves both deadlocks and starvation
 2. Includes network failures
6. Provides a digital system with fault tolerance that includes Byzantine failures
7. Provides a database for a digital system
 1. Include Loosely-Control Coupled Requirement 6
 2. Include failures that can force the database to be inconsistent
8. Provides digital systems that have different configurations/versions of software installed on each of the systems
 1. Includes all permutations of homogeneous and heterogeneous software and/or hardware

*J. Krachenbaum, M. Slovsky, P. Bucco, T. Adema, S.A. Arndt, "Benchmark Development for Comparing Digital Instrumentation and Control System Reliability Modeling Approaches", PSA DS, on CD-ROM, American Nuclear Society, LaGrange Park, IL (September 2005)

64



Proposed Benchmark, Procedures and the Requirements for the Reliability Modeling of Digital Instrumentation and Control Systems – Benchmark Compliance

- The benchmark problem satisfies most of the benchmark requirements
- It is also representative of the digital SG feedwater control systems used in operating PWRs.
- Some of the requirements are less relevant to systems use in the current nuclear reactor protection and control systems and are not represented by the benchmark system (e.g. networking, shared external resources).
- Two particularly challenging feature of the benchmark system from a reliability modeling viewpoint are the following:
 - Reliability modeling of some of its fault tolerance capabilities requires consideration of the system history
 - System failure mode may depend on the exact timing of failure events, and not just the order of failure events

65



Proposed Benchmark, Procedures and the Requirements for the Reliability Modeling of Digital Instrumentation and Control Systems – Modeling Requirements*

1. The model must be able to predict encountered and 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 quantitatively be able to represent dependencies between failure events accurately.
5. The model must be designed so it is not hard for an analyst to learn the concepts and it is not be hard to implement.
6. The data used in the quantification process must be credible to a significant portion of the technical community.
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.

*T. Aldener, D.W. Miller, M. P. Stovsky, J. Kaschenbaum, P. Bucci, A. W. Fentman, L. A. Mangin, Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901, U.S. Nuclear Regulatory Commission, Washington, D.C. (February 2006)

66



Proposed Benchmark, Procedures and the Requirements for the Reliability Modeling of Digital Instrumentation and Control Systems – Modeling Compliance

- Neither methodology (Markov or DFM) is based on purely operating experience and both have been tested on both loosely and tightly control-coupled systems. In that respect, both methodologies predict encountered and future failures well (Requirement 1).
- Both methodologies can account for all the features of the benchmark system which is representative of the digital SG feedwater control systems used in operating PWRs as well as containing the features of digital I&C systems used in nuclear power plants, in general (Requirement 2).
- Both methodologies make valid and plausible assumptions* (Requirement 3).
- Both methodologies can quantitatively represent dependencies between failure events accurately (Requirement 4).

*For example, the assumption that process dynamics can be represented through a Markov transition matrix or a decision table (of DFM) have been validated through previous work. Similarly, the normal operation of the benchmark system and its assumed failure modes were based on operating PWRs as well as other digital I&C systems encountered in practice. Both methodologies can account for all the features of the benchmark system.

67



Proposed Benchmark, Procedures and the Requirements for the Reliability Modeling of Digital Instrumentation and Control Systems – Modeling Compliance

- Both methodologies can differentiate between a state that fails one safety check and those that fail multiple ones, as well as between faults that cause function failures and intermittent failures (Requirement 8)
- Both methodologies have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results (Requirement 9).
- Both methodologies can 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 (Requirement 10).

68



Proposed Benchmark, Procedures and the Requirements for the Reliability Modeling of Digital Instrumentation and Control Systems – Challenges

- Both methodologies have substantially steeper learning curves and are more labor intensive than the conventional ET/FT methodology (Requirement 5).
- The failure data used by either methodology for quantification are not necessarily credible to a significant portion of the technical community (Requirement 6). However, the proposed methodologies can be used to obtain qualitative information on the failure characteristics of digital I&C systems (i.e. prime implicants) as well as quantitative.
- Finally, the proposed methodologies may require highly time-dependent or continuous plant state information (Requirement 11). On the other hand, both methodologies can be also used for simple description of the connectivity between events if the correct system behavior under normal and abnormal operation can be inferred from qualitative arguments only.

69



Summary and Conclusion (1/2)

- A benchmark digital I&C system (feedwater controller of a PWR) has been specified for the assessment of the methodologies proposed for the reliability modeling of digital I&C systems using a common set of hardware/software/firmware states.
- The benchmark system specification includes procedures for system component failure mode identification and failure data acquisition.
- An example initiating event (turbine trip) has been used with the benchmark system to illustrate how the DFM and the Markov methodology can be used for the reliability modeling of digital I&C systems. These methodologies were identified by NUREG/CR-6901 as the methodologies that rank as the top two when evaluated against the requirements for the reliability modeling of digital I&C systems.

70



Summary and Conclusion (2/2)

- Both methodologies can be used to obtain qualitative as well as quantitative reliability information for digital I&C systems
- Possible challenges with the methodologies include:
 - analyst skill levels needed for the implementation of the methodologies,
 - computational demand for the correct description of the coupling between failure event,
 - acceptability of the data used for quantification by a significant portion of the technical community,
 - need for highly time-dependent or continuous plant state information for correct reliability modeling of the system failure modes if the system failure modes depend on the exact timing of the events
- Some of properties of the benchmark system considered in this first study may not apply to all the reactor protection and control systems in nuclear power plants . For digital I&C systems which may have less complex interaction between the failure events, the conventional ET/FT approach may be adequate for the reliability modeling of the system

71



Next Steps

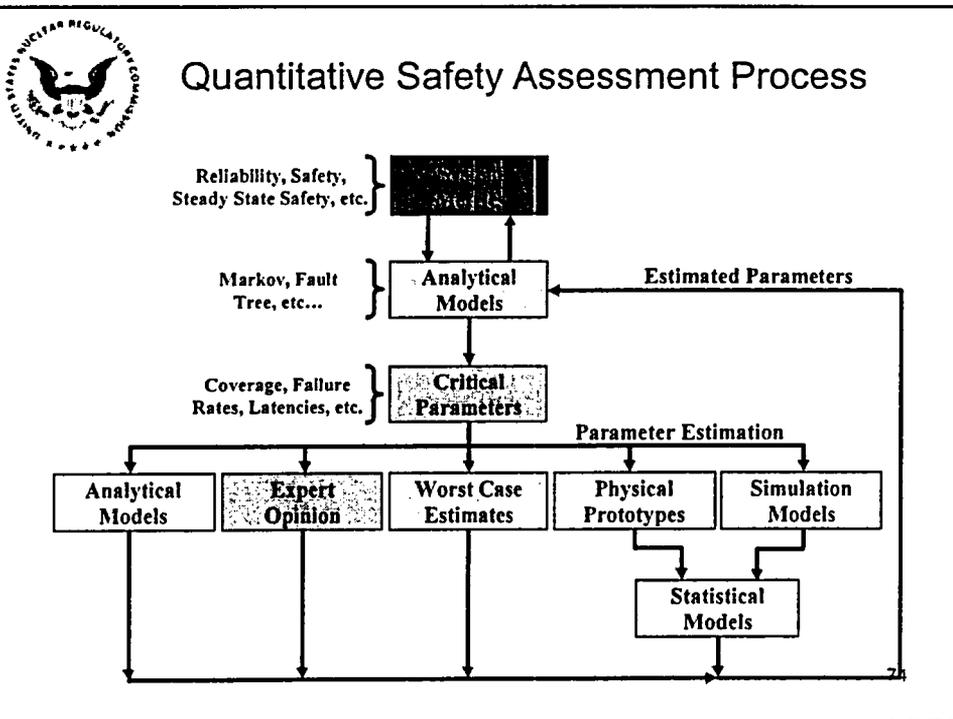
1. A standalone reliability modeling of the full benchmark system using the DFM, Markov methodology and the conventional ET/FT approach.
2. Qualitative comparison of the event combinations that lead to the benchmark system failure as obtained by the DFM, Markov methodology and the conventional ET/FT approach
3. Quantitative evaluation of the models in Item 1 using data obtained through the fault injection procedure as well as other means (e.g. field data, data libraries)
4. Incorporation of models in Item 1 into an existing PRA for selected initiating events (e.g. turbine trip, station blackout, loss of main feedwater)
5. Specification of another benchmark problem reflecting the properties of the reactor protection system
6. Performing Items 1 through 4 for the new benchmark problem.

72



BACKUP SLIDES

73





Fault Injection Methods: Collecting Critical Parameters.

- Principle nature of fault Injection:
 - *Validation technique that is based on the realization of controlled experiments where the observation of the system behavior in presence of faults, is explicitly induced by the deliberate introduction (injection) of faults into the system. Artificial faults are injected into the system and the resulting behavior is observed.*
- Tests the response behavior of the system.
 - *How effective is the system's error detection capability to a class of expected faults.*
- The Purpose of fault Injection:
 - *To uncover deficiencies, oversights, and non-compliant error detection responses of fault tolerant systems.*
- What model parameters are generated by fault injection?
 - *Fault coverage, fault latency times, reconfiguration times, system failure mode response data.*

75



Generic Fault Modeling

- In general, completely proving the sufficiency of the fault model is usually very difficult, if not impossible
- It is more traditional to assume that the fault model is sufficient, justifying this assumption to the greatest extent possible with
 - Experimental data
 - Historical data
 - Results published in literature
- To this end, UVA has developed a behavioral-level generic processor fault model, based on state-of-the-art in fault modeling literature
- Applied this generic processor fault model to the AMD486 processor architecture (benchmark system).
- Tested generic processor fault model for sufficiency via simulations.

76



Generic Fault Modeling

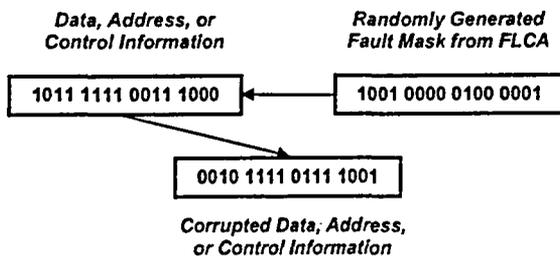
- Generic fault model based on traditional von Neumann architecture performing basic fetch-execute cycle
- Any accessible registers and memory locations can be corrupted
- Detailed fault models have been derived from the literature for
 - Register file/memory faults
 - Register selection faults
 - Program Counter (PC) faults
 - Control Unit/Instruction Decode logic faults
 - Data/address/control bus faults
 - Arithmetic and Logic Unit (ALU) faults

77



Generic Fault Modeling: Fault Injection Implementation

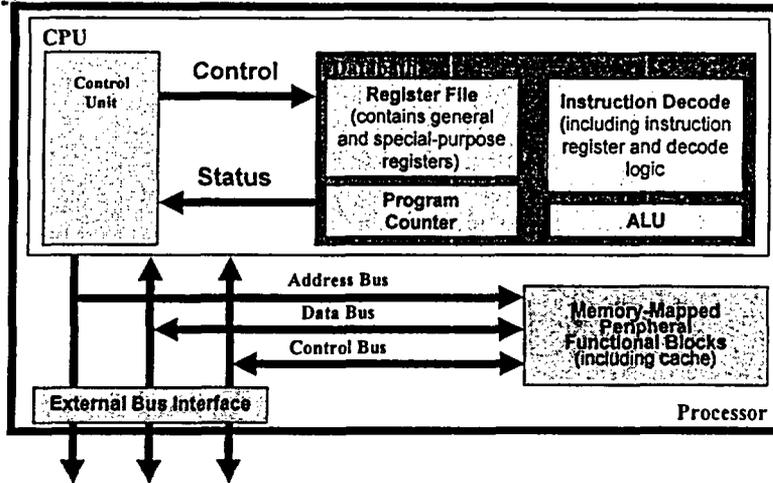
- It is shown that the fault behaviors can be represented by a random fault/error masking process



78



Generic Fault Modeling: Processor Model

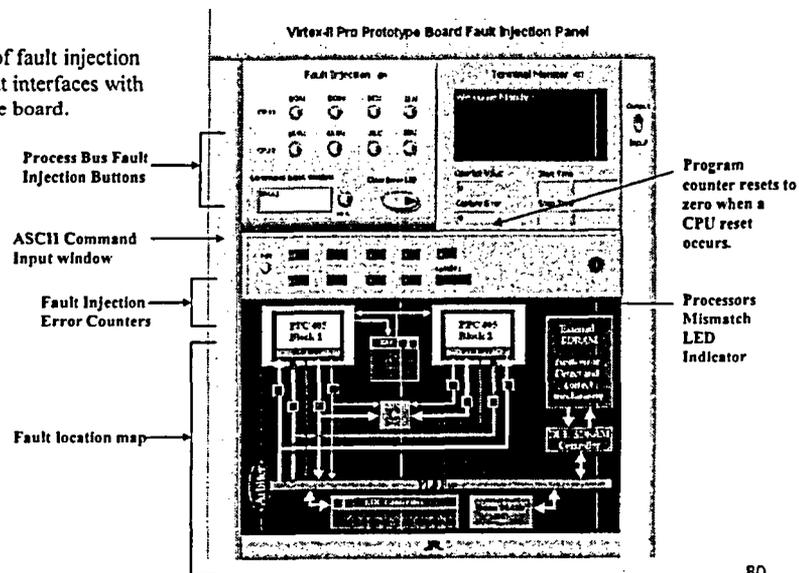


79



Preliminary Labview Fault Injection Panel

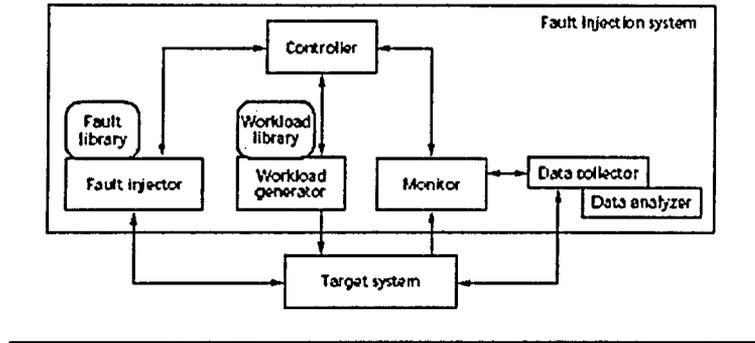
Screenshot of fault injection emulator that interfaces with the prototype board.



80



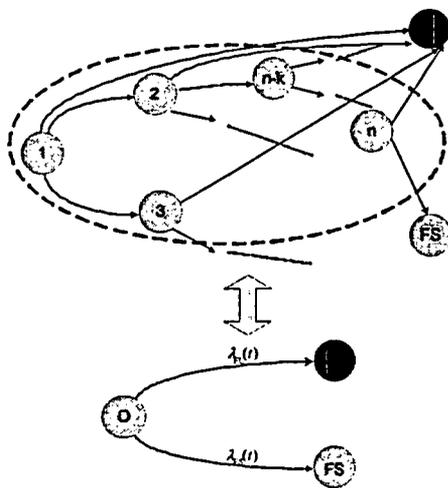
Typical Fault Injection Environment



81



Modular Markov Chain Construction



Lemma 5.2

$$\lambda_{FS}(t) = \frac{\sum_{x \in \left[\begin{array}{l} \text{a set of states which} \\ \text{have outgoing} \\ \text{transition to FS} \end{array} \right]} P_{A,x}(t) \cdot \lambda_{x,FS}}{\sum_{j=1}^n P_{A,j}(t)}$$

$$\lambda_{FU}(t) = \frac{\sum_{y \in \left[\begin{array}{l} \text{a set of states which} \\ \text{have outgoing} \\ \text{transition to FU} \end{array} \right]} P_{A,y}(t) \cdot \lambda_{y,FU}}{\sum_{j=1}^n P_{A,j}(t)}$$

= 82



Summary of Fault Injection Based Safety Assessment

- Compared to other SW/HW testing techniques:
 - Relatively Inexpensive.
 - Requires minimal information about the design of the HW/SW systems.
 - Makes minimal assumptions about the system operation.
 - Fault injection under complete control of the assessor.
 - Can Inject a fault at any location, for any duration of time at any time.
 - High stress testing of the SW/HW system.
- Operational profiles (system inputs) are under the control of the assessor.



Development of a Probabilistic Approach for Modeling Failures of Digital Systems Using Traditional PRA Methods

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

June 27, 2006

Todd Hilsmeier

Division of Risk Assessment and Special Projects
Office of Nuclear Regulatory Research
(301-415-6788, tah1@nrc.gov)

Tsong-Lun Chu

Brookhaven National Laboratory
(631-344-2389, chu@bnl.gov)

Gerardo Martinez-Guridi

Brookhaven National Laboratory
(631-344-7907, martinez@bnl.gov)



Presentation Outline

- Background
- Project plan
- Provide status of project
- Discuss development of a failure parameter database for quantifying probabilistic failure models of the hardware of digital systems
- Review of system failure events induced by software faults to identify failure modes and mechanisms/causes of software

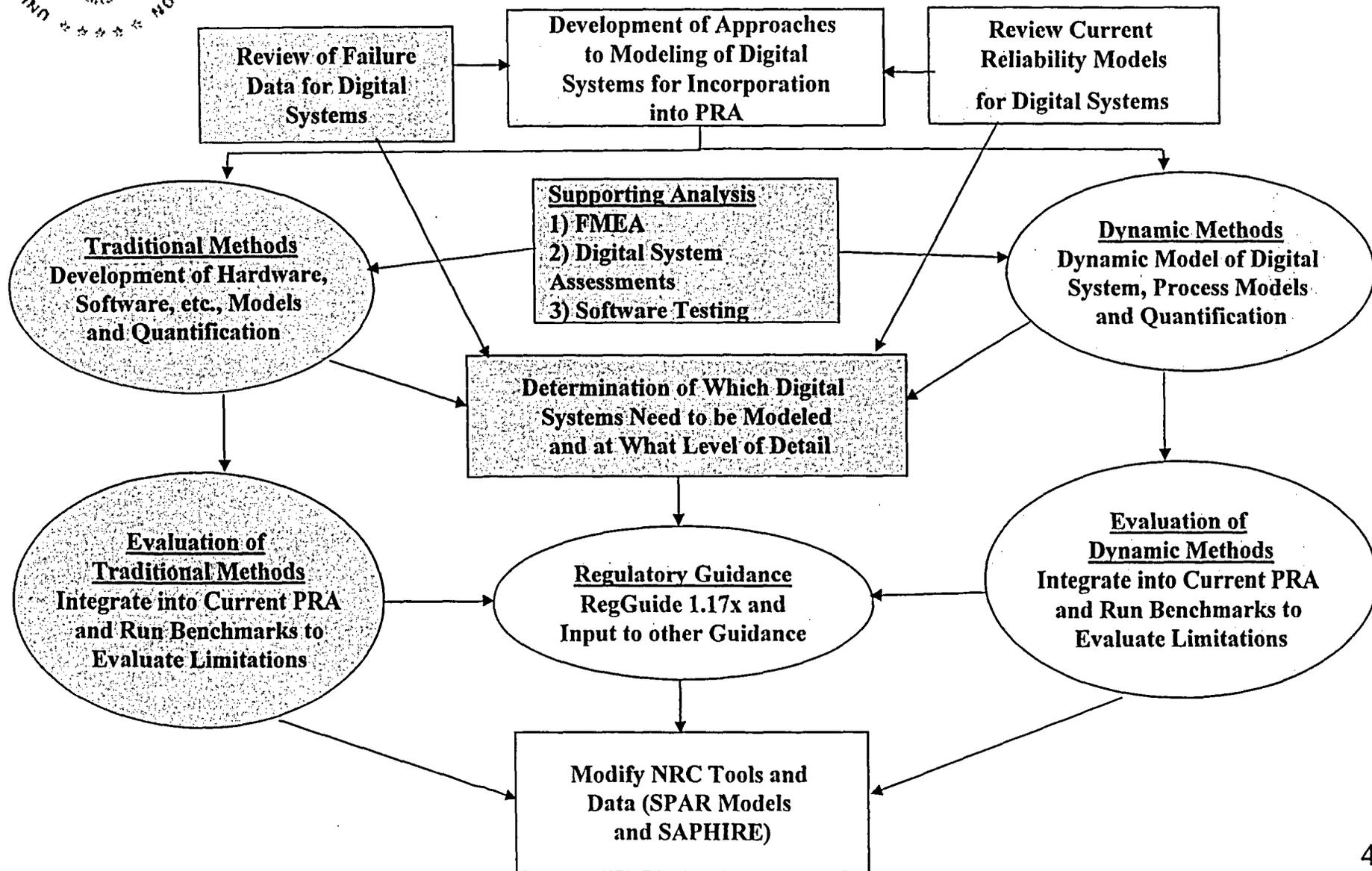


Background

- NRC has a comprehensive Digital System Research Plan that complements existing regulatory activities governing the safe and secure use of digital systems in U.S. nuclear facilities and applications
 - Includes probabilistic modeling of digital system failures using Traditional and Dynamic PRA methods that can be integrated with a PRA
 - The “Digital Systems PRA” project focuses on the use of Traditional PRA methods



NRC Digital System Risk Program





Objective of the “Digital Systems PRA” Project

- Develop a probabilistic method for modeling failures of digital systems using Traditional PRA methods (static fault trees and event trees) that can be integrated with a PRA, for those systems that do not require dynamic methods
- Provide input into Regulatory Guidance including needed modeling detail

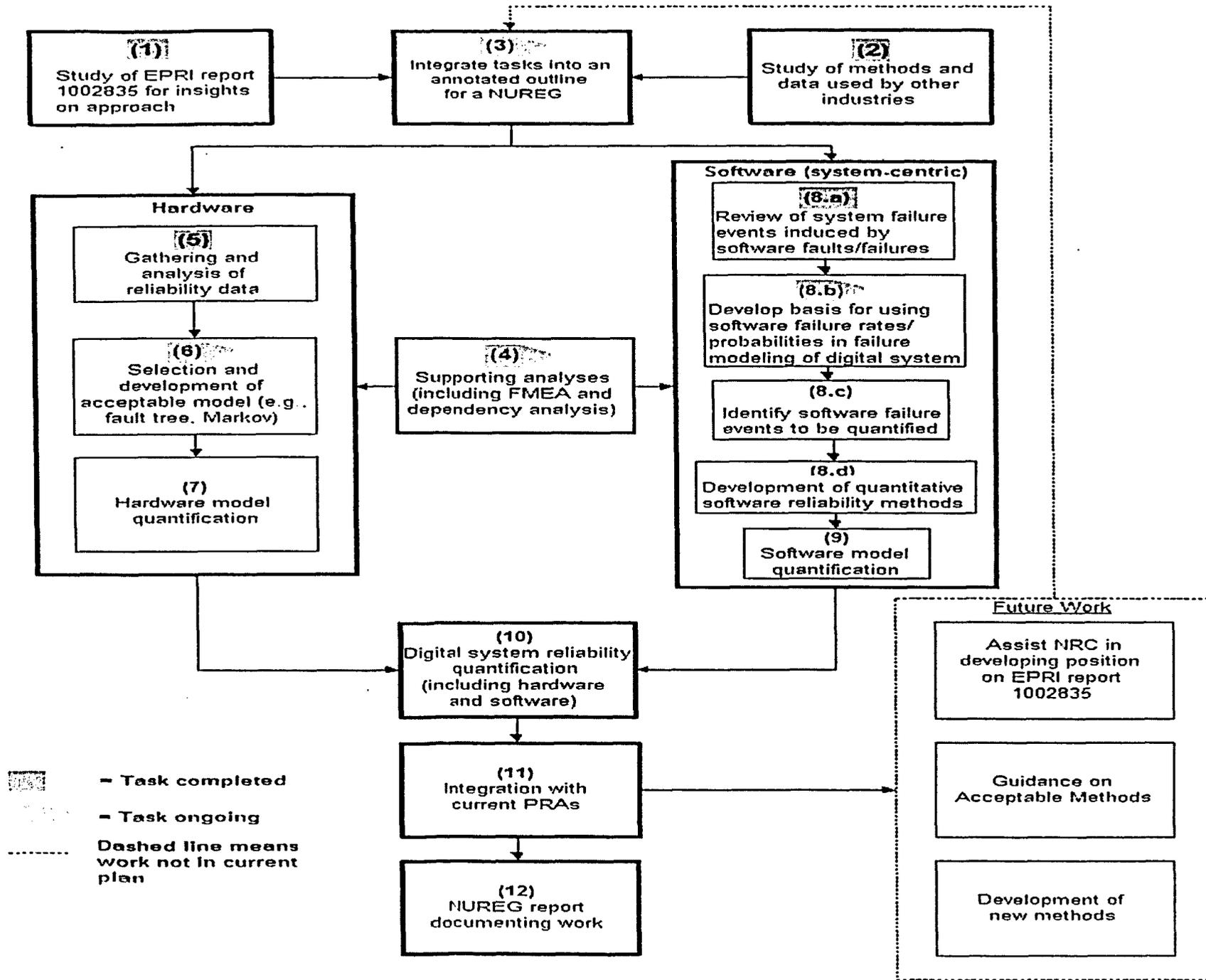


Figure 1
 Technical Tasks/Activities Associated with Digital Systems PRA Project

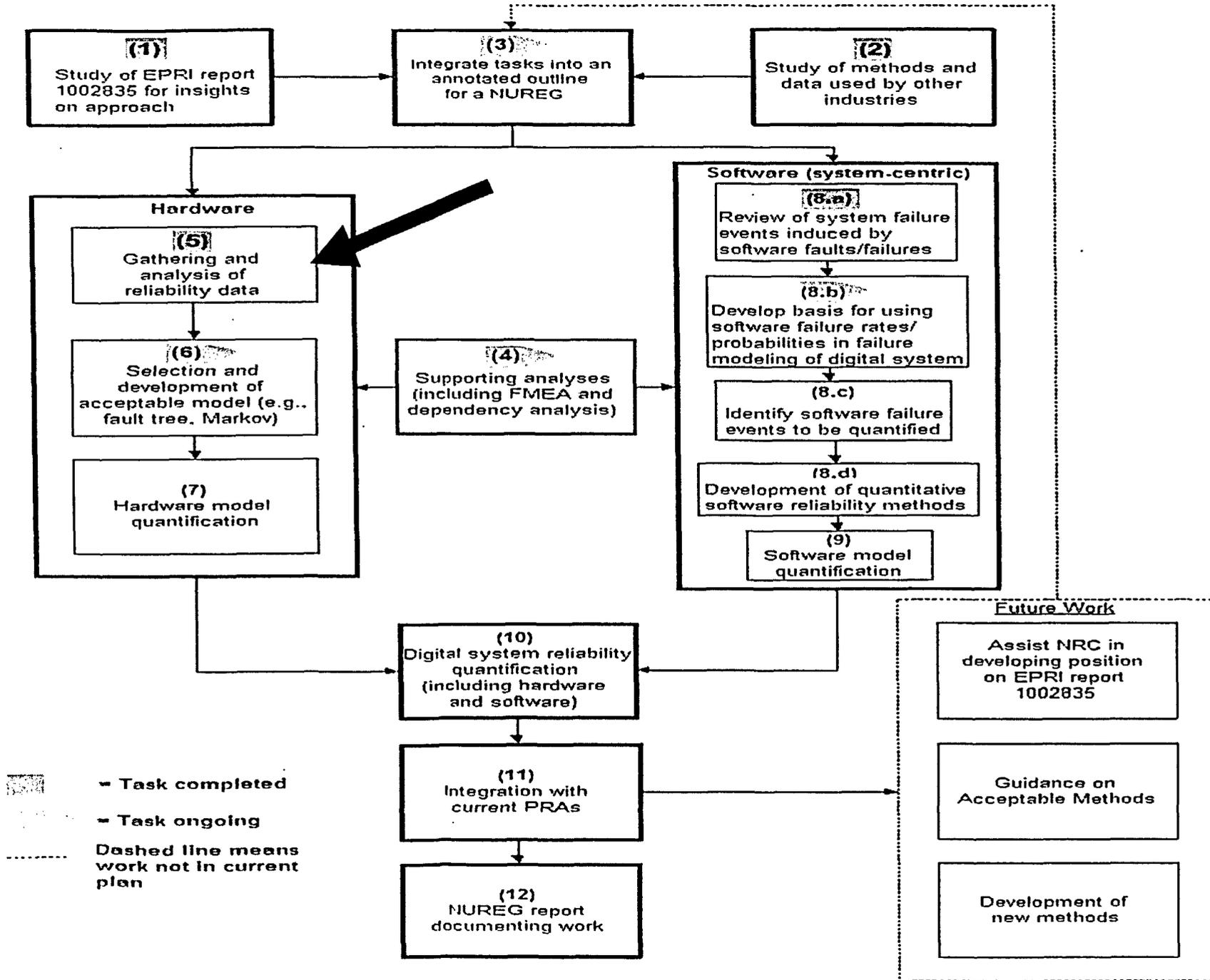


Figure 1
 Technical Tasks/Activities Associated with Digital Systems PRA Project



Development of a Failure Parameter Database for Quantifying Probabilistic Failure Models of the Hardware of Digital Systems (Task 5)

Objective:

Develop failure parameter database for digital hardware, based on currently available data, for quantifying digital system reliability models

Approach and Analysis:

Presented by Brookhaven National Laboratory

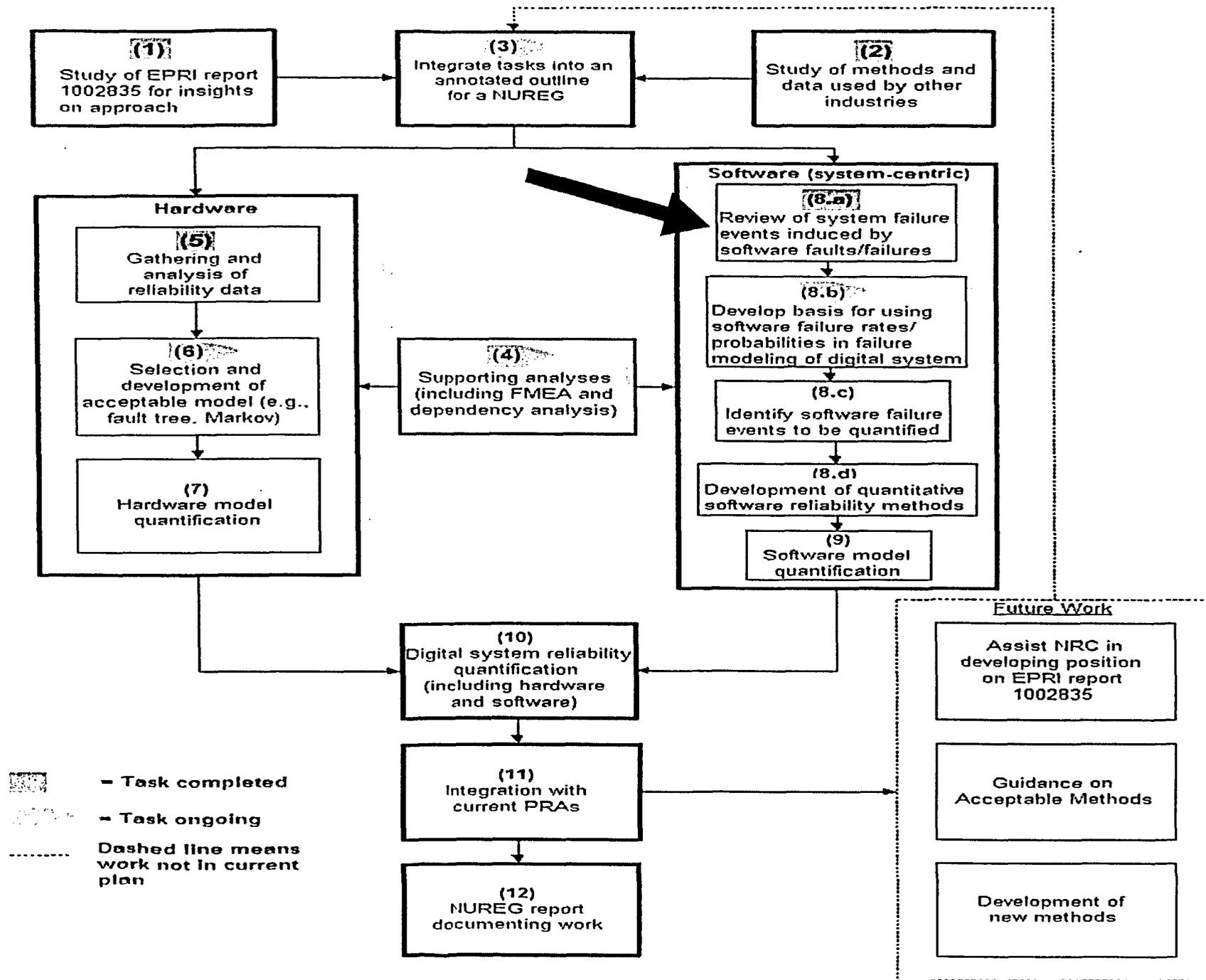


Figure 1
 Technical Tasks/Activities Associated with Digital Systems PRA Project



Review of System Failure Events Induced by Software Faults/Failures (Task 8.a)

Objective:

Review system failure events induced by software faults/failures to identify the failure modes, failure causes, occurrence frequencies, and the insights on modeling software failures in a PRA

Approach and Analysis:

A preliminary (draft) report has been completed by BNL and is currently undergoing NRC peer review

Evaluation of software-induced failure events (presented by BNL)

Development of a Failure Database for Digital System Hardware

**Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
Meeting**

Rockville, MD

June 27, 2006

T. L. Chu

(631 344-2389, Chu@BNL.GOV)

**Energy Sciences and Technology Department
Brookhaven National Laboratory**

Outline

- Objective
- Review of failure rate databases
- Hardware reliability prediction methods
- Hierarchical Bayesian method (HBM)
- Failure rate estimates using HBM
- Conclusions
- Proposed additional data collection

Objective

Development of a generic failure parameter database of digital components, based on currently available data, in support of developing reliability models, i.e., fault tree and Markov methods, of digital systems.

Approach

- Review of reliability methods and databases
- Hierarchical Bayesian analysis of raw data extracted out of PRISM
- Proposal on additional data collection

Review of Failure Rate Databases

- Existing nuclear databases (IEEE Std 500, SPAR, T-book, ZEBD) do not contain digital component failure rates.
- Some studies (AP600, Korean Standard Nuclear Power Plant) contain scattered failure rate estimates based on proprietary data.
- Hardware reliability prediction methods (Military Handbook 217, Telcordia, PRISM) are commonly used by defense, aerospace, and telecommunication industries.
- LER database and EPIX database contain failure events subject to limitation on reporting criteria, and limited information on total demands or time in service.
- SINTEF has a data handbook supporting Markov model of IEC 61508.

Hardware Reliability Prediction Methods

- Military Handbook 217, Telcordia SR-332, and software tool PRISM developed by Reliability Analysis Center (RAC).
- Attempting to capture many causes of variability explicitly is too ambitious.
- 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 good applicable failure data is available. Extrapolation could lead to significant errors.
- Lack of uncertainty consideration.

Population Variability Distributions of Digital Components Using PRISM Failure Records

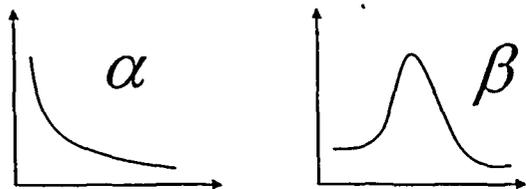
- PRISM is a software developed by the Reliability Analysis Center (RAC) for making reliability predictions of series systems, .e.g. circuit boards.
 - Failure records of components, e.g., microprocessors and RAMs, from different sources, i.e., warranty repair data, are in the form of “n failures in m hours”.
 - Large variations (see table) exist in data from different sources due to different specific designs, operating conditions, manufacturers etc.

Failure Data of A Digital Component

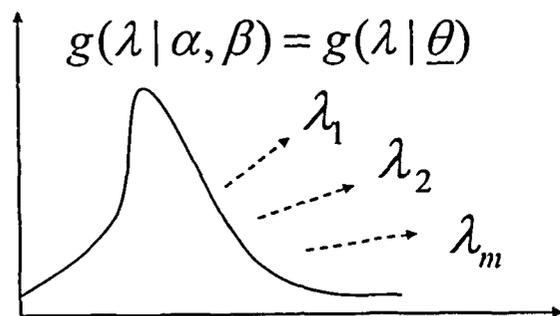
Quality	Environment	Number of Failures	Number of Hours (*1.0E6)	Point Estimate Failure Rate (per million hours)
Commercial	GB	12	633.8929	1.89e-02
Unknown	GB	0	0.2600	
Unknown	GB	0	0.0625	
Commercial	GB	16	2597.365	6.16e-03
Commercial	GM	4	701.1615	5.70e-03
Commercial	N/R	2	509.1335	3.93e-03
Commercial	GB	28	22751.18	1.23e-03
Commercial	GB	0	1105.13	
Unknown	GB	80	444.0000	1.80e-01
Unknown	GB	44	307.8874	1.43e-01
Unknown	GB	0	6.5937	
Commercial	GB	0	19.3613	
Commercial	GB	188	20069.9345	9.37e-03
Commercial	GM	1	692.6390	1.44e-03
Military	N/R	1	149.2384	6.70e-03
Military	AIF	0	0.0253	
Military	AIF	0	1.8755	
Military	AIF	0	11.3706	

Hierarchical Bayesian Method: A Illustration of Two-stage Analysis

Hyper-priors:



PVC:



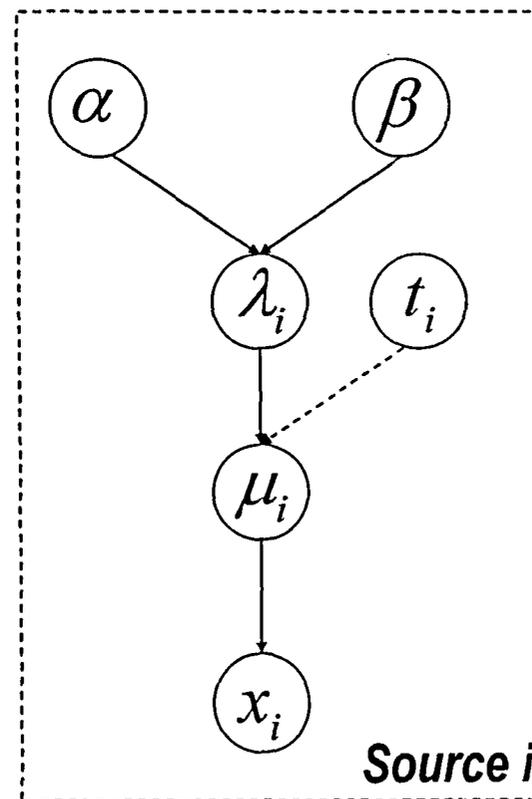
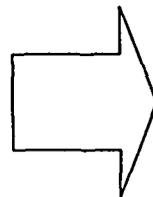
Source Specific Data:

Source 1: $(\lambda_1, t_1) \rightarrow X_1 \sim \text{Poisson}(\lambda_1, t_1)$

Source 2: $(\lambda_2, t_2) \rightarrow X_2 \sim \text{Poisson}(\lambda_2, t_2)$

...

Source m : $(\lambda_m, t_m) \rightarrow X_m \sim \text{Poisson}(\lambda_m, t_m)$



Hierarchical Bayes Analysis of PRISM Data

- 30 digital components were analyzed.
- WinBUGS software for solving hierarchical bayes models was used.
- Failure rates were assumed to be Lognormal, and Gamma distributions.
- The parameters of the distributions (hyperprior distributions) were assumed to be uniform, exponential, and normal distributed.
- Wide population variability distributions were obtained due to large variations in failure records.

Failure Rates of Gamma Distribution

- For Gamma distributed failure rates, the likelihood function
 - ✓ becomes the likelihood of a common incident rate model for large α and β
 - ✓ is improper and difficult to select hyper-priors to make the hyper-posterior proper
 - ✓ has no maximum and is asymptotically maximal along a ridge. Thus, a finite rectangle truncation of α and β can not be defined to contain most of the hyper-posterior mass, and different choices could significantly shift the region in which the population variation is localized
- Problems can be avoided using lognormal distribution

Failure Rates of Digital Components (1)

Component	Mean	5th	Median	95th	Error Factor
Buffer	0.39	1.0E-4	1.0E-2	0.80	88
Control	0.70	4.8E-5	6.6E-3	0.98	142
Counter/Divider	9.4E-2	7.8E-6	1.7E-3	0.17	147
Decoder	7.0E-2	9.2E-4	1.7E-2	0.24	16
Encoder	3.8	2.0E-4	4.0E-2	5.6	170
EPROM	2.4E-3	1.3E-5	2.9E-4	6.7E-3	23
Error Detection/Correction Gate	13	7.1E-4	0.11	21	173
Latch	4.96E-2	4.29E-4	8.9E-3	1.9E-1	21
Line Bus Driver	1.2E-2	1.6E-3	7.7E-3	3.6E-2	4.7
Line Bus Receiver	4.6E-1	3.4E-4	2.0E-2	1.02	55
Line Bus Receiver	6.2E-2	2.2E-3	2.2E-2	2.2E-1	10
Linear Amplifier	2.1E-2	2.6E-3	1.4E-2	6.0E-2	4.8
Linear Comparator	2.0E-1	8.1E-4	2.3E-2	5.8E-1	26.8
Linear Converter	3.9E-2	6.2E-4	9.4E-3	1.4E-1	15
Linear Multiplexer	4.3E-2	9.9E-4	1.4E-2	1.5E-1	12.3
Linear Operational Amplifier	1.1E-1	1.8E-4	3.8E-4	3.4E-1	43.5
Linear Timer	1.4E-1	5.3E-3	3.6E-2	4.4E-1	9.1
Linear Voltage Regulator	4.1E-02	1.8E-3	1.7E-2	1.4E-1	8.8

Failure Rates of Digital Components (2)

Component	Mean	5th	Median	95th	Error Factor
Micro Controller	5.5E-2	5.1E-5	3.7E-3	1.3E-1	50
Microprocessor	3.3E-2	4.6E-4	8.5E-3	1.2E-1	16
Multiplexer	3.3E-2	1.6E-4	4.0E-3	9.6E-2	25
Optoisolator	1.0E-2	4.2E-3	3.4E-2	3.2E-1	8.7
Processing Unit	3.3	1.3E-4	4.6E-2	15	339
PROM	2.6E-2	2.3E-3	1.3E-2	6.6E-2	5.3
RAM	0.33	8.8E-5	7.2E-3	0.51	76
Receiver-Transmitter	9.2E-2	7.8E-4	1.6E-2	0.34	21
Register	6.1E-2	4.0E-4	8.3E-3	1.9E-1	22
ROM	4.0E-2	6.0E-4	8.2E-3	0.11	14
UVEPROM	0.37	4.7E-3	8.6E-02	1.2	16
Tranceiver	3.5E-2	9.4E-4	1.1E-2	1.2E-1	11

Conclusions

- A process for estimating failure rates using raw data in a Hierarchical Bayesian analysis was developed.
- Population variability curves of many components are too wide due to large variability of limited raw data.
- Estimated failure rates in published studies are scattered and based on unknown proprietary data.
- Modeling using Gamma distribution should be reconsidered.
- Better data should be collected for future work.

Proposed Additional Data Collection

- The objective is to collect better data that are more applicable to I&C components used at nuclear power plants.
- Identify contacts at equipment manufacturers, e.g., Siemens, Westinghouse, GE, Triconex, MicroMac, and Fisher and Porter, and request failure data of digital components.
- Perform LER and EPIX search to identify digital component failures, and establish contacts at the plants to obtain information on the number of the same components in use and their operating hours.
- Evaluation of SINTEF data handbook for its use in Markov analysis.
- Cooperation with NASA on data collection and analysis.

A Review of Software-Induced Failure Events in Different Industries

**Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
Meeting**

Rockville, MD

June 27, 2006

T. L. Chu and G. Martinez-Guridi

(631 344-2389, Chu@BNL.GOV;

631 344-7907, Martinez@BNL.GOV)

**Energy Sciences and Technology Department
Brookhaven National Laboratory**

Outline

- Objective
- Approach
- A preliminary model of software failures
- Review of events at domestic nuclear power plants
- Review of events of other industries and foreign nuclear plants
- Categorization of software-induced failure events
- Description of selected events
- Discussion of ACRS comments
- Review of software reliability methods
- Conclusion

Objective

The objectives of this study are:

- to discuss software failures,
- present the approach used for collecting operational events related to these failures, and
- address ACRS comments in light of the insights gained during the review of these events.

Approach

- Search LER database for software-induced failure events at domestic nuclear power plants.
- Search for events in other industries.
- Develop a preliminary model of software failure.
- Analyze in detail selected software-induced failure events.
- Review literature of software FMEA and develop a categorization method of software failure events.
- Update earlier reviews of software reliability methods.
- Review ACRS comments.

A Preliminary Model of Software Failure

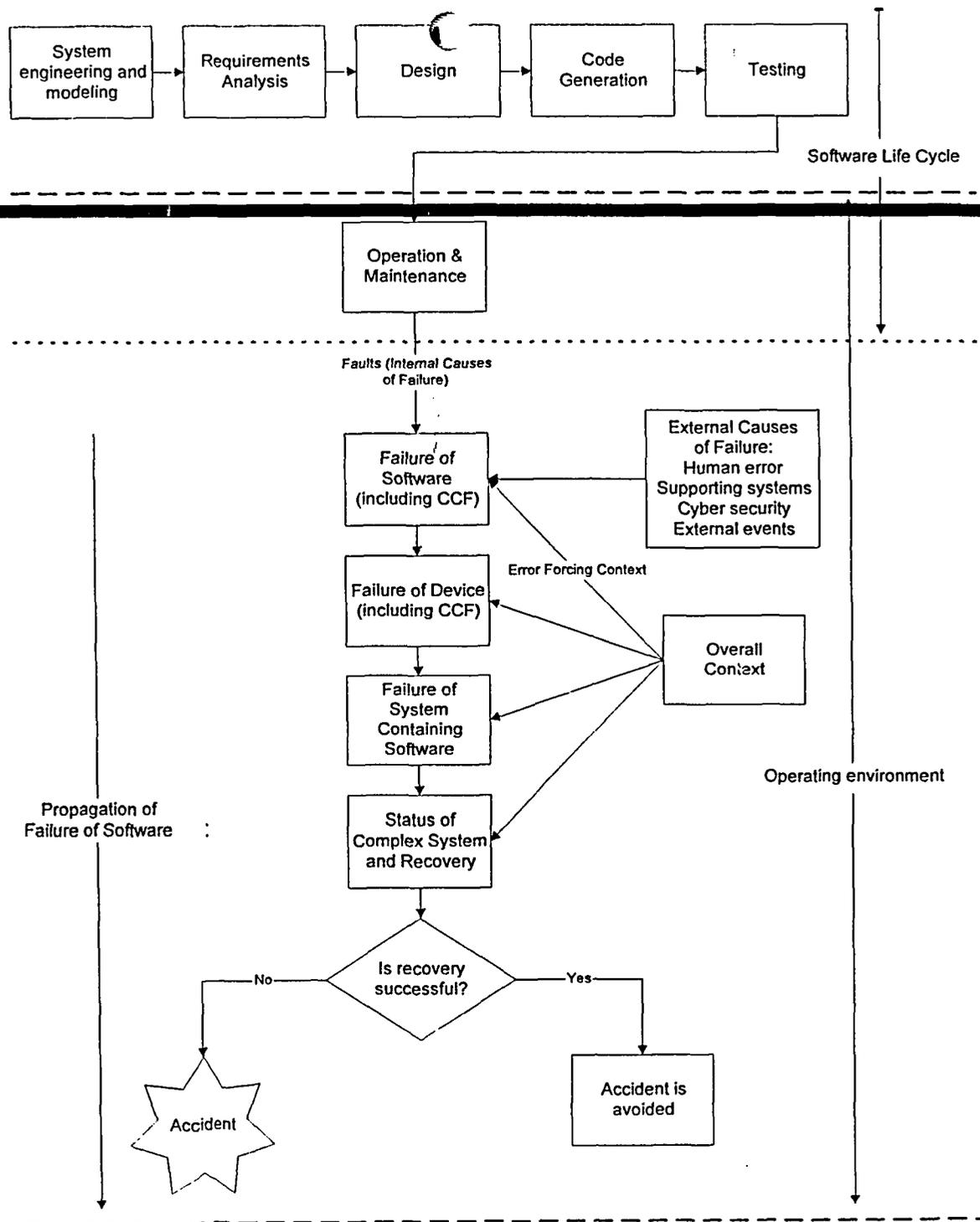
- A conceptual model of the causes of software failures, and the propagation of these failures in a complex engineered system
- The objectives are:
 - to gain a good understanding of the nature of software failures
 - To establish the basis for developing a probabilistic model of software failure (later task)
- Causes of software failures
 - Internal causes
 - External causes

Propagation of Software Failures

- In general, a software failure may be propagated to:
 - The device(s) controlled by the software (e.g., the flow control valves of the MFW),
 - The associated system
 - The overall plant
- Propagation depends on:
 - The overall context of the plant, and
 - The tolerance to failures of the design of the software, device(s), system, and the plant

Potential for Dependent Failures

- The redundant trains (or channels) of a system may use the same or similar software.
- The failure of the software means that the software in all trains fails, thus failing all trains.
- If this dependent or common-cause failure (CCF) occurs, it may cause a failure of:
 - All the device(s) controlled by the software (e.g., the flow control valves of the MFW)
 - The entire associated system



Review of Software Failures at Domestic Nuclear Power Plants

- Software failures in domestic NPPs were identified to gain insights into the nature of these failures in terms of such characteristics as:
 - The specific cause of failure of the software
 - The associated error-forcing context
 - Any dependent failures, such as common cause failures
- Identification of software failures by:
 - Using the Licensee Event Report (LER) Search System
 - 22 years were searched for software failures: from January 1, 1984 through December 31, 2005
 - All plants that operated during this period
 - All modes of operation of the plants
 - Searching for LERs containing the keyword “software” in the LER’s abstract and title
- The search was complemented with:
 - 6 additional events from Volume 2 of NUREG/CR-6734
 - We were aware of an additional event (LER 293-1997-007)

Database of Software Failures at Domestic Nuclear Power Plants

- Each LER obtained using this process was reviewed
- Those LERs documenting a software failure were selected for a database
- The current total number of LERs included in the database is 113
- Each LER is characterized in the database in terms of the following properties:
 - LER Number
 - Event Date
 - Specific nuclear unit(s) involved
 - Title of the event given by the LER
 - Description of the software failure
 - Cause(s) of the software failure
 - Consequences of the software failure
 - Error forcing context
 - Dependent failure

Insights of Review of Software Failures at Domestic NPPs

- 71 different nuclear units have at least one event related to software failure during the period studied.
 - Software failures have occurred in a significant number of units
 - This type of failure may occur in any of the operating units that use software-supported systems.
- 130 software failures in operating nuclear units are described in the 113 LERs that document software failures (i.e., 17 of the 113 LERs involved two nuclear units).

Insights of Review of Software Failures at Domestic NPPs (2)

- The 45 LERs that occurred during the last 10 years of the period stored in the database were analyzed to classify the “software failure mode” and the cause of the failure
- 31 out of the 45 events (i.e., about 69%) had the failure mode “Runs with wrong results that are not evident.”
 - This may be a reason for concern because it is undesirable to have software that is executing, sometimes for long periods of time, and producing incorrect results.
- The two main causes of failure are:
 - “Software requirements analysis” with 16 out of the 45 events (i.e., about 36%). In general, when software fails due to this cause, it fails to perform a function because when its requirements were specified, they did not include this function.
 - “Operation and maintenance” with 12 out of the 45 events (i.e., about 27%). Most of these events involve a failure introduced during modifications of the software after the software operated for some time.

Insights of Review of Software Failures at Domestic NPPs (3)

- In many cases, the EFC was identified for a particular LER.
 - In some cases a failure may occur as soon as the software becomes operational, and may remain hidden for a long time, i.e., several years. In these cases, the EFC is the normal operation of the plant.
 - The failure may be discovered by indirect means, such as discrepancies in the results produced by alternative calculations.
- In 29 of the events, i.e., about 26% of the 113 LERs, some type of dependent failure, including CCF, occurred.
 - An additional 13 LERs, i.e., about 12% of the 113 LERs, potentially involved dependent failures.
 - Hence, the potential of software failures to cause dependent failures, including CCF, is demonstrated.
 - Since a dependent failure can be significant to the risk of a NPP, a software failure has the potential to be a significant contributor to the risk.

Identification of Events of Other Industries and Foreign Nuclear Power Plants

- Internet search is the main method for identifying software-induced events.
 - “Computer Horror Stories” compiled by professor Nachum Dershowitz, School of Computer Science at Tel Aviv University,
 - “Collection of Software Bugs” compiled by professor Thomas Huckle, Institute of Information, Technical University, Munich,, Germany
 - Risks Digest compiled by Peter G. Neumann of SRI International Computer Science Laboratory
- NTSB Aviation Accident Database was reviewed.
- NASA website description of missions was reviewed.
- Other sources include news media, DOE and university websites.
- A Report written by PWR-1 Task Group on Computer-based Systems Important to Safety, NEA/CSNI/R(97)23, September 10, 1998 is the source of events at foreign nuclear plants.
- COMPSIS is developing guidelines and database structure on international operational experience.

Screening of Software-Induced Failure Events in Other Industries

- Most events were selected based on the severity of the consequences.
- Some events were selected because their failure modes (e.g., communication related failures) and causes (e.g., cyber security related events) are interesting.
- Some events were selected to cover specific industries, e.g., railway industry.
- A total of 48 events in 10 different industries were analyzed, i.e., medical service, electric power supply, commercial aviation, space, defense, telecommunication, financial service, water treatment, natural gas distribution, railway.

Categorization of Software-Induced Failure Events Based on Failure Modes and Causes

- In general, generic software failure modes are difficult to define because they depend on the level of detail at which the software is being evaluated and the specific application of the software.
- A literature review of software FMEA was performed to see how others have defined software failure modes.
- Often, failure causes, modes and effects are mixed up, probably they are used at different levels of detail.
- A categorization scheme of failure modes and causes was developed based on both the literature review and the review of software failure events.

Failure Modes of “Software System” and “Software Elements”

Software System Failure Modes (SFM)		Software Elements Failure Modes
M-I-1	SFM-1: Halt/abnormal termination with clear message	<i>Software Elements:</i> E-1: INPUT E-2: OUTPUT E-3: COMMUNICATION E-4: RESOURCE ALLOCATION E-5: PROCESSING <i>Generic Failure Modes of Software Elements:</i> <ol style="list-style-type: none"> 1. Timing/order failure, 2. Interrupt induced failure, 3. Omission of a required function or attribute, 4. Unintended function or attribute in addition to intended functions and attributes, 5. Incorrect implementation of a function or attribute, 6. Data error which cannot be identified and rejected by software logic
	SFM-2: Halt/abnormal termination without clear message	
M-I-2	SFM-3: Runs with evidently wrong results	
	SFM-4: Runs with wrong results that are not evident	
M-II	SFM-5: Problematic, confusing, or less informative interface	

Examples of Software Element Specific Failure Modes

- INPUT - Failure to interact with I/O board, excessive demand on I/O devices.
- OUTPUT- Failure to interact with I/O board, excessive demand on I/O devices, faulty message, checkpoint file failure, e.g., a file that describes status of hardware checked by operating system during the computer reboot.
- COMMUNICATION - Failed interaction (in subroutine calls, data communications) between processes, failed synchronization, dead lock (two processes prevent each other communicating)
- RESOURCE ALLOCATION - Failure to interact with CPU resources, competing for resource, priority error, resource conflict; internal capability exceeded, dead lock (two processes prevent each other obtaining resource), lockout (a process is never able to acquire the resource).

Software Failure Causes

- Software failure causes are defined in terms of errors committed during software lifecycle stages or external causes such as cyber security related, incorrect human input, support system failures, and environmental problems.
- The failure causes of the events may potentially be used to support developing quantitative software reliability methods.

Classification of Software Failure Causes

- C-I System engineering and modeling
- C-II Software requirement analysis
- C-III Software analysis and design
- C-IV Code generation
- C-V Testing
- C-VI Operation and maintenance
- C-VII External causes

Insights of Review of Software-induced Failures in Other Industries

- Software failures occur in every industry.
- Incorrect implementation and omission of functions or attributes are important failure modes.
- Errors during software requirement analysis stage are the most important failure causes.
- The occurrence of error forcing context triggering a software failure is a reasonable way of considering software failures
- Software failures may occur at a very low level which requires low level-of-detail modeling to account for their occurrence.
- Some software failures involve software that are not application software, e.g., hardware diagnostics, operating systems, and communication software.
- Software CCFs do occur.
- Man-machine interface is a contributor to some events.

Turkey Point Diesel Generator Sequencer 1994

- During a test in Unit 4, the 3A HHSI pump failed to start due to a failure in the software of the 3A sequencer. The software logic defect is limited to the test function, but the defect is common to all four sequencers.
- There was another error in the software that would preclude the automatic start of the CS pumps. The condition identified occurs when the High-High Containment Pressure (HHCP) signal is received by the sequencer during an approximate 60 millisecond (ms) time window just prior to the end of sequencer load block 3 for LOCA or LOOP coincident with LOCA events.
- System failure mode: Runs with wrong results that may not be evident.
- Element failure mode: One of the elements of the software (possibly, the processing element) incorrectly implemented some functions of the sequencer.
- Internal causes:
 - The software error causing failure of a sequencer to respond to an SI signal was introduced during the stage "System analysis and design" of the software development.
 - The cause of the error in the sequencer software that would preclude the automatic start of the CS pumps was not found in the LER. Possibly, it is the same cause.
- EFC:
 - Regarding failure of a sequencer to respond to an SI signal, in general, the EFC is the sequencer executing some tests.
 - Regarding failure of a sequencer to automatically start the CS pumps, the EFC is a HHCP signal received by the sequencer during an approximate 60 ms time window just prior to the end of sequencer load block 3 for LOCA or LOOP/LOCA events.
- Consequences:
 - The periodic inoperability of all four sequencers has existed since the sequencers were installed in 1990/1991. Since the sequencers would not have responded properly to an SI signal as designed, Units 3 and 4 were operating outside their design basis.
 - The LER considered the failure of the automatic start of the Containment Spray (CS) pumps to be not significant to safety.

Common Cause Failure of Vital 120 volt AC Buses at Pilgrim - 1997

- Pilgrim was in cold shut down. During a severe storm, the safety-related 120 volt AC buses 'A' and 'B' de-energized on two occasions.
- The cause of the de-energizing of these buses was the automatic shut downs of voltage regulating transformers X55 and X56.
- The 345 Kv system experienced brief but severe voltage transients.
- The voltage on the 480 volt load center was as low as 350 volts.
- Regulating transformers were designed to regulate input voltages of 480 volts 20 percent (384 - 576 volts).
- Each regulating transformer contains a microprocessor (MCU).
- The software contained in an MCU automatically shut down its regulating transformer if input voltage was outside the range of 384 to 576 volts.
- System failure mode: Runs with evidently wrong results.
- Element failure mode: One of the elements of the software (possibly, the processing element) of an MCU has the unintended function of shutting down the regulating transformer when the input voltage is less than 384 volts (greater than zero volts).
- Internal cause: Inadequate requirements of the software, in particular, unspecified exception conditions.
- EFC: An event, such as the severe storm, that could cause the 480 volt load center to be below 384 volts.
- Consequence: The undervoltage shut downs of the regulating transformers was outside the Pilgrim Station design basis.

Core Protection Calculators Inoperable at Palo Verde 2 - 2005

- The Core Protection Calculators (CPCs) consist of four software-supported redundant channels. The CPC system provides two trip signals to the RPS.
- When both analog input modules within a CPC channel indicate an error simultaneously, the CPC uses the last known good value. However, a channel trip should be initiated for this event. Software release 6.1 resulted in the CPCs not being able to generate this trip signal.
- System failure mode: Runs with potentially wrong results that are not evident.
- Element failure mode: There was an omission of the function that should generate the channel trip signal. One of the elements of the software (possibly, the processing element) was missing this function.
- Internal causes: The LER states that investigation into the cause of this event is ongoing, and that preliminary results indicate the direct cause is that a CPC system requirement specification was not properly translated into the CPC software by the vendor. Accordingly, it appears that the error was introduced during the development of the software, possibly during the stage of "System analysis and design."
- EFC: The simultaneous failure of both analog input modules within a CPC channel. Possibly, the EFC also includes failures of the analog sensors providing input to both analog input modules within a CPC channel.
- Consequences: All four channels of the CPCs were inoperable, and the plant operation violated Technical Specifications since the software was installed. In addition, the plant had to be shutdown from approximately 100% power.

Refueling Accident at Unit 4 of Ontario Hydro's Bruce plant 1998

- The CANDU reactors perform fueling operation while the reactor is online. A fueling machine which is moved by a bridge must lock onto each end of the fuel channel and be pressurized. The end plugs of the channel are then removed and new fuel is pushed in from one end and spent fuel is pushed out of the other end. A fueling machine can be positioned at the bridges of any reactor and be controlled by a computer system.
- A computer system which was used to control a fueling machine which is clamped to one end of a fuel channel had a previous error. The error handling routine had a fault (introduced in a software revision) which caused the return address be incorrectly set to the routine which would release the brakes on the bridge.
- When an operator trying to use the computer system to control a different bridge triggered an error which caused the software to remember the previous event and called for release of the brakes. The fueling machine moved down 40 cm and caused damage to the fuel channel fitting and a loss of D2O.
- A protective computer which would have prevented the accident was not in service.
- Software failure categorization
 - System failure mode: Software runs with wrong results that are evident
 - Element failure mode: Incorrect interrupt return
 - Failure causes: Coding error, inadequate testing subsequent to a software revision
 - A small loss of coolant accident

Discussion of ACRS Comments

- We developed a preliminary model of software failure which depicts how software failures occur, and how these failures may propagate into accidents.
- We reviewed software-induced failures in different industries, and developed a way of categorizing the events based on their failure modes and causes.
- Software failures occur because there are faults in the software and triggering events/EFC activate the faults. The occurrence of triggering events is random and can be modeled probabilistically.
- The frequency that a software failure occurs is the same as the frequency that the EFC occurs. Constant failure rate is a reasonable assumption for software failures as long as the operating conditions do not change.
- Identification of EFC is difficult.

On “System-Centric” vs “Software-Centric” Viewpoints

- The “system-centric” view point includes the interactions of the software with the rest of the plant. Conceptually, it is possible to identify the EFCs.
- Viewing software failure as a property of the software itself is incorrect. The issue is that it appears that the “software-centric” view point would only analyze the software in “isolation”. In this sense, we agree that such narrow analysis of software would fail to discover many relevant EFCs.
- Consideration of the operating environments and operational modes is an important part of the development lifecycle of a software.
- The “system-centric” view point considers and models the world around the software, while the “software-centric” view point considers the operating environments as boundary conditions of the software.
- There is no contradiction between the two viewpoints. They have different emphases.

Review of Methods on Software Reliability

- Two types of methods were reviewed, methods for identifying software faults, and methods for quantitative reliability modeling of software.
- Methods for identifying software faults – hazard analysis, FMEA, testing, formal methods, DFM.
- Methods for quantifying software reliability-reliability prediction methods, Markov model and Petri net, fault tree analysis, Bayesian belief network, reliability growth models, IEC 61508.
- A more critical review will be done in our next task.

Methods for Identifying Software Faults

- **Formal methods**

- Formal methods are mathematically based languages, techniques, and tools for specifying and verifying design requirements of hardware and software systems.
- The process of specification using these methods is the act of writing requirements down precisely. It allows a developer to gain a deeper understanding of the system specified and to discover design flaws, inconsistencies, ambiguities, and incompleteness.
- An example is the application to Traffic Collision Avoidance System II [Heimdah and Leveson 1996].
- Formal techniques such as model checking and theorem proving are also used for verification of hardware and protocols, instead of simulation models.
- Application of formal methods recognizes 1) the original requirements are usually specified in a natural language, and may be incorrect or incomplete; 2) the translation into a formal language may introduce errors; and 3) the formal model of software requirements is not the same as the source code which may contain additional faults.

Methods for Quantitative Reliability Modeling of Software

- **Bayesian Belief Networks (BBN)** are complex diagrams that organize the body of knowledge in any given area by mapping out cause-and-effect relationships among key variables and encoding them with distributions that represent the extent to which one variable is likely to affect another. Tables of conditional probabilities are used to represent the influence relationships of the nodes. Bayes' rule is used as the mechanism for updating probabilities given that additional evidence is obtained.
- Recently, BBN has been used in making prediction about software defects, determining the number of tests needed to achieve a given dependability, and assessing probability of system failure. We consider that it is possible to build a software reliability prediction model based on BBN.
- The basic idea is to set the characteristics/metrics of a software as one of the nodes, and the other nodes are factors influencing or determining the metrics. The metrics are dependent on factors that cannot be measured directly, such as the quality of the process used in its development. Expert judgment, based on observations of these factors of software, and other information such as failure data can be used to estimate the probabilities of these nodes.

Conclusions (1)

- Software failures occur in many different ways. Experience of other industries is in general applicable to the nuclear industry.
- There is no contradiction between software-centric and system-centric viewpoints. They have different emphases.
- Some failures took place in such a way that implies very detailed modeling would be required.
- Some failures involve non-application software, e.g., operating system, hardware diagnostics, and communication software. This has implication on the scope of any software analyses.
- It is reasonable to model software failures in terms of their frequencies, because the occurrence of the failure triggering events is random.
- It is possible to estimate the frequency of past software-induced accidents. The frequency represents that of historical events, and may not be useful in predicting future events.

Conclusions (2)

- Different methods can be used to identify software faults. They have different advantages and limitations. It appears that no single method is able to find all faults in a software.
- Formal methods are designed to support requirement specifications. These are promising methods deserving exploration.
- No commonly accepted method for quantitative software reliability exists.
- For safety-critical software systems, e.g., RPS, subjective judgment of experts is probably the only way to model software failures, given the current state of the art. BBN is one of such methods and its use will be further explored.



DEVELOPMENT OF REGULATORY GUIDANCE FOR RISK-INFORMING DIGITAL SYSTEM RISK REVIEW

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 27, 2006

Steven A. Arndt
Instrumentation and Electrical Engineering Branch
Division of Fuel, Engineering & Radiological Research
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)



OVERVIEW

- As part of the overall Digital System Risk Research Program the NRC will develop needed regulatory guidance to support risk-informing digital system reviews
- To develop this guidance the NRC is working to
 - Understand the status of failure data
 - Assess which modeling methods might be usable
 - Determine which systems need to be modeled and at what level of detail
 - Develop acceptable methods
 - Develop regulatory acceptance criteria



CURRENT SITUATION

- Licensees are replacing analog systems with digital systems
- Industry has expressed interest in using risk-informed regulation (Regulatory Guide 1.174) as an alternate method for licensing these systems
- As the NRC licensees replace analog systems with digital systems, the current PRA's are not keeping up with these changes
- An NRC program to develop risk analysis tools and data is providing input into what models and methods are needed



NEED FOR GUIDANCE

- Regulatory Guide 1.174 provides guidance for risk-informed decision-making, but does not provide specific criteria for digital systems
- Because of the unique characteristics of digital systems, additional guidance needs to be provided associated with
 - Digital system modeling
 - Maintaining sufficient safety margin
 - Meeting current regulations and defense-in-depth philosophy
 - Performance measurement strategies



STRATEGY FOR DEVELOPMENT

- Develop an understanding of the characteristics of digital systems that need to be modeled (NUREG/CR-6901 and other work)
- Identify methodologies for modeling digital systems and incorporating these models into existing PRA's
- Develop an understanding of the data issues associated with digital system reliability modeling
- Develop draft regulatory guidance (DG-1151 "An Approach for Plant-Specific, Risk-Informed decision making for digital systems)
- Conduct public meetings to discuss proposed regulatory guidance (August 2006)
- Publish for comment draft regulatory guidance (December 2006)



OVERALL STRUCTURE FOR DG-1151 “AN APPROACH FOR PLANT-SPECIFIC, RISK-INFORMED DECISION MAKING FOR DIGITAL SYSTEMS”

- Modeling requirements
- Integration of digital system models with full PRA models
- Data requirements
- Uncertainty analysis
 - Model uncertainty
 - Operational profile uncertainty
 - Data uncertainty
 - Operational history
 - Testing
- Acceptance criteria
- Meeting current regulations and defense-in-depth philosophy
- Maintaining sufficient safety margin
- Performance measurement strategies



MODELING REQUIREMENTS

- The model must account for the important relevant features of the system under consideration.
- The model must make valid and plausible assumptions about system characteristics and justify these assumptions.
- The model must quantitatively be able to represent dependencies between failure events accurately, including support systems failures, common mode failures, and dynamic interactions associated with the process and digital systems, or demonstrate that they are not important
- The model must be able to differentiate between faults that cause function failures and intermittent failures; and differentiate between a state that fails one safety feature and those that fail multiple features or demonstrate that there is no important significance to the differences.
- The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results.
- 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.



LEVEL OF MODELING DETAIL

- Needs to be adequate to capture all of the unique aspects of digital systems:
 - Discrete time aspects of digital systems
 - Complex interactions between the components of the digital I&C system and between the digital I&C system and process physics which may lead to potentially significant dependencies
 - Unique failure modes of digital I&C systems
 - Digital systems environmental failure modes
 - Interaction between hardware and software that may lead to failures, including internal and external communication
 - Digital I&C systems shared data transmissions, functions, and process that may lead to common cause failure (CCF).
 - Unique characteristics of software failures and testing
 - Digital system non-continuous behavior



LEVEL OF MODELING DETAIL (CONT.)

- If simplified models are used
 - Validate that unique aspects are not important to the particular system or application
 - Validate that the data used in the simplified model captures the important aspects of the failure modes
 - Validate that common mode failures can be accounted for
 - Validate that events that have happened, can be adequately modeled at that level of modeling abstraction
- Examples will be included in DG-1151



INTEGRATION OF DIGITAL SYSTEMS MODEL WITH PRA'S

- Integration of digital system models with full PRA models
 - Needs to include all important interactions and dependencies
 - Needs to include all systems that will impact/will be impacted by the digital system changes



DATA REQUIREMENTS

- Data requirements
 - Generic Operational Data
 - LER and other nuclear data
 - Generic databases (RAC, etc.)
 - Plant/System Specific
 - Testing-Based Data
 - Needs to demonstrate applicability to delivered product
 - Needs to quantify coverage
- Data issues
 - Data collection needs to be done systematically and in a structured manner
 - Configuration control based on measures and metrics used
 - Detailed Root Cause Analysis



UNCERTAINTY ANALYSIS

- Uncertainty analysis
 - Model uncertainty
 - Operational profile uncertainty
 - Knowledge of possible input states and probability distributions
 - Data uncertainty
 - Operational history
 - Testing



ADDITIONAL REQUIREMENTS

- Acceptance criteria
 - RG-1.174
 - Additional guidance on acceptable uncertainty
- Meeting current regulations and defense-in-depth philosophy
 - 10CFR50.55a(h).
- Maintaining sufficient safety margin
- Performance measurement strategies
 - Validation of data used
 - Monitoring of industry wide events to assure assumptions continue to be valid



SUMMARY

- This research into current state of data, analysis methods, and acceptance criteria will support the development of regulatory guidance for risk-informing digital system reviews
- Broad-based program that will look at a number of potentially viable methods for developing acceptable digital system risk models
- Assess the capabilities and limitations of the state-of-the-art and develop appropriate regulatory requirements
- Regulatory guidance will be performance-based₄