

Official Transcript of Proceedings ACRST-3272

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Plant Operations Subcommittee

Docket Number: (not applicable)

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005

Location: Rockville, Maryland

Date: Friday, March 26, 2004

Work Order No.: NRC-1387

Pages 1-299

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

~~ACRS OFFICE COPY~~
RETURN FOR THE LIFE OF THE COMMITTEE

TROY

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

+ + + + +

PLANT OPERATIONS SUBCOMMITTEE MEETING

DIGITAL INSTRUMENTATION AND CONTROL

+ + + + +

FRIDAY,

MARCH 26, 2004

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The subcommittee met at the Nuclear
Regulatory Commission, Two White Flint North,
Room T2B3, 11545 Rockville Pike, at 8:30 a.m., John D.
Sieber, Chairman, presiding.

COMMITTEE MEMBERS:

JOHN D. SIEBER, Chairman

GEORGE E. APOSTOLAKIS, Member

MARIO V. BONACA, Member

F. PETER FORD, Member

THOMAS S. KRESS, Member

STEPHEN L. ROSEN, Member

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

1 ALSO PRESENT:

2 SERGIO B. GUARRO, Consultant

3 MARVIN D. SYKES, Cognizant Staff Engineer

4 JAMES D. WHITE, Consultant

5

6 NRC STAFF:

7 STEVEN ARNDT, RES

8 MICHELE EVANS, RES

9 TEKIA GUN, RES

10 JIAN HONG, NRR EEIB

11 DEAN OVERLAND, RES

12 ROMAN SHAFFER, RES

13 DOUG TIFFT, RES

14 MIKE WATERMAN, NRR

15 PETER R. WILSON, RES

16

17

18

19

20

21

22

23

24

25

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

I-N-D-E-X

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

AGENDA ITEM

PAGE

| | |
|--------------------------------------|-----|
| Opening Remarks | 4 |
| Overview of Digital I&C Research | 5 |
| Program, State-of-the-Art in Digital | |
| System Reliability Modeling and PRA | |
| Modeling Program | |
| Digital Systems Modeling Using Fault | 112 |
| Injection Methods | |
| Software Reliability Modeling | |
| Staff Plans for Digital Reliability | |
| Models | |
| General Discussion and Adjourn | |

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

(8:30 a.m.)

CHAIRMAN SIEBER: The meeting will now come to order. This is a joint meeting of the Plant Operations and Reliability and PRA Subcommittees.

I'm Jack Sieber, Chairman of the Plant Operations Subcommittee. And with us also is George Apostolakis, who is Chairman of the Reliability and PRA Subcommittee.

ACRS members in attendance are Mario Bonaca, Stephen Rosen, Tom Kress, and Peter Ford. And we also have two of our consultants present, Sergio Guarro and Jim White. Marvin Sykes of the ACRS staff is the Designated Federal Official for this meeting.

The purpose of this meeting is to discuss digital instrumentation and control research activities, including the development of digital system reliability models. We will hear presentations from representatives of the Office of Nuclear Regulatory Research, the University of Virginia, and the University of Maryland.

The subcommittees will gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full committee.

NEAL R. GROSS

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

1 The rules for participation in today's
2 meeting have been announced as part of the notice of
3 this meeting previously published in the Federal
4 Register on March 8, 2004.

5 A transcript of the meeting is being kept
6 and will be made available as stated in the Federal
7 Register notice. Therefore, we request that speakers
8 identify themselves and speak -- move to a microphone
9 and speak directly into the microphone with sufficient
10 clarity and volume so that they may be readily heard.

11 We have received no written comments or
12 requests for time to make oral statements from members
13 of the public regarding today's meeting.

14 We will now proceed with the meeting, and
15 I call on Steve Arndt of the Office of Nuclear
16 Regulatory Research to begin. Steve?

17 MR. ARNDT: Thank you. I'd like to
18 introduce my Division Director. He may have a couple
19 of introductory remarks.

20 MR. MAYFIELD: Good morning. I'm Mike
21 Mayfield, Director of the Division of Engineering
22 Technology, and this work is sponsored out of my
23 division. We want to thank the committee --
24 subcommittees for the opportunity to come and discuss
25 this. We have tried unsuccessfully a couple of times

NEAL R. GROSS

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

1 to schedule onto your calendar, and events kept
2 overtaking us, so we appreciate the opportunity to
3 come brief you on this important work.

4 We think we've put together a pretty
5 comprehensive story to present to you today, and we
6 look forward to feedback and the opportunity to
7 interact with the committee.

8 With that, Steve?

9 CHAIRMAN SIEBER: Thank you.

10 MR. ARNDT: Thank you. We've put together
11 a pretty aggressive schedule. You have in front of
12 you -- but I just want to highlight what we're going
13 to try and accomplish today.

14 The first presentation, which I will give,
15 is an overview of the research program, a discussion
16 of the state of the art -- actually, the state of the
17 practice is probably better terminology -- in this
18 area, and review of several of our research programs.

19 Following that, the University of Virginia
20 and the University of Maryland will highlight two of
21 our larger programs specifically. I will then come
22 back to the microphone to discuss future plans in the
23 area, and then we'll have the adjournment.

24 So the idea basically is to give you a
25 comprehensive overview of the program, highlighting

NEAL R. GROSS

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

1 the two particular programs that the committee has
2 been interested in in recent years.

3 As I mentioned, the overview will give you
4 a context of where this -- of where the reliability
5 program fits into the overall I&C program, and also
6 discuss some of the issues we have with the particular
7 state of the art in this area.

8 As requested by the committee, we will
9 have conclusions, review of the I&C program, boundary
10 conditions and drivers, why are we going down this
11 particular path at this particular time, review of
12 digital system reliability modeling, current methods,
13 and then discussion of the research programs.

14 Our research program is designed to answer
15 the questions that we think we're going to get as an
16 agency in digital system risk assessment. The
17 drivers, as I will discuss later, have to do with
18 getting ready for the reviews that the licensees are
19 likely to submit.

20 So as much as we'd like to do exotic, fun
21 research, we also have to temper that with, do we have
22 enough information of the methods that are most likely
23 going to be submitted to be able to make reasonable
24 judgments.

25 Research includes model development, data

1 collection and analysis, and guidance development.
2 What we're trying to do is put together a tool package
3 for our licensing brethren, so that they can do their
4 jobs more efficiently and realistically.

5 We're working on development tools not
6 only to understand the methodology but also to assess
7 the methodology as a check tool. And some of those
8 are in the demonstration phase right now, and we're
9 trying to work with both our contractors and other
10 researchers in the area to stay abreast of the state
11 of the art.

12 The particular issues are to develop the
13 kinds of guidance we need. We need to be able to
14 assess whether or not there is enough information and
15 enough experience in the application of these methods
16 in the domain we're interested in to make some
17 judgments.

18 We currently think that the models are
19 sufficiently mature to do that. Now, are they great?
20 Maybe not. But the threshold here is, are they mature
21 enough that we can make judgments as to whether or not
22 they are sufficient for the application they're going
23 to be looking at?

24 We have ongoing future work -- we'll talk
25 about that later in the day -- associated with

NEAL R. GROSS

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

1 integration into PRA models and audit calculations,
2 and things like that. There are a lot of different
3 issues that we continue to have and we continue to
4 work to, especially including the data issues and the
5 coordination with our international colleagues. So
6 that's one of the issues that we continue to strive to
7 improve on.

8 The next few slides are going to be an
9 overview of the I&C research program as a whole to
10 give you a context of where the reliability program
11 fits. As you know, the current program plan was
12 embodied in SECY-01-0155, published in August '01. It
13 will come to an end -- the planning horizon for that
14 plan -- at the end of this fiscal year.

15 So we're in the process right now of
16 developing a new research program plan, which will
17 describe our successes, the things we haven't gotten
18 to for resource or commitment issues, and then talk
19 about what we're going to do in the future. We'll
20 probably have some interactions with the committee
21 late summer or early fall on that issue.

22 The research plan was developed in answer
23 to the National Academy of Sciences' National Research
24 Council study calling for a more systematic and
25 integrated research program in this area. It was

NEAL R. GROSS

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

1 reviewed and endorsed by the ACRS and the Commission.

2 It has five basic program areas. We'll
3 get to those in a minute. The reliability program is
4 one of the five program areas within the research
5 program. Our goal is basically to improve the staff's
6 analytic capabilities and their fundamental knowledge.

7 To do any kind of reasonable assessment
8 you need both a fundamental knowledge of how the
9 systems work and how they fail and what problems you
10 can get yourself into, and the analytical
11 capabilities, the tools, the models, the procedures,
12 to be able to use that knowledge in a review process.
13 And that's our basic goal -- to get those two pieces
14 and provide them to our regulatory brethren.

15 MEMBER KRESS: Your 10 minutes are up.

16 MR. ARNDT: Okay.

17 MEMBER KRESS: Is this research in
18 cooperation with any of the industry? Is EPRI or NEI
19 involved at all?

20 MR. ARNDT: We've done some cooperative
21 work with EPRI. That is always a challenge, to try
22 and find efforts that mesh well and also don't have a
23 conflict of interest in various other areas. As with
24 all of the other research programs, we meet with EPRI
25 on a fairly regular basis, with industry brethren on

NEAL R. GROSS

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

1 an occasional basis, to talk about what's going on,
2 what we can do.

3 We currently are doing some work I believe
4 in the wireless program collaboratively with the
5 industry, but none of the reliability programs are
6 currently collaborative in a strict sense. We're
7 using work in the industry.

8 MEMBER APOSTOLAKIS: Yes. Can you go back
9 to 6?

10 MR. ARNDT: Yes.

11 MEMBER APOSTOLAKIS: On what basis have
12 you decided that the current analysis methods are
13 sufficiently mature?

14 MR. ARNDT: The basis -- well, we'll talk
15 about that later in the presentation. But the basis
16 is that they're being used in other industries for
17 safety-critical decisionmaking.

18 There has been -- define "successful" as
19 you like -- successful applications of these
20 methodologies for safety decisionmaking in industries
21 that are sufficiently similar to the kinds of
22 decisions and the kinds of systems that we have to be
23 practical for -- in implementation.

24 MEMBER APOSTOLAKIS: And these industries
25 are?

1 MR. ARNDT: The transportation industry,
2 for example, the rail industry --

3 MEMBER APOSTOLAKIS: Is NASA using any of
4 these?

5 MR. ARNDT: NASA is using many of these
6 methods. The aerospace industry -- not all of the
7 industries are using the same methods. All of them
8 are as comfortable with the methods as others.

9 MEMBER KRESS: When you say "methods," are
10 there more than one?

11 MR. ARNDT: Yes.

12 MEMBER KRESS: To say the fault injection
13 process?

14 MR. ARNDT: Well, there's a number of
15 methods, and you can dice them up any of a number of
16 ways. One would be a fully integrated system modeling
17 type method versus modeling systems that are not fully
18 integrated, like software separate from hardware --

19 MEMBER KRESS: Yes.

20 MR. ARNDT: -- things like that. You can
21 dice and buy the kinds of particular analytical method
22 to use, petri nets, dynamic fault trees, dynamic flow
23 graphs. You can dice them by whether they're
24 primarily data-driven or system model driven. You can
25 dice them in a lot of different ways.

NEAL R. GROSS

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

1 But the point is that some subset of the
2 models have been successfully used in a regulatory
3 sense, which is the basic piece of information that
4 drives the conclusion that it -- we are capable of
5 doing -- writing regulatory guidance.

6 Now, whether or not we can write
7 regulatory guidance that would be effective in this
8 industry is something that remains to be seen.

9 MEMBER APOSTOLAKIS: But when we say
10 "analysis methods," maybe we can make a distinction
11 between methods that search for faults in the software
12 and methods that attempt to quantify the reliability
13 or probability of failure. And you're referring to
14 both sets?

15 MR. ARNDT: I'm referring to both sets.

16 MEMBER APOSTOLAKIS: Because a number of
17 years back the staff, when they were writing the
18 standard review plan I think, they told us they talked
19 to Boeing, and Boeing told them to forget about all of
20 these markers, and just test the thing. And, in fact,
21 there is a regulatory guide that --

22 MR. ARNDT: Yes.

23 MEMBER APOSTOLAKIS: -- or someplace where
24 it says the staff, at this time, does not place any
25 confidence in --

NEAL R. GROSS

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

1 MR. ARNDT: Yes, that is --

2 MEMBER APOSTOLAKIS: -- on that.

3 MR. ARNDT: That is the current regulatory
4 position.

5 MEMBER APOSTOLAKIS: So since then things
6 have changed.

7 MR. ARNDT: Since then, the progress of
8 technology, both in the ability to model how the
9 system fails, and the ability to quantify that, has
10 progressed.

11 MEMBER APOSTOLAKIS: Okay. Okay. We'll
12 see later --

13 MR. ARNDT: Okay.

14 MEMBER FORD: Steve, I've got a general
15 question.

16 MR. ARNDT: Okay.

17 MEMBER FORD: Some time ago you mentioned
18 to me that you were involved in SCSIM development.

19 MR. ARNDT: Yes.

20 MEMBER FORD: Is that with respect to
21 quality?

22 MR. ARNDT: No.

23 MEMBER FORD: Are you using it in this
24 program?

25 MR. ARNDT: We're not. That happens to be

NEAL R. GROSS

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

1 just one of my personal sidelines.

2 MEMBER FORD: Oh, okay.

3 MR. ARNDT: Examples of meeting those
4 goals have to do with developing analytical models,
5 updating guidance like the reg guide that you recently
6 saw from us, and doing technical support of other
7 regulatory programs, be it software quality,
8 instrument work, systems and review work, etcetera.

9 The four aspects -- the five aspects of
10 the program -- I will go through quickly the four that
11 are not reliability programs, just to give you a
12 context. One of them is systems aspects of digital
13 systems, environmental stressors, PMI/RFI
14 environmental qualifications, those kinds of issues,
15 requirement specifications, operating systems. These
16 are things that have generic application to a large
17 group of systems or component-level type issues.

18 Software quality assurance issues,
19 requirement specifications, the issue of how do you
20 test requirements, how do you test failures like that,
21 how do you look at engineering -- specific engineering
22 criteria -- the work at Maryland touches on this
23 program as well as the reliability program.

24 Emerging technologies and their
25 applications -- this is a proactive part of our

1 program where we're looking at specific technologies
2 that either are becoming or already have become major
3 issues in the balance of plant applications and may
4 become safety issues in the future.

5 So advanced instrumentation, smart
6 sensors, wireless communications, large programs for
7 security, as you might imagine. And we also have a
8 program that continuously reviews technology to
9 determine what we should fold into this program.
10 Things like application-specific ICs and things like
11 that will probably get folded into the next update of
12 the plan this year.

13 Advanced reactor I&C infrastructure -- as
14 you have heard from many briefings on advanced
15 reactors, one of the parts is the reapplication
16 reviews. The other part is the infrastructure
17 development. I&C has a piece of that. We're looking
18 at various different issues. We have a lessons
19 learned document looking at what we can learn from the
20 other plants.

21 One of the recommendations of the National
22 Academy's study was to do more, learn more from what
23 has happened in the industry, other places than the
24 United States. And I will point out that one part of
25 the advanced reactor program is the development of

NEAL R. GROSS

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

1 risk assessment for plant applications --
2 specifically, developing issues to, one, support I&C
3 in the risk framework for advanced reactors, as well
4 as look at specific applications to new technology
5 that's going to be developed for advanced reactors and
6 how that will impact our other work in the reliability
7 program.

8 Risk assessment of digital systems -- this
9 is the program we're going to talk about today. There
10 are four basic areas, and they kind of, over the last
11 four years since we wrote the plan, have kind of
12 diverged a little bit.

13 But the basic areas are looking at data
14 sets and understanding what's available, how we can
15 use it, how we can bound things, not only for specific
16 applications of developing failure rates, but also
17 what does the data tell us? Is it confirming our
18 assumptions? Is it giving some information on what's
19 more important and what's less important? Those kinds
20 of issues.

21 MEMBER APOSTOLAKIS: You'll address this
22 later?

23 MR. ARNDT: Yes. We'll talk about this
24 later.

25 MEMBER APOSTOLAKIS: Good.

1 MR. ARNDT: But one of the big issues is:
2 will there ever be enough data to really do
3 reliability predictions? Well, that's a debatable
4 issue, but there will always be some data. And we can
5 use that data to do these other things as well.

6 MEMBER APOSTOLAKIS: These are failure
7 data from other industries, I suppose.

8 MR. ARNDT: Well, both -- very limited
9 from the nuclear industry and from other industries.

10 MEMBER APOSTOLAKIS: Okay.

11 MR. WHITE: Steve, this is James White.
12 One of the -- a couple of things that we found in the
13 National Academy's study was we had a lot of -- people
14 seemed to have a lot of difficulty finding this
15 reliability data, that vendors who had worked in other
16 industries were a little reluctant to share that data.
17 I'd be interested in how much progress you think we've
18 made since the National Academy's study.

19 And the second question, before I forget
20 it, is that we found that it -- it seemed that the
21 nuclear industry was talking to itself a lot when it
22 was wrestling with the software reliability problem.
23 And I'd be interested -- and maybe you're going to
24 cover it in your presentation -- how we are really
25 putting out work that is: a) published with peer

NEAL R. GROSS

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

1 review, and b) how we are becoming part of the
2 community, so that we are not alone in the work.

3 Thank you.

4 MR. ARNDT: I will attempt to answer those
5 questions as part of my presentation in the
6 presentation to the contractors. If I don't, please
7 remind me again, because one of the big issues in
8 this, as you say, is it's a very difficult problem.
9 It's a problem we've been wrestling with as a
10 community in the software business and the digital
11 system business for some time.

12 Nuclear is a very small piece of it. It's
13 a very specialized small piece of it, in addition to
14 that. So tying in, both consciously and through our
15 contractors and through collaborative work, is a
16 conscious effort we have made to try and improve that
17 over the last four or five years. And we've been I
18 think reasonably successful in that area. Obviously,
19 we can do more, and we're working to do more, both in
20 the nuclear area as a whole and the other industries
21 and other efforts.

22 The two areas here -- digital failure
23 assessment methods and digital reliability assessment
24 methods -- this really gets to, do we understand the
25 systems? Do we understand how the systems fail? Do

1 we understand the failure modes? Can we model them
2 properly?

3 And this basically has to do -- once we
4 know that, and we take that and put it into a
5 methodology, that will get us actual quantitative
6 numbers that we can then use in regulatory space.

7 And then the last part, of course, is
8 guidance, be it reg guides or review guidance or
9 checklists, or whatever, for assisting NRR staff in
10 their ability to review this work.

11 Just to give you a --

12 MEMBER APOSTOLAKIS: Well, let me
13 understand this a little better. What actions,
14 regulatory actions, do you foresee NRR will face in
15 the next couple of years?

16 MR. ARNDT: Okay. We're going to talk
17 about this a little bit more. But to give you the
18 five-second version, a lot of the plants are upgrading
19 their systems, both small individual pieces and some
20 plants -- I think the number now is four that have
21 already told us they're going to do complete control
22 room upgrades. And we suspect that there's going to
23 be a lot more than that.

24 As well as -- that's basically large-scale
25 reviews that are going to hit all of the different

NEAL R. GROSS

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

1 areas, including software and other things, as well as
2 there are several plants that as part of that review
3 would like to risk-inform at least parts of their
4 application, particularly the defense-in-depth and
5 diversity requirements.

6 So we have both the issue of specific
7 areas that are going to want to use risk information
8 that we need to find methods to assess and information
9 to validate, as well as the overall process that we
10 would like to improve, make more quantitative, more
11 realistic, more consistent.

12 MEMBER APOSTOLAKIS: So do you foresee
13 that we may have a regulatory guide like we have now
14 for risk-informed ISI and --

15 MR. ARNDT: That's under discussion.

16 MEMBER APOSTOLAKIS: Okay.

17 MR. ARNDT: We haven't -- we haven't
18 discussed it enough with NRR for me to comment on it.

19 MEMBER APOSTOLAKIS: That's fine.

20 MR. ARNDT: It's something that we're
21 looking at.

22 MEMBER APOSTOLAKIS: Yes.

23 MR. ARNDT: Just to give you a quick
24 perspective, the budget for the I&C section, all of
25 the stuff I've just talked about, is about

NEAL R. GROSS

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

1 \$3.8 million in ISDE. Of that, about one FTE and
2 \$1 million is devoted to the reliability program.

3 This gives you a quick perspective on the
4 kind of resources we're spending on this kind of --

5 MEMBER APOSTOLAKIS: So reliability
6 program means Virginia and Maryland?

7 MR. ARNDT: No. It means everything we're
8 going to talk about today -- Virginia, Maryland, the
9 BNL work.

10 MEMBER APOSTOLAKIS: Okay.

11 MR. ARNDT: Some of our in-house work.

12 MEMBER APOSTOLAKIS: Okay.

13 MR. ARNDT: Okay. Program external drive
14 -- we've talked about this a little bit. National
15 Academy of Sciences' National Research Council
16 recommendations -- Jim was on that committee.

17 One of the many issues that they raised
18 was this whole issue of software reliability and
19 digital systems reliability, and we should be more
20 proactive in that. We'll talk about it a little bit
21 more.

22 I mentioned the DOE I&C and human machine
23 interface working group recommendations. This was a
24 group of people that was convened by DOE a little less
25 than two years ago to specifically look at what are

NEAL R. GROSS

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

1 the things that advanced reactors aim for? Basically,
2 the NERI/NEPO kinds of issues. What is going to come?
3 Why is it going to be an issue?

4 They had a subgroup on regulatory issues.
5 The biggest recommendation out of that subgroup was
6 you've got to be able to risk-inform the applications.
7 Outside the mainstream you can't do that, particularly
8 since the advanced reactors reviewed are hopefully
9 going to be more risk-informed.

10 There was a workshop in Halden in December
11 of 2002 that also looked at this from an international
12 standpoint. There were recommendations out of that
13 that basically said we need to do more than -- there
14 is not self-consistency within the international
15 community, and that we need to develop these issues.

16 And I'll talk to this last one. In
17 particular, the draft EPRI report on diversity and
18 defense-in-depth -- that's what I mentioned a few
19 minutes ago. The diversity and defense-in-depth
20 requirements were written when we rewrote Chapter 7 of
21 the standard review plan, because at the time the
22 information available on software common mode failure
23 and those kinds of issues was very sparse. The
24 requirement, in the opinion of many in the industry,
25 is unnecessarily restrictive.

NEAL R. GROSS

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

1 EPRI has developed a draft topical report
2 that they tell us they will submit in I think it's
3 August of this year for review.

4 MEMBER KRESS: Is that diversity you're
5 talking about having a separate analog system?

6 MR. ARNDT: Yes.

7 MEMBER KRESS: Okay.

8 MEMBER APOSTOLAKIS: Can we get a copy of
9 this EPRI report?

10 MR. ARNDT: Is it publicly available, do
11 you know?

12 MEMBER APOSTOLAKIS: Do you have a copy?

13 MR. ARNDT: Yes, I have a copy.

14 MEMBER APOSTOLAKIS: Then we should have
15 a copy.

16 MR. ARNDT: It was given to us for a
17 courtesy review.

18 MEMBER APOSTOLAKIS: Yes. Well, not the
19 public, I don't think. If you have a copy, we should
20 have a copy. And we will treat it appropriately.

21 MEMBER ROSEN: A follow-up to Tom's
22 question, you said on this diversity and defense-in-
23 depth it was -- it meant an analog system backing up
24 a digital. Is that what I heard you say, or could it
25 mean a different digital system backing up?

NEAL R. GROSS

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

1 MR. ARNDT: It can be a different digital
2 system.

3 MEMBER ROSEN: Either one.

4 MR. ARNDT: Yes.

5 MEMBER ROSEN: Okay. Now, while I've got
6 your attention, let me just ask what your thumbnail
7 sketch is of what you mean by "risk-informing these
8 requirements." I could guess, but I'd rather hear
9 what you think.

10 MR. ARNDT: The draft that's on the table
11 basically uses a methodology that we'll talk about a
12 little bit more in -- later in the presentation to
13 come up with a criteria based on .174 risk criteria
14 that basically says, "This is good enough from a risk
15 standpoint."

16 The current requirement asks you to go
17 through and do a very detailed review of what can
18 happen if a system fails due to a common mode failure
19 software. This is an alternate method to do that
20 analysis that basically uses risk-informed criteria as
21 the decision point as opposed to a deterministic
22 analysis of, if it fails, it's not a problem.

23 MEMBER KRESS: So it takes into account
24 the consequences of failure, not just the fact of
25 failure.

1 MR. ARNDT: Yes.

2 MEMBER KRESS: Is that what you're saying?

3 MR. ARNDT: Yes.

4 MEMBER KRESS: It takes into account the
5 frequency also.

6 MR. ARNDT: It derives a frequency of
7 failure of the system, of the software --

8 MEMBER ROSEN: And then assesses the
9 consequences and comes up with a risk.

10 MR. ARNDT: Right.

11 MEMBER ROSEN: As opposed to just saying,
12 "Deterministically, show me that everything that
13 failed -- that can fail, will fail, and what the
14 effects are."

15 MR. ARNDT: Well, it's a somewhat unusual
16 thing, because it requires certain specific
17 assumptions on how the system failed and what you can
18 credit and what you can't credit. But basically
19 that's correct. It says, "These are the basic
20 assumptions you have to make, do a deterministic
21 analysis and come up with, will it meet the threshold
22 or not?"

23 MEMBER ROSEN: Okay. Thank you.

24 MEMBER APOSTOLAKIS: Was the DOE report
25 really a driver, though, Steve?

1 MR. ARNDT: It wasn't a driver so much as
2 a confirmation that -- the people who design things
3 and look at these kind of things are going the same
4 direction.

5 MEMBER KRESS: Was the National Academy
6 report useful to you?

7 MR. ARNDT: It was, more so in some areas
8 than others. Of course, it's somewhat dated now, but
9 it highlighted some --

10 MEMBER KRESS: It was '93, wasn't it, when
11 it --

12 MEMBER APOSTOLAKIS: No.

13 MR. ARNDT: No, no, it was --

14 MEMBER APOSTOLAKIS: '99? 2000?

15 MR. ARNDT: I've got it right here.

16 MEMBER KRESS: Well, '93 is when it
17 started.

18 MR. ARNDT: Yes. But it was published in
19 '97.

20 MEMBER KRESS: Okay.

21 MR. ARNDT: The final recommendations were
22 hashed out relatively late in the process, if I
23 remember correctly.

24 MEMBER KRESS: The reason I ask is, you
25 know, I sometimes wonder whether ACRS recommendations

1 are useful to you. That thing got started as an ACRS
2 initiative.

3 MR. ARNDT: Yes, I know. Yes, they are,
4 particularly since the committee has a broader
5 perspective on these things than sometimes we do.

6 MEMBER APOSTOLAKIS: Are you asking him
7 whether the ACRS is useful?

8 MEMBER KRESS: Well, I was --

9 MEMBER APOSTOLAKIS: Did you expect him to
10 say no?

11 (Laughter.)

12 MEMBER KRESS: Actually, no, I didn't.
13 But actually, I was wondering --

14 MEMBER APOSTOLAKIS: Steve is an honest
15 guy, but this is pushing too far.

16 MEMBER KRESS: I was wondering in that
17 specific case whether it was good advice to them.

18 MR. ARNDT: A quick review of the -- what
19 the National Academy said and what the NRC's PRA
20 policy says. This was in your package that we sent
21 you, so I won't go over it in detail. But the basic
22 thrust was we need to be able to assess software
23 failures in a reliability sense.

24 We need to be able to develop failure
25 probabilities, particularly including COTS software,

1 or COTS hardware for that matter. We need to be able
2 to understand and analyze the systems, and we should
3 be working with whoever is appropriate to develop the
4 capabilities and expertise to be able to do this kind
5 of thing.

6 MEMBER KRESS: Well, that sounds like an
7 ACRS letter.

8 MR. ARNDT: Well, you can thank Jim and
9 his colleagues for that.

10 MEMBER APOSTOLAKIS: And by the way, that
11 letter the committee wrote, when was it, 10 years ago?

12 MEMBER KRESS: '91.

13 MEMBER APOSTOLAKIS: Yes. It was one of
14 the most obscure letters --

15 MEMBER KRESS: '93.

16 MEMBER APOSTOLAKIS: -- ever to come out
17 of --

18 MEMBER KRESS: Yes, I know it was --

19 MEMBER APOSTOLAKIS: -- this committee.

20 MEMBER KRESS: I know. Sort of wandered
21 around. That puts it in real concise terms.

22 MEMBER APOSTOLAKIS: Yes.

23 MR. ARNDT: Just a reminder that the PRA
24 policy asks the staff to increase the use of PRA. The
25 operative word here -- to the extent supported by the

NEAL R. GROSS

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

1 state-of-the-art methods and data.

2 The real issue is, as we've pointed out,
3 the last time we looked at this in the '97 timeframe
4 when we updated the SRP, we didn't think that it was
5 appropriate. Now we're looking at it again, and we
6 think it may be appropriate.

7 MEMBER KRESS: We were wondering what your
8 interpretation is of what's meant by state-of-the-art
9 methods. It can be interpreted several ways.

10 MR. ARNDT: Yes. My personal opinion is
11 state of the art was a poor choice of words when we
12 helped -- when we wrote that. I actually helped write
13 that particular part of the document. What it really
14 should mean is state of the practice.

15 MEMBER KRESS: That's what we thought.

16 MR. ARNDT: Can you practically do this
17 with the domain that you're interested in, with the
18 kinds of information that is necessary to make a
19 decision?

20 A quick review of the kinds of things
21 we're trying to attack -- this is actually from a
22 paper that Nathan and I wrote about a year and a half
23 ago. The kinds of things we need to be able to do
24 this work is an understanding of the state of the
25 data, what is it -- what are the limitations, what are

NEAL R. GROSS

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

1 we going to have to work around, understanding -- a
2 deep fundamental understanding of how the systems
3 fail, what kinds of effects are important, is
4 communication issues important, is timing issues
5 important, software important, strengths and
6 limitations of these models, what are they going to
7 tell you, what are they not going to tell you.

8 MEMBER APOSTOLAKIS: Has this been done?

9 MR. ARNDT: Part of our research in
10 several of the programs we're going to talk about gets
11 at this particular issue.

12 MEMBER APOSTOLAKIS: So there is a review
13 of the available models, so there will be a review of
14 available --

15 MR. ARNDT: Actually, almost all of our
16 projects have this as part of their program.

17 MEMBER APOSTOLAKIS: So we're going to
18 hear about it today?

19 MR. ARNDT: We're going to hear about some
20 of it today.

21 MEMBER APOSTOLAKIS: Okay.

22 MR. ARNDT: There was a short discussion
23 of this in the first report that University of
24 Virginia put out. There's going to be a much more
25 extensive discussion in the report of BNL. Our future

NEAL R. GROSS

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

1 work is also going to reassess these issues.

2 MEMBER APOSTOLAKIS: Because that has been
3 a major problem with the human reliability models.

4 MR. ARNDT: That's correct.

5 MEMBER APOSTOLAKIS: There was never a
6 critical review of other people's work, and, you know,
7 trying to build on the good parts of different models.

8 MR. ARNDT: Right.

9 MEMBER APOSTOLAKIS: Each guy develops his
10 own or her own. Okay.

11 MR. ARNDT: The whole issue of how do you
12 incorporate a model into the PRAs, not only PRA as a
13 whole but the actual PRAs that are being used -- the
14 practical applications that are being used. And there
15 are some significant limitations because of the
16 structure of the current PRAs that are out there.

17 And then, understanding what your
18 acceptance criteria is, not only for the actual number
19 and the uncertainty associated with that number, but
20 also, if you will, PRA quality or the model quality.
21 How good does it have to be? What kind of assumptions
22 are acceptable? What are not acceptable?

23 What we're trying to accomplish is to
24 improve the review process by providing additional
25 information, guidance, and tools. To accomplish this,

NEAL R. GROSS

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

1 we're going to basically develop the understanding,
2 improve the guidance, and develop tools that can
3 assess the system, inform the reviews and/or provide
4 audit calculation type capability.

5 I'll try and skip through the next three
6 or four slides pretty quickly. It's basically just
7 the structure of what we're trying to accomplish and
8 how we're trying to accomplish it, how the programs
9 fit into what I just said.

10 The kinds of products we're going to have
11 -- we'll basically develop a tool box that can develop
12 guidance as to what is acceptable and what's not by
13 quantitative measures to better inform the reviews.
14 At this point, we do not envision going entirely to a
15 quantitative review, like 2,200 degrees for fuel
16 mount.

17 What we want to do is make the reviews
18 that are currently very qualitative more quantitative
19 to increase their realism and their repeatability, and
20 perhaps demonstrate alternative methods to meet the
21 safety goals, like third party audits and things like
22 that.

23 These are the research projects that we
24 have in this program. These are diverse integrated
25 digital systems modeling, which you'll hear more about

NEAL R. GROSS

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

1 -- at the University of Maryland, the software metrics
2 project, which you'll hear more about.

3 And we have the BNL project on digital
4 system risks. This project is basically going at it
5 from the PRA standpoint backwards. These two projects
6 are basically going from the failure kind of methods
7 and the -- how you model how the system has failed
8 toward the PRA. So it's a different perspective on
9 the same problem.

10 And we have several other programs that
11 I'll go over briefly, basically some additional
12 database issues and some additional efforts, including
13 the work that Halden is doing in this area.

14 MEMBER ROSEN: And we're going to hear
15 about the BNL project, too?

16 MR. ARNDT: Right now.

17 DR. GUARRO: Excuse me, Steve. On
18 Chart 20, you say digital system failure mechanisms.
19 Can you clarify the scope of that? In other words,
20 when you -- the term "failure mechanism" extends to
21 what?

22 MR. ARNDT: It extends to how the system
23 fails. Basically, is it failing because of random
24 failures of the hardware? Is it failing because of
25 software encountering situations it was not designed

NEAL R. GROSS

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

1 for? Is it failing because of data communication
2 issues? Is it failing -- basically, how does it fail,
3 and why does it fail? And what design and
4 implementation issues or contexts --

5 DR. GUARRO: So you include the design
6 side as well.

7 MR. ARNDT: Yes.

8 DR. GUARRO: Thank you.

9 MR. ARNDT: Quickly, the way we're trying
10 to accomplish what I just talked about in these
11 particular programs -- the University of Virginia is
12 integrating -- is looking at integrated digital
13 systems modeling projects. They're going to develop
14 assessment methods that can be used by the staff for
15 independent assessment -- \$4 billion for that matter
16 -- to understand the models and come up with other
17 numbers on whether or not they function properly.

18 And they are also developing information
19 on failure modes in reliability that can be used in
20 the regulatory guidance to form our guidance
21 development.

22 MEMBER APOSTOLAKIS: So how is this
23 different than from what BNL is doing, digital system
24 risk?

25 MR. ARNDT: I'll tell you in a minute.

NEAL R. GROSS

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

1 MEMBER APOSTOLAKIS: Okay.

2 MR. ARNDT: They are basically developing
3 methods from the -- how does the system --

4 MEMBER APOSTOLAKIS: They? They?

5 MR. ARNDT: Virginia.

6 MEMBER APOSTOLAKIS: Yes.

7 MR. ARNDT: How does the system fail? How
8 can we model those failures? What are the critical
9 issues associated with it? And developing a
10 methodology that we can use to evaluate it.

11 MEMBER APOSTOLAKIS: Okay.

12 MR. ARNDT: And they're using the
13 information they gained through that process to form
14 our reviews.

15 Maryland's software metrics project is
16 developing methods to assess -- help us independently
17 assess software quality, basically developing a method
18 using software metrics that is readily available.
19 Metrics are developed as part of the design process
20 and testing process -- that can help us independently
21 assess the system. That will also --

22 MEMBER APOSTOLAKIS: Wait a minute now.
23 So you will have two methods for reliability
24 assessment -- Maryland and Virginia?

25 MR. ARNDT: Yes.

1 MEMBER APOSTOLAKIS: Two separate methods.

2 MR. ARNDT: Two separate methods.

3 MEMBER KRESS: Yes. I'm having trouble
4 figuring out how this University of Maryland work led
5 to reliability. I sort of envisioned you ended up
6 with a software quality index of some sort, based on
7 the processes it went over.

8 MR. ARNDT: Well, we'll talk about this in
9 detail this afternoon. But the issue is: you will
10 end up with an understanding of how the particular
11 metrics of software quality affect the overall quality
12 of the system, and also whether or not those are good
13 predictors of its reliability.

14 MEMBER KRESS: But you have to have
15 another way to measure the reliability in order to
16 make that assessment?

17 MR. ARNDT: Yes.

18 MEMBER KRESS: Yes.

19 MR. ARNDT: You have to test the system to
20 validate --

21 MEMBER KRESS: Okay.

22 MR. ARNDT: -- the methodology.

23 MEMBER KRESS: Okay. This --

24 MR. ARNDT: One of the things we're doing
25 is testing it by doing that to determine whether or

NEAL R. GROSS

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

1 not it is --

2 MEMBER KRESS: So this is like the six or
3 seven parameter input. It ends up with quality and
4 reliability, and you're going to try to --

5 MR. ARNDT: You've got to validate it.

6 MEMBER KRESS: -- get some sort of
7 correlation between the two or --

8 MR. ARNDT: Well, it's not a correlation.

9 MEMBER KRESS: Not a correlation, but
10 some --

11 MR. ARNDT: It's a model --

12 MEMBER KRESS: It's a --

13 MR. ARNDT: -- that basically says this
14 kind of information will give you a good prediction of
15 how well it will behave in the future, because --

16 MEMBER KRESS: You expect that to be a
17 qualitative thing rather than quantitative?

18 MR. ARNDT: It will be a quantitative
19 system. It probably -- we will probably not get to
20 the point that says, "If it meets this number, it's
21 okay." It's not going to be that kind of
22 quantitative, but it will be a number that we would be
23 able to use to inform the process.

24 MEMBER APOSTOLAKIS: So, and BNL is also
25 going to develop a risk model?

1 MR. ARNDT: The BNL project is focused
2 on --

3 MEMBER APOSTOLAKIS: Yes.

4 MR. ARNDT: -- these kinds of things.
5 They're looking at helping us write the regulatory
6 guidance. They're doing a detailed review of the
7 current methods, as you mentioned. They're looking at
8 the database issues, and they're looking at how do you
9 take these kinds of models -- these two models were
10 assessments of the systems.

11 This is specifically looking at taking
12 that and other data and putting them into the PRA
13 context.

14 MEMBER ROSEN: Are you going to give us
15 some more detail about that?

16 MR. ARNDT: Yes.

17 MEMBER ROSEN: So we have some sort of
18 flavor of what's being thought about?

19 MR. ARNDT: Yes, sir.

20 MEMBER APOSTOLAKIS: Well, it's
21 interesting that you are developing two reliability
22 models. Why?

23 MR. ARNDT: The big issue is we don't know
24 what the licensee is going to submit to us. There is
25 a lot of different methods out there currently, which

1 we'll talk about in a minute.

2 Some of them are completely integrated
3 systems. Some of them are not completely integrated
4 systems. As you know, there's a large debate as to
5 whether or not that is reasonable and how to do
6 different things like that.

7 The bottom line is we need to understand
8 how these issues affect the system, so we can make an
9 assessment. So we're going at it in several different
10 ways, so we can gain enough information to be able to
11 write guidance, what is acceptable, what is not
12 acceptable, what the limitations are of various
13 methods, and look at improving our regulatory process
14 in various specific ways.

15 MEMBER APOSTOLAKIS: So the thing that
16 will ultimately really be the final product is this
17 digital system PRA model.

18 MR. ARNDT: There will be several things.
19 The guidance will be --

20 MEMBER APOSTOLAKIS: Yes. Yes.

21 MR. ARNDT: -- an issue.

22 MEMBER APOSTOLAKIS: In terms of numbers.

23 MR. ARNDT: In terms of numbers, we hope
24 to have, either through this work or other work, a
25 tool that we can basically run like we run Sapphire

1 now, to give us a check on whether or not the number
2 that the licensee is giving us makes sense or not.

3 MEMBER APOSTOLAKIS: And work at Maryland
4 and Virginia and possibly other places provides input?

5 MR. ARNDT: That's correct.

6 MEMBER APOSTOLAKIS: Okay. That's a very
7 interesting approach.

8 MEMBER KRESS: Yes. Let me tell you what
9 my initial view of this was, and you tell me where I'm
10 wrong. The current way we look at software quality is
11 by evaluating the process mostly.

12 MR. ARNDT: Mostly.

13 MEMBER KRESS: Rather than the product.

14 MR. ARNDT: Correct.

15 MEMBER KRESS: Now, I viewed the
16 University of Maryland work as looking at that process
17 and trying to maybe rank the parts of it as to their
18 effect on quality in some way, but not yet looking at
19 the product. And I viewed the University of Virginia
20 work as focusing on the product and actually trying to
21 figure out a way to take the product and get some
22 measure of its reliability. And then you have a way
23 to maybe connect the two, and is that --

24 MR. ARNDT: Yes.

25 MEMBER KRESS: -- is that a pretty good

NEAL R. GROSS

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

1 view of what you're doing?

2 MR. ARNDT: It's an appropriate view.
3 It's not a comprehensive --

4 MEMBER KRESS: It's not comprehensive.

5 MR. ARNDT: -- approach, not inaccurate.

6 The process we're trying to do is to take
7 various pieces and both improve the current process,
8 which is mostly process and development based, and to
9 develop a new process that is primarily product based,
10 so that we can review the systems more effectively.

11 MEMBER APOSTOLAKIS: So there may be a
12 combination at the end.

13 MR. ARNDT: Absolutely.

14 MEMBER APOSTOLAKIS: Yes.

15 MR. ARNDT: And in many cases it will be
16 driven by what the licensees give us.

17 MEMBER ROSEN: Steve, I think that's my
18 cue for jumping in here. I'm a little bit surprised
19 by that attitude -- that it will be controlled by what
20 the licensees give us. We don't know what the
21 applicants are going to send to us to review.

22 I mean, those kinds of statements you made
23 are a little bit surprising, because I think there's
24 another way to go at this, which would be to define
25 through this research what the licensees or applicants

NEAL R. GROSS

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

1 need to give you.

2 MEMBER KRESS: Well, a lot of that will
3 come out of your guidance, I think, yes.

4 MR. ARNDT: And maybe the tone in which I
5 said it was not appropriate. But the research has
6 several slants on it. One, of course, is exactly what
7 you said. We develop an understanding of all of the
8 different commonly used methods, so we can assess what
9 is provided.

10 The other issue is we need to make a
11 decision, both in terms of a number if we're going to
12 use a number, and also on what is acceptable in terms
13 of modeling. If we make a determination that certain
14 models are simply not sufficiently accurate,
15 sufficiently reliable, whatever, based on our
16 research, then we draw a threshold there.

17 So, yes, you're right. A large part of
18 our research is to define what is acceptable, what the
19 validity of the models are, if you will.

20 You'll hear later this afternoon about a
21 lot of the programs, particularly in Maryland and
22 Virginia. It's not just the model, but it's also
23 validating the system. We're using actual nuclear
24 instrumentation and control systems to validate it.
25 Does it work? Is it acceptable?

NEAL R. GROSS

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

1 MEMBER ROSEN: I mean, to simplify this
2 discussion, it seems to me that one could say to an
3 applicant, "You can design software any way you like,
4 and to have it do anything you'd like it to do in the
5 powerplant. But you must analyze it after you're done
6 with that and submit that analysis this way," because
7 that's the way we evaluate the -- what your products
8 are.

9 And that would then allow the applicants
10 and the vendors to say, "Okay. Ultimately, we're
11 going to have to pass this test, so our software may
12 have to be -- and the way we design it -- may have to
13 facilitate that."

14 MEMBER KRESS: Yes. Quite often the reg
15 guides serve that purpose -- talking about developing
16 reg guides.

17 MR. ARNDT: The reg guide -- a reg guide
18 can serve that function, but not as strongly as you
19 just put it.

20 MEMBER KRESS: It's one way to --

21 MR. ARNDT: It highlights an acceptable
22 method. In some cases it becomes a de facto
23 requirement because of the way we --

24 MEMBER ROSEN: Because it's too hard to do
25 otherwise. To support the -- a review by the staff of

1 some alternate method that maybe somebody thinks is
2 better, they say -- you can rightfully say, "Well, you
3 can do anything you want to do not to comply with this
4 reg guide, but it will take us longer." And that's
5 rational.

6 So this becomes, de facto, the way they do
7 business. But as long as that de facto was is a good
8 way that's well supported by research and your
9 knowledge, I don't see there's anything really wrong
10 with that. And I would -- I would think that it's a
11 better posture to be in, saying that's where we're
12 headed, than saying, "Well, we'll have to deal with
13 anything they send us."

14 MR. ARNDT: Well, yes, and that has, in
15 point of fact, been done in several industries. And
16 I think Dr. Johnson will mention that in his talk,
17 because he has done work in --

18 MEMBER ROSEN: Well, it's the way the
19 agency does business now. I mean, you can't just send
20 us anything. We have, you know, regulatory guides.

21 MEMBER BONACA: But, yes, in general,
22 however, vendors also propose ways in which you should
23 be testing. I mean --

24 MR. ARNDT: Yes.

25 MEMBER BONACA: -- they propose -- or they

NEAL R. GROSS

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

1 will propose, you know, concepts that should be used
2 for testing. And so you are -- you are trying to
3 understand acceptability --

4 MR. ARNDT: We're trying to understand,
5 based on the things that have been proposed or been
6 talked about -- like the EPRI guidance -- what is
7 acceptable and what is not acceptable. And the
8 current methods that are being used, both in the
9 United States and other places in the nuclear
10 business, are not as sophisticated, shall we say, as
11 some of the research we're doing.

12 And we also have the issue that the
13 current structure is basically qualitative. And if we
14 want to change that --

15 MEMBER ROSEN: And we do.

16 MR. ARNDT: Yes.

17 MEMBER ROSEN: And we must, I think.

18 MR. ARNDT: Well, we then need to
19 demonstrate that not doing it the other way is not
20 sufficient.

21 MEMBER ROSEN: We need to demonstrate
22 that?

23 MR. ARNDT: Well, we have a backfit rule
24 that we can't --

25 MEMBER ROSEN: Oh, well, for existing

1 plants maybe that's so.

2 MR. ARNDT: Yes.

3 MEMBER KRESS: Is it premature for you to
4 -- I guess it is -- to start thinking about what your
5 acceptance criteria are? I can see we're going to
6 have -- you know, look at specific digital I&C systems
7 related to safety functions probably, and you're going
8 to look at the defense-in-depth aspects of it.

9 And then you're going to quantify the
10 reliability and see what its contribution is to the
11 actual risk of various sequences. I don't know what
12 the -- you know, I don't know how to say -- when
13 you're focusing on some specific SSC --

14 MR. ARNDT: Yes.

15 MEMBER KRESS: -- what an acceptance
16 criteria might be. I mean, are you giving some
17 thought to that?

18 MEMBER APOSTOLAKIS: Why couldn't it be
19 1.174?

20 MEMBER KRESS: Well, that's for the whole
21 -- I don't know how you parse .174 into various
22 sequences and various components.

23 MR. ARNDT: You don't.

24 MEMBER APOSTOLAKIS: No. You just --

25 MEMBER KRESS: I know. But what we're

NEAL R. GROSS

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

1 doing is you're going to -- you're going to have
2 before you an I&C system for the safety function, and
3 we'll say, "Is it acceptable or not?" And I don't
4 know how you parse that into 1.174.

5 MEMBER APOSTOLAKIS: But we don't parse
6 anything out.

7 MEMBER KRESS: I know. But that's what
8 they're going to be faced with -- the decision. Is
9 that acceptable or not?

10 MR. ARNDT: Yes. And, really, the more
11 difficult issue, although that will be a difficult
12 issue, is the licensee may come to us with an analysis
13 based on whatever methodology and say, "The answer is
14 X, and that meets the .174 threshold," or acceptance
15 criteria.

16 The real issue we're going to have is: is
17 the analysis quality sufficient?

18 MEMBER KRESS: What's the uncertainty in
19 that --

20 MR. ARNDT: What is the uncertainty? What
21 is the -- do we believe the answer based on the
22 methodology that they use?

23 MEMBER ROSEN: And that's my exact point.

24 MR. ARNDT: And that's exactly correct.

25 That is the --

1 MEMBER ROSEN: That's my exact point. You
2 shouldn't get into that box. You should have your own
3 way of analyzing the software which you impose.

4 MR. ARNDT: Right.

5 MEMBER ROSEN: So you can analyze it any
6 way you like for your own purposes. But when you come
7 in here for regulatory approval, you must analyze it
8 this way. This is the way we understand it. We get
9 a delta CDF from that. We can compare to 1.174, and
10 make a judgment as to whether that's accurate --
11 acceptable within our --

12 MR. ARNDT: And one way to write the reg
13 guide is --

14 MEMBER APOSTOLAKIS: Now, you know, Steve,
15 yesterday we had a meeting on another subject, but we
16 were told that EPRI has started a project on
17 uncertainties in general with particular focus on
18 model uncertainty. We were also told that the staff
19 here -- Mary Druin I think is involved in that -- has
20 a parallel effort, and now they will start talking to
21 each other.

22 I believe you should at least be aware of
23 what they are doing and maybe give them some input,
24 because in my opinion you will have a serious model
25 uncertainty issue here --

NEAL R. GROSS

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

1 MR. ARNDT: Yes.

2 MEMBER APOSTOLAKIS: -- and all these
3 questions from Steve and Tom, you will have to address
4 it --

5 MR. ARNDT: Yes.

6 MEMBER APOSTOLAKIS: -- you know, the
7 issue of acceptability. So if the industry is doing
8 something on it, the staff itself is doing something
9 on it, you should be a participant and maybe by giving
10 them some of your problems you will help them as well
11 to do a better job. But you should also be aware of
12 what they are doing.

13 Right now they are looking at the major
14 model uncertainties in Level 1 PRA --

15 MR. ARNDT: Right.

16 MEMBER APOSTOLAKIS: -- like the RCB or
17 seal LOCA.

18 MR. ARNDT: Right.

19 MEMBER APOSTOLAKIS: And so on, and human
20 reliability. Yours is closer to human reliability.
21 I suspect you're going to have model uncertainty
22 that's pretty significant here.

23 MR. ARNDT: Yes. And --

24 MEMBER APOSTOLAKIS: So were you aware of
25 these efforts?

1 MR. ARNDT: I am aware of the effort. I
2 have not been an active participant in it.

3 MEMBER APOSTOLAKIS: Well, take it as a
4 first piece of advice from the subcommittee.

5 (Laughter.)

6 You should be aware of what they're doing.

7 MR. ARNDT: Oh, absolutely.

8 MEMBER APOSTOLAKIS: And they should be
9 aware of your problems.

10 MR. ARNDT: Absolutely. And one of the
11 challenges in this work is, of course, we have various
12 stakeholders within the agency. We have our PRA
13 group, we have NRR's PRA group, we have our I&C group,
14 we have the regulatory PRA group, we have the various
15 stakeholders outside the agency, including EPRI and
16 their --

17 MEMBER APOSTOLAKIS: That's model
18 uncertainty right there.

19 (Laughter.)

20 MR. ARNDT: Okay.

21 MEMBER APOSTOLAKIS: Okay, great.

22 MR. ARNDT: At the risk of trying to --

23 MEMBER BONACA: I just -- this is for
24 information for me. I mean, I am not an I&C person,
25 and I -- before you made a statement regarding the

NEAL R. GROSS

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

1 fact that some of the applications are -- maybe I
2 misunderstood, but limited or simple or -- now --

3 MR. ARNDT: Many of the models that are
4 being used --

5 MEMBER BONACA: Okay.

6 MR. ARNDT: -- particularly in the nuclear
7 area --

8 MEMBER BONACA: Yes.

9 MR. ARNDT: -- where this has gone a
10 little bit further down the path like in some of the
11 foreign countries, are more simplistic than the ones
12 that we are going to talk about today -- was the
13 statement I made.

14 MEMBER BONACA: What's the limitation? I
15 mean, why are they so simplistic? I mean, it seems to
16 me that, you know, we live in a world where there is
17 so much application of digital systems right now with
18 tremendous sophistication. I mean, what is limiting?
19 I'm trying to understand the limitations you are
20 talking about, the simplistic portion.

21 MR. ARNDT: The limitations are mostly
22 driven by compulsive -- the model you want to use, the
23 data you have available to populate that, either
24 failure data in a more generic sense or actual faults
25 and testing of the faults, and things like that, the

NEAL R. GROSS

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

1 amount of information you have about the proprietary
2 systems, and those kinds of things, because, as Dr.
3 Johnson will talk about a little bit -- and we'll talk
4 about a little bit elsewhere -- one of the challenges
5 in any kind of models like this is getting sufficient
6 information to populate them appropriately.

7 You have a lot of different computational
8 problems associated with it, which we are to a point
9 now I think it's not a major problem anymore, because
10 there have been some new methods developed, but not
11 everyone has embraced those, things like states-based
12 proliferation and things like that.

13 So there's a lot of specific modeling
14 challenges associated with this, and there are much
15 simpler kinds of methodologies, like software fault
16 trees and things like that, that don't deal with some
17 of these issues.

18 MEMBER BONACA: Okay.

19 MR. ARNDT: And it's a judgment call. Is
20 it sufficient? Is it a sufficiently accurate model
21 for the application you're trying to do? Can you
22 decouple software failures from the hardware context?

23 MEMBER ROSEN: Well --

24 MEMBER BONACA: Okay.

25 MEMBER ROSEN: -- I think the question of

NEAL R. GROSS

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

1 sufficiency is one of risk. I mean, it depends upon
2 what the risk introduced is.

3 MR. ARNDT: That's correct. And there
4 have been some proposals that basically say for
5 certain kinds of systems you need to demonstrate risk
6 to a certain level. One way of writing the criteria,
7 as has been proposed, is basically to say, for a
8 certain kind of system you have to have a sufficient
9 demonstration of the risk as lower than -- choose a
10 number -- 10^{-4} failures per demand with a reasonable
11 uncertainty, and develop a criteria based on that kind
12 of statement.

13 That's what was done in part at the size
14 we'll be analysis that they did. They basically set
15 a criteria that they didn't want the system to have
16 a --

17 MEMBER BONACA: Okay.

18 MR. ARNDT: -- failure on demand worse
19 than a particular thing --

20 MEMBER BONACA: So when you use the word
21 "simplistic," really you are talking about simplistic
22 approaches to evaluating the reliability of the
23 systems and determining faults. Okay. Because, I
24 mean, I was thinking about systems themselves and the
25 sophistication that they may have.

NEAL R. GROSS

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

1 MR. ARNDT: Yes.

2 MEMBER BONACA: And you focus, of course,
3 on the -- okay, I understand. Did we get a written
4 report from BNL?

5 MR. ARNDT: No.

6 MEMBER BONACA: No.

7 MR. ARNDT: That's still in draft form.

8 MEMBER BONACA: Okay.

9 MR. ARNDT: When it's available, we will
10 forward it to you.

11 Quickly, the other programs are focused on
12 providing the traditional information in these areas.
13 We'll talk about them very briefly. We're running a
14 little late on this.

15 We've talked about a lot of this, but let
16 me go through this quickly. The modeling issues that
17 we're facing -- the state of the practice now -- have
18 to do with issues of what kind of failure modes do you
19 include, how do you know you have all of the failure
20 modes, have you done a failure mode effects analysis,
21 and it has what kind of systems, the level of detail
22 of the models, both the software and the hardware, is
23 processor level sufficient, do you need to go lower
24 than that.

25 The big issue, of course, is: can you

1 treat hardware and software independently or not? To
2 a certain extent, that's a bit of a red herring,
3 because you -- you always have to treat software, to
4 some extent, dependent on hardware because software
5 doesn't exist in isolation of what the system is
6 running on. But can you separate it from an analysis
7 standpoint?

8 And software diversity issues, of course,
9 is a big issue. How diverse really is this software?
10 How do you ensure diversity and things like that? The
11 whole issue of the number of possible states and space
12 proliferation. Although some of the more
13 sophisticated stratified testing has dealt with this,
14 there's not as much need to anymore.

15 The requirements -- what is the ability to
16 predict? How do you demonstrate that the analysis is
17 really predicting the real failure? And what kind of
18 validation studies are necessary? And things like
19 that. And is it at least supportive or at least
20 consistent with what data is available?

21 MR. WHITE: I'm sorry to interrupt you.
22 But on software diversity, as you will remember, on
23 the National Academy panel we spent months wrestling
24 with that. Where is your program on the issue of
25 maybe having to write the requirements in a different

NEAL R. GROSS

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

1 way to assure that you get software diversity?

2 You know, the argument that Nancy Levenson
3 was putting forth is, if you and I sit down with the
4 same requirements and write software, we're going to
5 make the same mistakes regardless if you use one
6 language and I use another language.

7 And we just didn't have time to -- to
8 wrestle that particular concern to ground. Are you
9 going to address that today, or could you just give me
10 a quick summary of where you are?

11 MR. ARNDT: We're not planning on
12 addressing that particular issue today. But as you
13 point out, that is an issue. There has been several
14 actual studies done in the last few years specifically
15 looking at that particular issue. Are you going to
16 use different languages and different databases, and
17 things like that? And the real solution that has been
18 proposed that I am aware of is basically enforced
19 diversity basically.

20 You don't just put two people in a room
21 and tell them to go use different methodologies. You
22 force them to use a different methodology. And that,
23 I believe, is the state of the practice for that
24 particular issue.

25 As we've talked about, there are various

NEAL R. GROSS

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

1 methods available that have been used -- are being
2 used. I'll talk a little bit more about what the
3 current state of the practice is. But the real issue
4 is, as we've talked about, is setting an acceptance
5 criteria for both the modeling fidelity and the system
6 reliability. That's the real challenge.

7 MEMBER APOSTOLAKIS: I guess Dr. Guarro is
8 the originator of the dynamic flow graph methodology,
9 and I have worked on it, too, so he and I will say
10 nothing when it comes to this.

11 (Laughter.)

12 MEMBER KRESS: That would be unusual.

13 MEMBER APOSTOLAKIS: Huh?

14 MEMBER KRESS: That will be unusual.

15 (Laughter.)

16 MR. ARNDT: A lot of the methods,
17 particularly the dynamic flow graph methodology, are
18 very powerful and effective in doing this kind of
19 analysis. Again, the challenge we have is setting a
20 threshold. What is acceptable?

21 The context we have --

22 MEMBER APOSTOLAKIS: When you comment on
23 DFM, I have to reply the way the French team replied
24 -- non salons il voltre repons. Nobody seems to know
25 French.

NEAL R. GROSS

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

1 MEMBER KRESS: Oh, yes. I knew what you
2 meant.

3 MEMBER ROSEN: I just don't understand it
4 with a Greek accent.

5 (Laughter.)

6 MEMBER APOSTOLAKIS: But that's how the
7 team said it.

8 (Laughter.)

9 MR. ARNDT: The background or context is
10 what's -- where we currently are. Most of the trial
11 methods that you see in nuclear space are using
12 methodologies that more theoreticians would have
13 serious problems with. The biggest particular issue
14 is treating software failures, in a modeling sense,
15 independent from hardware failures. That is a
16 significant problem.

17 Some methods are even not that
18 sophisticated. They use very simplistic bounding
19 analysis. That is to say, demonstrating that the
20 particular failure mode of a particular component is
21 no worse than its analog colleague without dealing
22 with issues associated with timing issues and
23 communications issues, and common mode issues, and
24 things like that.

25 Where we set the threshold in this area is

1 one of the reasons we're doing -- investigating
2 various methods to understand the advantages and
3 disadvantages.

4 MEMBER APOSTOLAKIS: But it's not always
5 the acceptability, though, Steve, isn't it? I mean,
6 if you first satisfy yourself that maybe by using two
7 or three methods you have identified the important
8 failure modes, without any attempt at quantifying,
9 that will be a major achievement.

10 MR. ARNDT: Yes.

11 MEMBER APOSTOLAKIS: Then you go to the
12 next level, which brings up risk acceptability, and so
13 on, where things are a little shakier there.

14 MR. ARNDT: Right.

15 MEMBER APOSTOLAKIS: So maybe the
16 separation should be always in our minds that certain
17 methods do a really job at identifying certain failure
18 modes, but there is another method that does a better
19 job for other failure modes.

20 And I think that's where a lot of the work
21 out in the literature is. And another thing that's
22 happening in the -- and I've seen it in other places
23 -- oh, we have to use a model for reliability of
24 software, and somebody I know is using this model.
25 So, and it was published in the proceeding, so this

NEAL R. GROSS

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

1 really must be good. Let's use it.

2 And you are actually evaluating
3 critically, I hope, the underlying assumptions for
4 each model, not just because somebody used it.

5 MR. ARNDT: Right.

6 MEMBER APOSTOLAKIS: Okay.

7 MR. ARNDT: What are the advantages --
8 what are the inherent limitations of the modeling
9 technique?

10 MEMBER APOSTOLAKIS: Right.

11 MR. ARNDT: What are acceptable
12 assumptions? What are unacceptable assumptions?
13 Those --

14 MEMBER APOSTOLAKIS: Yes.

15 MR. ARNDT: Those kinds of issues. For
16 example, as Steve mentioned, we can set a particular
17 methodology, or we can set a set of issues that have
18 to be addressed in whatever methodology that's been
19 put forth. We're currently going down the second
20 path, although we can certainly look at the first as
21 an alternative.

22 But the particular issue, particularly
23 when you start dealing with things like -- that are
24 not state of the practice models, is is it at that
25 threshold where it is dealing with the assumptions

NEAL R. GROSS

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

1 that it -- that it's making in a way that makes sense
2 and can be useful?

3 I'll go back to the first part of your
4 comment having to do with there are really two issues
5 dealing with failure modes and understanding them
6 better and understanding the more reliability and
7 failure-type issues as opposed to the PRA issues.
8 That is specifically what we're trying to -- we're
9 trying to both go down the path of risk-informing, but
10 also trying to make the current methodology a little
11 more realistic.

12 MEMBER APOSTOLAKIS: And I suspect you
13 will make the methodologies more quantifiable. I
14 suspect you will make much more progress on the
15 failure mode analysis than the quantification, which
16 will -- probably will be challenged more by the
17 reviewers than by us, of course, but --

18 DR. GUARRO: Steve, do you have any
19 activity, either ongoing or planned, to try to
20 determine whether in the context of the nuclear
21 industry this assumption of separating software from
22 hardware is a good one or bad? Because -- and I'm
23 asking this because some of the more spectacular
24 failures that have occurred in the aerospace industry
25 have occurred because the software was simply the

NEAL R. GROSS

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

1 messenger of the sign error.

2 So is that declared out of scope or --

3 MR. ARNDT: No, it is not. That is a
4 specific area that we are looking at. You'll hear Dr.
5 Johnson this afternoon -- this morning talking about
6 his methodology which, of course, doesn't make that
7 assumption. It looks at it in an integrated fashion.
8 But also in our review of the methodology it was done
9 by BNL, which we're going to talk about in a second,
10 as well as future work.

11 We're going to look at that -- those
12 specific kinds of assumptions. Can you make those
13 assumptions? If you make those assumptions, is there
14 any way to mitigate those assumptions? How you look
15 at something else that will catch some of those
16 issues.

17 What is the threshold, in essence, for an
18 acceptable model? And this is obviously one of the
19 big issues.

20 DR. GUARRO: Okay, thanks.

21 MEMBER ROSEN: Steve, I'm getting a little
22 troubled by one sense I'm getting, and maybe you can
23 help me understand it better.

24 MR. ARNDT: Okay.

25 MEMBER ROSEN: The sense is that we're

1 going to analyze this very hard problem and figure out
2 how to deal with it, and then overlay that
3 understanding with the risk approach. And it seems to
4 me that the risk approach itself has the power to make
5 your first problem easier. Let me explain.

6 If risk -- if you use the risk approach
7 integrated with the underlying assumptions, underlying
8 work you're doing in the static failure modes and
9 effect, you can say the risk approach brings in the
10 question of consequences. And if the consequences of
11 a failure of a particular set of software is very
12 limited, then you're almost done with the problem
13 before you have to get -- you don't have to solve it
14 from a first principle aspect.

15 If you can say, well, the worst that can
16 happen, for example, is it will trip main feedwater,
17 well, tripping main feedwater happens now, and it's --
18 you know, the plant will scram, and that's a
19 relatively benign event.

20 MR. ARNDT: Right.

21 MEMBER ROSEN: I mean, so you can use the
22 risk modeling --

23 MR. ARNDT: Yes.

24 MEMBER ROSEN: -- to make your first
25 problem easier.

1 MR. ARNDT: You can do it backwards,
2 basically.

3 MEMBER ROSEN: Yes.

4 MR. ARNDT: And that's actually the
5 fundamental concept behind most of the bounding
6 methods. They look at, if it fails anyway, is it
7 going to be --

8 MEMBER ROSEN: What kind of failure can it
9 make?

10 MR. ARNDT: What kind of failure can it
11 make? And will it be any worse than X? Analog
12 equivalent or the issue associated with it -- it won't
13 drive you to Part 1 under release or whatever.

14 MEMBER APOSTOLAKIS: Which is a fault tree
15 type analysis. You start with the consequence, and
16 you are asking yourself, now, how can the system, in
17 combination with the software, can take me there?

18 MR. ARNDT: Right.

19 MEMBER APOSTOLAKIS: Right?

20 MEMBER ROSEN: Well, I'm not sure exactly
21 that's what I meant. I was looking at thinking about
22 the software's function, saying if the worst that this
23 software can do, regardless if it just locks up, it
24 doesn't do anything, or it sends a signal, the worse
25 it can do -- the only wire it's got is to the main

NEAL R. GROSS

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

1 feed pump circuit.

2 MR. ARNDT: Right.

3 MEMBER ROSEN: Then, the worst that can
4 happen is I can -- my main feed pumps can go to full
5 speed, or they can go to zero speed I guess. There
6 aren't any other options, are there? And so -- and
7 both of those are okay, I mean, from the standpoint of
8 consequences.

9 MR. WHITE: Well, it's an interesting
10 perspective. The problem is that the software that
11 would, first of all, cause a failure of the main
12 feedwater pump, or indicate a failure of the main
13 feedwater pump, might also cause a failure in another
14 piece of software where the consequences would be more
15 important. That makes it a little more difficult
16 to --

17 MEMBER ROSEN: Well, I understand that
18 that may be the case in some software. But in -- for
19 the particular software you're looking at has the
20 feature that it can only affect what the main feed
21 pumps do or don't do. Then you have a much simpler
22 problem.

23 MR. ARNDT: Yes. And at the risk of being
24 difficult, that's one of the reasons why we're trying
25 to evaluate different kinds of methodologies for their

NEAL R. GROSS

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

1 acceptability for the particular application. If it's
2 an isolated system, it doesn't have any significant
3 impact on other systems, if you can model the software
4 in such a way that it doesn't have the kind of issues
5 that Jim brought up, then you can use a less
6 sophisticated model.

7 MEMBER ROSEN: That's my only point.

8 CHAIRMAN SIEBER: Well, but the software
9 really isn't written that way.

10 MR. ARNDT: In most cases that's correct.

11 CHAIRMAN SIEBER: For example, you may
12 have a software module that acts like a controller.
13 Okay? And then sitting someplace else is the contents
14 of the scaling manual that says, "Here's proportional
15 band, here's rate, here's reset," etcetera. And that
16 same model is used in 500 different applications, the
17 same piece of software.

18 So you really can't say that if the -- if
19 you have a software failure some device quits doing
20 its thing. It may be that every device in the plant
21 quits doing its thing. It would --

22 MEMBER KRESS: At the same time?

23 CHAIRMAN SIEBER: Yes, because it's the
24 same model.

25 MEMBER KRESS: Same input to each one of

NEAL R. GROSS

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

1 them.

2 CHAIRMAN SIEBER: Yes. And so if you
3 crash the model, or it has some kind of a hang-up loop
4 that's not available to do anything else. So to me I
5 think the problem is pretty complex for systems that
6 are designed that way.

7 Now, there are other systems that are
8 independent. And, you know, for the sake of diversity
9 they have separate trains with separate models using
10 different algorithms, and so forth. And we've seen
11 some examples within the last two years of -- some of
12 us -- of that kind of methodology. And maybe you can
13 comment on that.

14 MEMBER KRESS: I don't think looking at it
15 in a backwards way like that helps you a lot, because
16 you already their subsystems, that if they fail you're
17 in trouble, like the control systems, the scram
18 systems. If things don't work right, you've got a
19 problem.

20 MEMBER ROSEN: Well, you're talking about
21 the solid-state protection system, for instance, in a
22 Westinghouse plant. You can't --

23 MEMBER KRESS: So if there's -- so if
24 there is a number of systems like that that you
25 already know, you're going to need this information.

1 MEMBER ROSEN: Sure. I'm not saying that
2 you're not going to need this. I'm just saying
3 there's a class of problems where it might get
4 simpler, and you should think about those, too.

5 MR. ARNDT: Yes, absolutely.

6 The next part of the presentation is on
7 the BNL research. We're running a little late, so
8 I'll go through this reasonably quickly. The BNL
9 research was designed to basically look at the issues
10 from a more PRA standpoint as opposed to a digital
11 failure standpoint. Of course, they dealt with those
12 issues as well.

13 And they looked at strengths and
14 weaknesses of current models. They looked at what was
15 necessary to develop guidance in this area,
16 suggestions for improving the integration methods,
17 database failure type issues.

18 The reports that they're going to have
19 will include basically this information: the review
20 of the current models, list of issues associated with
21 probability failure, and some of the things we've
22 talked about already. Some of those were new issues.
23 Some validated what we already knew.

24 The draft interim review guidance that
25 we're going to use --

NEAL R. GROSS

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

1 MEMBER APOSTOLAKIS: So is BNL going also
2 to present, or this is it?

3 MR. ARNDT: This is it.

4 MEMBER APOSTOLAKIS: Okay. When will we
5 get the draft report? You said they are preparing a
6 draft report.

7 MR. ARNDT: It should be available fairly
8 soon.

9 MEMBER APOSTOLAKIS: You have to step to
10 the microphone and tell us who you are.

11 MR. OVERLAND: Dean Overland, Risk
12 Assessment Group in Research. The draft report will
13 be available -- I believe it should be available this
14 month, this upcoming month.

15 MEMBER ROSEN: From the PRA standpoint,
16 PRA Committee, that's what we want to see. That's how
17 we would --

18 MEMBER APOSTOLAKIS: Maybe we can have
19 another subcommittee meeting in the future to talk
20 about the risk aspects.

21 MR. ARNDT: Well, depending upon how
22 aggressive we are on the guidance, we may want to come
23 talk to you about that specifically anyway.

24 MEMBER APOSTOLAKIS: Well, you said that
25 this year you will develop a plan for the next several

1 years.

2 MR. ARNDT: Yes.

3 MEMBER APOSTOLAKIS: Like to have our
4 input.

5 MR. ARNDT: Yes.

6 MEMBER APOSTOLAKIS: So I guess in the
7 next several months we will have to write a letter.
8 Is that correct?

9 MR. ARNDT: It probably won't be several
10 months, but probably late summer by the time we
11 discuss it and get input from various --

12 MEMBER APOSTOLAKIS: So you will come to
13 us in the fall some time?

14 MR. ARNDT: Probably, yes.

15 MEMBER ROSEN: Well, George, don't you
16 think it would be better for -- once they get the
17 draft report, for them to review it internally rather
18 than just send it to us at the same time in parallel?
19 I don't think there's that --

20 MEMBER APOSTOLAKIS: I don't understand
21 what --

22 MEMBER ROSEN: Well, I would rather hear
23 from the staff about what they think about the BNL
24 report rather than being sent the BNL report and --

25 MEMBER APOSTOLAKIS: Well, let's get it

NEAL R. GROSS

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

1 first.

2 MEMBER ROSEN: -- alone and --

3 MEMBER APOSTOLAKIS: Oh, you are proposing
4 another subcommittee meeting?

5 MEMBER ROSEN: I'm proposing, yes, a
6 subcommittee meeting in which the staff and BNL come
7 together and say, "Here's the report we got three,
8 four months ago."

9 MEMBER APOSTOLAKIS: Because that's the
10 ultimate problem, actually. You're right.

11 MEMBER ROSEN: Right. And then -- and
12 here is -- at which point, you know, we get staff's
13 view as well, and then we write the letter.

14 MEMBER APOSTOLAKIS: So when do you think
15 that can be --

16 MR. ARNDT: Well, we're mixing apples and
17 oranges here. There is three issues that were talked
18 about. One is the BNL report specifically. That will
19 be available next month, and then what we're going to
20 do with it we'll figure out shortly thereafter.

21 The other issue is any guidance document
22 that we may develop, that will be a little bit longer
23 timeframe. The third thing is the staff plan for the
24 overall digital I&C program.

25 MEMBER APOSTOLAKIS: Right.

NEAL R. GROSS

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

1 MR. ARNDT: Which will be late summer.

2 MEMBER APOSTOLAKIS: Right.

3 MR. ARNDT: So we could combine these, we
4 could do them independently, whatever you guys think
5 is most appropriately -- appropriate.

6 MEMBER APOSTOLAKIS: Well, certainly from
7 past experience, I assume you would like to come and
8 brief us on what you are doing on the guidance --

9 MR. ARNDT: Yes.

10 MEMBER APOSTOLAKIS: -- before you finish
11 the guidance.

12 MR. ARNDT: Yes.

13 MEMBER APOSTOLAKIS: Get some ideas back
14 and forth, and so on. So that is one of the most
15 critical meetings we're supposed to -- we are going to
16 have.

17 MR. ARNDT: Right.

18 MEMBER APOSTOLAKIS: Why don't we leave it
19 up to you and our staff to arrange? Because the time
20 is short, actually. We can't have too many
21 subcommittee meetings. But we will have to judge --

22 MR. ARNDT: Okay.

23 MEMBER APOSTOLAKIS: My inclination is --
24 would not be to do all three in one subcommittee
25 meeting.

NEAL R. GROSS

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

1 MR. ARNDT: Okay. I agree. It's, one,
2 too much material, and they are different aspects of
3 the issue.

4 MEMBER APOSTOLAKIS: Yes.

5 MR. ARNDT: Okay. One of the areas was
6 the interim guidance. Basically, it identifies
7 particular needs in the review and makes information
8 -- makes use of some of the information that they
9 generated when they did an evaluation of one of the
10 generic platforms.

11 As you all know, or should remember, there
12 are three generically approved digital platforms.
13 These are most likely going to be the basis for most
14 of the safety grade upgrades in the plants in the
15 future. Brookhaven used one of those generic
16 platforms in its work.

17 MEMBER APOSTOLAKIS: Now, I'm a little
18 curious, because I wasn't involved in the approval.
19 How did the NRC approve those platforms? I mean, was
20 it -- did they do any of this, the stuff that you
21 presented to us the last hour and a half?

22 MR. ARNDT: They used the current version
23 of the standard review plan, which, as we discussed --

24 MEMBER APOSTOLAKIS: Okay.

25 MR. ARNDT: -- is primarily qualitative.

NEAL R. GROSS

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

1 MEMBER APOSTOLAKIS: Process-oriented.

2 MR. ARNDT: Process-oriented, yes.

3 MEMBER APOSTOLAKIS: Now --

4 MR. ARNDT: Now, they're going to do
5 another plant-specific review when the plants use the
6 generic platforms for plant-specific application.

7 MEMBER APOSTOLAKIS: Well, that would be
8 more limited, then, because you have already approved
9 the platform. It's like approving AP1000, the design,
10 and then somebody actually builds it. You don't start
11 from scratch, right?

12 MR. ARNDT: No, you don't start from
13 scratch, but I would -- I would caution to say
14 limited. It's going to be a fairly extensive review.

15 MEMBER APOSTOLAKIS: Okay.

16 MR. ARNDT: And we're hoping to have some
17 of these tools available to at least inform those
18 reviews.

19 MEMBER APOSTOLAKIS: Processes.

20 MR. ARNDT: As part of BNL's work to
21 develop the guidance, they did some quantitative
22 assessments. They looked at analysis. They looked at
23 the initiating events, particularly the differences in
24 initiating events from a traditional --

25 MEMBER APOSTOLAKIS: This is too exciting,

NEAL R. GROSS

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

1 Steve. You're really giving us stuff that is really
2 very interesting, but we're not going to talk about
3 it. So why don't you skip it?

4 MR. ARNDT: Okay.

5 MEMBER APOSTOLAKIS: I mean, you are
6 talking about new initiating events. I'm dying to see
7 what they've done. And you say, "No, no, no, you're
8 not going to see it." So keep going, then.

9 CHAIRMAN SIEBER: Well, before we go too
10 far, we would like to take a break this morning. When
11 is a good place for you to stop to allow us to take
12 that break?

13 MR. ARNDT: This is probably as good a
14 time as any.

15 CHAIRMAN SIEBER: That's what I was
16 thinking.

17 (Laughter.)

18 Why don't we take a break until quarter
19 after 10:00.

20 (Whereupon, the proceedings in the
21 foregoing matter went off the record at
22 9:55 a.m. and went back on the record at
23 10:15 a.m.)

24 CHAIRMAN SIEBER: Okay. Let us return to
25 session.

1 MR. ARNDT: Thank you, Mr. Chairman.

2 When we left, I had just started a brief
3 description of the BNL work. As we're running a
4 little late, I will try and work through that fairly
5 quickly.

6 As part of their review, they looked at
7 both state-of-the-art issues and modeling issues.
8 Some of the issues that they looked at in the
9 development of the guidance we talked about. They
10 also looked at software failure issues, both the whole
11 issue of whether or not probabilistic modeling is
12 appropriate, as we have discussed previously, for
13 software failures independent of hardware.

14 The various kinds of models were looked
15 at, as well as the common cause failure issues for
16 software. They looked at hardware failures,
17 particularly the issues associated at what level of
18 component failures needs to be modeled in an
19 appropriate model, as well as the issues associated
20 with failure data for hardware systems, common cause
21 hardware failures, particularly things like
22 communication buses and things like that that can have
23 potential issues, software-hardware interactions,
24 which are a particular issue, and then the integration
25 of the digital systems within existing PRAs.

NEAL R. GROSS

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

1 One of the challenges of this methodology
2 is there is a lot of fairly sophisticated methodology,
3 some of which are easy to integrate into static PRAs
4 and some of which are not very easy to integrate into
5 static PRAs. And --

6 MEMBER ROSEN: The question here is: if
7 a plant -- an existing plant with an existing PRA
8 chooses to make a safety-related system improvement
9 using digital software --

10 MR. ARNDT: Right.

11 MEMBER ROSEN: -- how does one then
12 incorporate that into the model to answer the question
13 as to what happens to the CDF --

14 MR. ARNDT: Right.

15 MEMBER ROSEN: -- to the whole plant?
16 That's the question I have.

17 MR. ARNDT: That is -- the primary issue
18 in the bullet referred to as integration of -- into
19 the existing models.

20 MEMBER ROSEN: Okay. So you're going to
21 -- somebody is going to answer that question for me.
22 I'm not smart enough to answer it. I just want the
23 world to answer it.

24 MR. ARNDT: That is one of the issues, and
25 there are methods that have been proposed. For

NEAL R. GROSS

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

1 example, dynamic fault trees and Markov models can be
2 integrated into static PRA or the whole PRA can be
3 turned into a dynamic fault tree and then integrated.

4 Those are not easy things to do, but they
5 are theoretically possible. Obviously, there are
6 other methodologies that can be developed. You can
7 use them as an input to a particular failure rate that
8 then goes into this an initiating event, upfront
9 module, ahead of the initiating event.

10 MEMBER ROSEN: Right. Events

11 MR. ARNDT: Events.

12 MEMBER ROSEN: Not much one.

13 MR. ARNDT: Multiple events. There are
14 several different methodologies that have been
15 proposed and have been worked on. NASA, for example,
16 has done a lot of work on dynamic fault trees for
17 these kinds of issues. So there is examples in the
18 literature on how to do this.

19 MEMBER ROSEN: Dealing with the issue of
20 the fault tree is what fails first, and then assess
21 how the system reacts to it, or the system has an
22 upset of some kind --

23 MR. ARNDT: Right.

24 MEMBER ROSEN: -- and the fault failure --
25 software fails during the upset.

NEAL R. GROSS

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

1 MR. ARNDT: Right.

2 MEMBER ROSEN: Or -- so, I mean, both of
3 those issues.

4 MR. ARNDT: Right. Both of those issues,
5 and the issue of, in the particular model that you're
6 using, is issues particularly common with failure is
7 the model you're going to use capturing all of the
8 common mode failures of a software-driven system.

9 MEMBER ROSEN: The most challenging piece
10 of it seems to me to be that if the software system
11 fails first, it would initiate the transient, and
12 you're relying on the same software system to mitigate
13 the occurrence that it just initiated.

14 MR. ARNDT: That's right. And on top of
15 that, one of my personal pet peeves is there have been
16 failures in which not only are you counting on it to
17 mitigate it, but also the failure prevents you from
18 doing other things that might mitigate it, like, for
19 example, it locks out the manual action, things like
20 that, which is both difficult to model but potentially
21 very significant from a consequence standpoint.

22 MEMBER ROSEN: Okay. I just checked to
23 make sure the scope of what you're addressing is
24 something like what I hope you're addressing. I think
25 I got the answer yes.

1 MR. ARNDT: It looked at a variety of
2 methodologies -- for example, the fault tree analysis
3 for AP6000, the INEL study, the work that Barry is
4 doing in fault injection methodologies that uses
5 Markov models.

6 They looked at some of the other guidance
7 that is out there and that has been proposed. The
8 Bayesian belief network, which is a methodology that
9 some of you are familiar with that is very useful for
10 combining qualitative and quantitative data to provide
11 information to basically make a decision.

12 We're also investigating this on a
13 separate project, both from a reliability standpoint
14 but more importantly for improving the review process.
15 As we get more quantitative information, how do we
16 integrate that into our current qualitative programs?

17 And as part of their work, they did a
18 failure modes and effects analysis for one of the
19 generically approved platforms, to understand how this
20 can be done and what the appropriate level of modeling
21 should be.

22 The did the traditional top-down step-by-
23 step approach, identified the potential dependencies,
24 and generated the questions about the particular
25 design that you would have to answer to do an

NEAL R. GROSS

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

1 effective analysis.

2 And that's one of the big issues, because
3 when -- if you're going to do more detailed modeling,
4 you're going to need more information, or in some
5 cases different information than you would ask if
6 you're going to do a process-based analysis.

7 Some of the insights they got when they
8 did that, in order to capture the information you
9 basically have to do what you would do in any
10 probabilistic model. You have to have a very detailed
11 understanding of how the system fails, which we
12 discussed that previously.

13 And you have to have a generic method for
14 evaluating various kinds of issues, such as
15 communication between redundant channels as an
16 example. You have to figure out how you're going to
17 do that and have an agreed-upon method to do that.

18 Another part of the review -- we asked
19 them to go and look at the databases that are
20 available, both within the nuclear industry and in
21 other industries. One of the things they did was they
22 looked at the LER work. There is a large number of
23 failures in the LER database, and many of them are
24 digital systems or software-based systems.

25 One of the biggest issues with that

NEAL R. GROSS

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

1 database, not only for this application but for other
2 applications, is the amount of information you have.
3 And that's one of the biggest challenges in the
4 digital failure databases is frequently, one, the
5 people who have the failure data may not populate it
6 into the database.

7 But also, they may not have it, because
8 the solution was a card failed, we pulled it out, we
9 put a new card in. And exactly what failed, how it
10 failed, and what the root cause of that was may not
11 exist, or may not be populated in the database. So
12 that's one of the significant challenges.

13 MEMBER ROSEN: Now, there are plants that
14 are repairing cards.

15 MR. ARNDT: That's correct.

16 MEMBER ROSEN: And those people know what
17 failed on the cards. And they can then tell you or
18 give you access to data which would let you know what
19 that failure did.

20 MR. ARNDT: That's correct.

21 MEMBER ROSEN: If you know that this
22 electrolytic capacitor, for example, failed on the
23 card, because it was replaced and the card worked --

24 MR. ARNDT: Right.

25 MEMBER ROSEN: -- then you know a lot more

NEAL R. GROSS

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

1 than -- and so one of the threads you might try to
2 pull is, where are places that are repairing digital
3 cards? Because they will have data that will be
4 useful to you, and may be willing to share it.

5 MR. ARNDT: Yes. And the biggest
6 challenge in all of this is going out and pulling all
7 of those threads, or finding other people who have
8 pulled them before and building them on, as George
9 mentioned, what people have done, what information is
10 available.

11 One of the reasons we asked BNL to do this
12 was to get a better understanding of not only what is
13 and is not available but what people are doing with
14 it. They reviewed the MIL handbook data, PRISM data.
15 They looked at other sources that could be pursued,
16 other industries and government agencies,
17 manufacturers, and remanufacturers in the case of
18 cards.

19 MEMBER APOSTOLAKIS: NUREG 6734 is what?
20 Is it the data?

21 MR. ARNDT: Yes.

22 MEMBER APOSTOLAKIS: Can we get a copy of
23 that?

24 MR. ARNDT: I think so. I'd have to go
25 and --

1 MEMBER APOSTOLAKIS: Well --

2 MEMBER ROSEN: One minute. I don't think
3 -- maybe we're not communicating yet.

4 MR. ARNDT: Okay.

5 MEMBER ROSEN: You said remanufacturers.
6 Sure, but I was talking about utilities, maintenance
7 staffs, I&C maintenance staffs, that are repairing
8 their own cards.

9 MR. ARNDT: Yes.

10 MEMBER ROSEN: Those people will be a
11 great source of data.

12 MR. ARNDT: Yes.

13 MEMBER ROSEN: So I just wanted to make
14 sure you understood what I meant.

15 MR. ARNDT: Okay. Yes, I understood. I
16 was remembering different -- yes, sir.

17 DR. GUARRO: Just curious -- what were you
18 looking into in the review of 217?

19 MR. ARNDT: I'm going to have to defer
20 that question to one of our contractors who is in the
21 audience.

22 MR. CHUN: This is Lewis Chun, Brookhaven
23 Lab. Mainly we got hold of the 217 and see what
24 information is there, and see how people use the
25 method provided there in their analysis. Basically,

NEAL R. GROSS

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

1 it's part -- part stress method they use, and then the
2 PRISM database is kind of a replacement database that
3 -- because 217, my understanding, was discontinued,
4 and the PRISM is kind of like replacement, which keep
5 updating the data in the database.

6 DR. GUARRO: Well, yes. The direction of
7 my question was two ways. In 217, there is nothing
8 that is software-specific. I was wondering how that
9 will apply to the --

10 MR. CHUN: Right. It's lumped -- if you
11 look --

12 DR. GUARRO: Also, yes, it is true that it
13 has not been updated since 1991. So it's very old
14 data, in any case. PRISM is an evolution, but it's
15 also now no longer a government-endorsed database. So
16 it -- the usefulness of it is sometimes questioned.

17 MR. CHUN: We look at it as just another
18 source of data, and it's somewhat like a continuation
19 of 217. But the method there is still similar to that
20 of 217, so in terms of software failure I think it is
21 embedded in the failure events that they use in
22 estimating the failure rates.

23 DR. GUARRO: Okay. Thanks.

24 MR. CHUN: How adequate that is, you know,
25 is questionable.

1 MEMBER APOSTOLAKIS: What kind of events
2 are these? I'm not familiar with 217. Is it
3 aerospace, or what?

4 DR. GUARRO: 217 is an electronic
5 component failure rate database.

6 MEMBER APOSTOLAKIS: Who developed it?

7 DR. GUARRO: The Department of Defense.

8 MEMBER APOSTOLAKIS: Okay.

9 MR. ARNDT: It was across --

10 DR. GUARRO: It was one of the MIL
11 Standards that was discontinued in the acquisition
12 reform era in the '90s.

13 MR. ARNDT: The primary idea is not only
14 looking at what's available, but what are the
15 underlying assumptions in the databases that are
16 available. So understanding what's in there, both
17 what you can use and what you can't use.

18 As Professor Guarro said, that particular
19 one is not particularly useful for the regulations.

20 We looked at both significant major type
21 issues, like the Airbus crash and the Therac and other
22 large issues, but also looked at what information
23 we've been able to derive so far in various studies.
24 There have been some limited studies over the last
25 five or six years, but look at information from

NEAL R. GROSS

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

1 available sources.

2 This particular analysis looked at all of
3 the different LERs in this timeframe and tried to comb
4 out what failures were digital system failures and try
5 to attribute some level of consequence associated with
6 them, to give us a perspective in dealing with --

7 MEMBER APOSTOLAKIS: So these reactor
8 trips were spurious reactor trips I hope.

9 MR. ARNDT: Yes. So --

10 CHAIRMAN SIEBER: Well, I wonder about
11 that data, since there aren't very many digital
12 systems in existing powerplants right now. That seems
13 very high.

14 MR. ARNDT: Well, yes, that -- that is
15 correct. The issue you have to understand is, because
16 of the level of detail of the information here, that
17 particular study was done in such a way to be
18 inclusive. So if, for example, the LER discussed
19 potential application or potential root cause, and if
20 any of the root causes included a digital system, then
21 it was included as a potential failure.

22 So how do I put this to give you a
23 perspective? The idea of this particular study was to
24 try and scope the issue. Are there cases where we're
25 getting spurious drips or initiating events associated

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 with digital systems?

2 So the input filter on this particular
3 study was not if this system didn't fail, would the
4 event have happened? It was, was there a digital
5 system involved in the initiating event? So it was a
6 broader --

7 CHAIRMAN SIEBER: Whether it failed or
8 not.

9 MR. ARNDT: Well, it had to have had an
10 impact on the failure. But it didn't have to be the
11 single initiating event was the failure of the digital
12 system.

13 CHAIRMAN SIEBER: Let's say a pressure
14 transducer failed and it failed high, which would
15 initiate a reactor trip. Would you call that a
16 digital system?

17 MR. ARNDT: If it was --

18 CHAIRMAN SIEBER: If the signal processing
19 was digital?

20 MR. ARNDT: In this study, yes.
21 Understand, this was a very generalized scoping-type
22 study, but it did -- the biggest issue is that the
23 LERs contain digital failures, and you can get some
24 information out of it, is the point you should take
25 away from this particular example.

NEAL R. GROSS

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

1 There is information -- one of the big
2 issues is it's difficult at the level of detail of
3 LERs to make that distinction, because that -- the
4 situation you just described may have been the event,
5 but the description in the LER might have been the
6 digital feedwater system failed.

7 The reason it failed -- it may have been
8 because the pressure transducer associated failed, but
9 we just didn't have that level of information in the
10 LER.

11 CHAIRMAN SIEBER: All right.

12 MR. WHITE: I think the Chairman has made
13 a very interesting point, and maybe you're mining this
14 data already. But one of the questions that leaps to
15 mind is, out of all the LERs you looked at how many of
16 those systems -- how many of those plants had digital
17 systems that could have contributed, so we could get
18 to the -- I think the point the Chairman was making.

19 Does it look like 20 percent of all the
20 digital systems that could cause failures have been
21 causing failures? Or 25 percent? Or five percent?
22 And I didn't know if you intended to look at that a
23 little -- have you already looked at it? And if not,
24 are you planning to?

25 MR. ARNDT: One of the studies that we did

1 was looking at, of these kind of failures, what
2 systems are failing, both slicing it -- associated
3 with the kinds of plants, the kinds of systems, and
4 things like that.

5 This data is a little bit old now, because
6 things are changing more rapidly now, so the
7 usefulness of this particular analysis is becoming
8 less and less effective, because these are mostly
9 older systems, many of which are starting to be
10 replaced now with newer digital systems.

11 But yes, that particular slicing of what
12 was failing, why -- what kinds of systems were
13 failing, were they safety systems or non-safety
14 systems, were they feedwater systems or other systems,
15 was done in this cut.

16 MEMBER ROSEN: Could you tell me a little
17 bit about Therac-25, 1985 to '87? Is that what --
18 what is -- I mean, the first bullet I don't understand
19 at all.

20 MR. ARNDT: The Therac system is a very
21 well-known digital system failure. It's not a real-
22 time system. It was a therapeutic irradiation system
23 in Canada. It is very well-known, one, because it
24 killed people, but, two, because it was a classic
25 example of a lot of the problems that hopefully have

NEAL R. GROSS

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

1 been solved by now in terms of software requirements
2 and not understanding software-hardware interaction,
3 and issues like that.

4 It was basically a software -- a set of
5 software that ran the therapeutic irradiation
6 device --

7 MEMBER ROSEN: Okay.

8 MR. ARNDT: -- that irradiated the
9 patients. And because of the way the software was
10 written, and particularly the way the software
11 revisions were done, had some inherent flaws in the
12 software. And as part of their revisions, they put
13 more and more safety functions into the software and
14 took them out of the hardware interlocks. And this is
15 a classic example of all of the bad things you can do
16 in software design, and it killed people. So that's
17 one of the more --

18 MEMBER ROSEN: Okay.

19 MR. ARNDT: -- significant events.

20 MEMBER APOSTOLAKIS: Did you discuss the
21 last bullet while I was out?

22 MR. ARNDT: Yes.

23 MEMBER APOSTOLAKIS: Poor timing.

24 MR. ARNDT: Again, we looked at --

25 MEMBER APOSTOLAKIS: But wouldn't that

1 argue against treating the software as a separate
2 entity with its own failure rate? I mean, you say it
3 was divided, so --

4 MR. ARNDT: Yes, it would.

5 MEMBER APOSTOLAKIS: It would.

6 MR. ARNDT: As we mentioned while you were
7 out, the study was limited, and the amount of
8 information you could obtain from it.

9 MEMBER APOSTOLAKIS: Okay.

10 MR. ARNDT: But yes.

11 CHAIRMAN SIEBER: It's not clear to me
12 that what you would get out of LERs you could even
13 tell whether it was hardware-software or human
14 interface.

15 MR. ARNDT: Again, as we discussed, what
16 we could tell gave us that -- it was a limited study,
17 one, because of the timing --

18 CHAIRMAN SIEBER: Okay.

19 MR. ARNDT: -- of the dates we looked at,
20 as well as the amount of information you can get.

21 CHAIRMAN SIEBER: Okay.

22 MR. ARNDT: This is basically just a
23 discussion, again, of what kind of things we were
24 looking at for the larger databases. The point in
25 particular is that these databases make certain

NEAL R. GROSS

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

1 assumptions about the data that's in them.

2 And one of the biggest issues with using
3 these data, or other databases, is you really have to
4 understand the assumptions associated with it, because
5 they're making estimations and they're making
6 assumptions based on a particular model in mind in
7 most cases, be it a reliability growth model or a
8 straight amount of failures per time in service, or
9 whatever.

10 And one of the biggest challenges in
11 gathering and combining data is understanding these
12 issues and being able to deal with them.

13 MEMBER APOSTOLAKIS: How extensive is the
14 review that something like ISO 9000 gets? I mean, is
15 it something that has been really reviewed by
16 competent people so I can -- we should take it
17 seriously? Or is it something that some committee
18 somewhere developed?

19 I mean, certification to estimate software
20 mean-time to failure -- wow. That assumes that there
21 is such a thing as a mean-time to failure.

22 MR. ARNDT: Yes.

23 MEMBER APOSTOLAKIS: There is such a thing
24 as a reliability growth model. Has anybody questioned
25 those things? Have they convinced themselves that,

NEAL R. GROSS

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

1 yes, this is a reasonable thing to do?

2 MR. ARNDT: The short answer to that
3 question is yes.

4 MEMBER APOSTOLAKIS: Well --

5 MR. ARNDT: The longer answer, and
6 probably more appropriate answer, is that the people
7 who are using the particular model -- in the case of
8 the ISO 9000 software model or the capability maturity
9 model for -- or whatever model they're using, are by
10 and large people who have a similar application
11 background, are doing it for a particular reason. And
12 they have convinced themselves that for the particular
13 application that they're using it's acceptable.

14 As you'll recall when we briefed a couple
15 of months ago about the validation and verification
16 program, there is a lot of different verification and
17 validation programs out there. The one that the NRC
18 endorses for real-time systems is the IEEE 1012, which
19 is -- with the various levels, which we basically say
20 for a real-time system has to be at the highest level.

21 But there's a lot of other people out
22 there that do this work at different levels using
23 different methods, and for the particular application
24 that they are working with they are -- they have
25 convinced themselves, either by standards committees

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 or by regulation in a particular domain, that they're
2 comfortable with this particular model.

3 MEMBER APOSTOLAKIS: Okay.

4 DR. GUARRO: In the review of major
5 software-induced or related failures, have you looked
6 at the ones that have occurred in the space systems?
7 Recently -- there was a string of recent -- recent
8 ones, in '98/'99 timeframe.

9 MR. ARNDT: I don't believe that was part
10 of our review.

11 MEMBER BONACA: Was it in the United
12 States, Sergio?

13 DR. GUARRO: Delta -- the Delta 3, first
14 flight; the Titan 4, 820 flight; and then a couple of
15 spacecraft failures. And they -- some of those were
16 -- as was mentioned before, you know, the software was
17 the messenger of a serious design problem. A couple
18 of those were actually errors in entering parameters.
19 So there is quite a bit of interesting material there
20 to look at.

21 MEMBER KRESS: Are we going to hear a
22 discussion on the concept of mean-time failure for
23 software? Because I was under the impression that
24 that's predicated on the basis of random failures, and
25 a question I would have is: how do we attribute

NEAL R. GROSS

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

1 random failures to software? And --

2 MR. ARNDT: I wasn't planning on going
3 into a detailed discussion of that particular issue,
4 beyond the issue that to do that kind of analysis you
5 have to make the assumption, one, that that makes
6 sense, and that you can come up with a failure rate,
7 if you will, for software. And there is argument in
8 the field associated with whether or not that makes
9 any sense.

10 It basically comes down to the fact: can
11 you model software in that way? From a theoretical
12 standpoint, it's pretty obvious that software doesn't
13 have a failure rate. But the real issue is: can you
14 model it that way in a meaningful way, and treat it
15 separately in a fault tree analysis or some other
16 analysis?

17 MEMBER APOSTOLAKIS: Won't later
18 presentations address this?

19 MR. ARNDT: It will address it to some
20 extent, yes.

21 MEMBER APOSTOLAKIS: Yes. So maybe we can
22 -- yes.

23 MR. ARNDT: Again, the assumptions in the
24 actual data is a particular issue. For example, we
25 talked about earlier fault tolerant systems, which is

NEAL R. GROSS

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

1 an important understanding of how it fails or doesn't
2 fail or gets -- it is -- you're not going to see that
3 in most databases, because it either fails or it
4 doesn't fail, and that's what in the system.

5 Redundant channels, the same kinds of
6 issues. In a lot of failure databases you cannot
7 extract that level of information. It's one of the
8 reasons that looking at -- sorry.

9 MEMBER ROSEN: I wanted to -- go ahead,
10 finish your thought. But I wanted to ask another
11 question about the prior slide -- 44.

12 MR. ARNDT: One of the things that we're
13 trying to evaluate is whether or not it makes sense to
14 have a real-time nuclear-specific database that
15 addresses the specific issues we have -- whether that
16 is a meaningful, cost-effective, rational thing to do.

17 MEMBER ROSEN: This first bullet under the
18 -- on this slide, the failure rates were estimated by
19 dividing the number of reported failures by the total
20 operating time, it can give you a lower bound, but
21 it's surely not, you know --

22 MR. ARNDT: Right.

23 MEMBER ROSEN: -- there's lots of other
24 failures that --

25 MR. ARNDT: Right.

1 MEMBER ROSEN: -- that happen that are
2 just simply not in the database. So if you treat that
3 as a lower bound that's okay. But otherwise, you're
4 making a mistake.

5 MR. ARNDT: Yes. And the point here is
6 you have to understand these underlying assumptions to
7 be able to utilize the data.

8 The tentative findings from their review
9 basically are things that we've talked about before.
10 Quantitative methods for assessing software failure is
11 something that works, that we need to be able to deal
12 with this.

13 One particular methodology that they
14 looked at was a Markov modeling at the processor
15 level, and the idea was: is that an acceptable
16 standard to put -- draw your line at? Is that good
17 enough?

18 Looking at the fact that, of course,
19 probably that level of detailed analysis of failure
20 modes to be able to support the analysis from a PRA
21 standpoint -- it goes back to the concept that just
22 having a failure rate doesn't necessarily make the
23 model work. You have to understand -- you have to
24 have the deterministic analysis of how it fails, and
25 things like that, to be able to support it.

NEAL R. GROSS

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

1 And, of course, data is needed to really
2 understand this, to be able to model these kinds of
3 issues.

4 MEMBER APOSTOLAKIS: So there is a
5 conclusion, then, that the concept of a failure rate
6 is meaningful here.

7 MR. ARNDT: It can be meaningful.

8 MEMBER APOSTOLAKIS: Well, I guess that's
9 a major issue. Sometime we have to discuss this. I
10 don't know whether it's today or some other day.

11 MR. ARNDT: If we have not discussed it
12 appropriately by the end of today, the we'll revisit
13 it.

14 MEMBER KRESS: Is that failure rate driven
15 by the rate at which the input carries the software
16 into some error mode? And it's really the rate at
17 which the software -- the input --

18 MR. ARNDT: It can be looked at in a
19 number of ways. That's one way of looking at it. The
20 likelihood that given the operational parameters that
21 it's --

22 MEMBER KRESS: But you will enter into a
23 combination of inputs that --

24 MR. ARNDT: Right.

25 MEMBER KRESS: -- exercises some part of

NEAL R. GROSS

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

1 the software that has an error in it.

2 MR. ARNDT: Right. And that's why I
3 mentioned earlier software failure probability, in and
4 of itself, is something of a misnomer, as George has
5 pointed out many times, because software has to run on
6 something. I mean, it can't independently do that.

7 The issue is: can you --

8 MEMBER KRESS: It seems like a real
9 stretch to consider that as a random failure.

10 MR. ARNDT: Right. And can you model it
11 -- one of the big issues is: can you model that
12 independently of its software -- hardware
13 interactions? It means you have hardware failures,
14 you have software failures in that -- the operational
15 condition on the hardware has exercised a software
16 failure, and then you have the interactions between
17 hardware failures and software failures, which,
18 depending upon what model you use, can be modeled
19 separately or can't be modeled separately.

20 And one of the things we found,
21 particularly in Dr. Johnson's work, is that a lot of
22 their bad failures are exactly that. It's the
23 interaction between hardware and software failures.

24 Let me quickly go through some of the
25 other work we're doing. We have two other database

NEAL R. GROSS

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

1 efforts. One is the international effort to develop
2 a software -- develop a database of -- and this is
3 actually a typo. It should be computer -- software-
4 driven computer system failures. It's not just
5 software failures. It's all failures in systems
6 driven by software in the nuclear industry.

7 And this is what I mentioned a minute or
8 two ago. We're currently evaluating whether it makes
9 sense to have a nuclear domain specific database with
10 all of the kinds of information that you need to be
11 able to make rational judgments.

12 MEMBER KRESS: Is this being done under
13 the --

14 MR. ARNDT: This is being done under the
15 auspices of NEA.

16 MEMBER KRESS: NEA. Okay.

17 MR. ARNDT: It's a CSNI project.

18 MEMBER KRESS: Yes.

19 MEMBER APOSTOLAKIS: So you are a member
20 of that?

21 MR. ARNDT: I am actually the Chairman of
22 it.

23 MEMBER APOSTOLAKIS: The Chairman.

24 MR. ARNDT: And this is actually Computer
25 Systems Important to Safety. This is the

NEAL R. GROSS

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

1 abbreviation.

2 We also started an in-house effort to do
3 this. Depending upon where we go in the future -- and
4 that will be decided this year when we redo our
5 research plan -- my guess is we're probably going to
6 fold this either into the Brookhaven effort or the
7 COMPSIS effort. But we have an in-house effort to
8 look specifically at the data.

9 There are several other efforts going on.
10 The committee is very aware of the Halden research
11 program. That's a collaborative NEA program that
12 looks at a whole bunch of different issues -- human
13 reliability, human factors, fuels, materials. They
14 also have a piece in digital system safety.

15 And in the last two or three years they
16 have expanded their digital system safety research
17 program extensively. One piece of that is a
18 reliability program, and they are particularly looking
19 at risk assessment of COTS systems and how do you deal
20 with the fact that it's a black box and you can't get
21 at the information, and things like that, what kind of
22 models can be used.

23 Human system interface issues dealing with
24 software and these things in an integrated fashion --
25 they, of course, have done a lot of work in human

1 reliability and human factors. So that's a natural
2 fit for them.

3 And the last of their major programs is
4 the Bayesian belief network to help integrate systems,
5 and that's the one we're dealing with.

6 MR. WHITE: Excuse me, Steve. This is an
7 example of one of the concerns we had in the National
8 Academy study, and you may have -- you may have
9 alleviated a concern. But the concern that the panel
10 had is that a lot of really interesting work and work
11 that could be very influential in what you do was not
12 subjected to peer review, and it was back to the old
13 concern of the nuclear industry just talking among
14 itself.

15 So have you made much progress in that
16 area of getting more open review of the Halden work?

17 MR. ARNDT: That, as you mentioned, has
18 been an open issue throughout the work. We are trying
19 a lot -- not only in this work, but all of the work in
20 the I&C area, to do more of that. And Carol and Barry
21 will mention that in their presentations, and I'm
22 trying to get out there more and our other researchers
23 are.

24 In the case of the Halden work, in
25 particular -- this is a challenge because of the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 proprietary nature of their reports. However, they
2 have made a specific conscious decision at the last --
3 I guess two years ago management meeting to do more
4 peer reviewed literature work.

5 They've made progress. Is it as much as
6 I would like? No. But they have made progress in
7 doing that work. They are publishing certainly a lot
8 more in peer reviewed proceedings, in the journals not
9 as much as I would like, but they are making progress.
10 At least they're doing much more in peer reviewed
11 proceedings to both put out the work they're doing and
12 also get feedback on the work they're doing.

13 MR. SYKES: I have a question.

14 MR. ARNDT: Yes, sir.

15 MR. SYKES: Before you showed us that
16 eight percent of LER contained digital I&C failures,
17 and nine percent of our PS. And that was for a period
18 of time '94 to '98. Do you have a sense that there is
19 a trend of decreasing failures in digital systems?

20 MR. ARNDT: In that study, we tried to
21 look at that particular issue. And we actually -- one
22 of the things we tried to look at was how recent was
23 the system implemented.

24 MR. SYKES: Okay.

25 MR. ARNDT: We didn't get -- we weren't

1 able to get a statistically significant interpretation
2 one way or the other.

3 MR. SYKES: Okay.

4 MR. ARNDT: The anecdotal data from
5 reading the LERS was that that was the case. When a
6 new system was introduced, the failures were high for
7 a period, and then they started reducing. But we
8 didn't have a statistically significant amount of
9 information to make that determination.

10 The issue, of course, is more complicated
11 than that, of course, because analog systems tend to
12 have a much longer lifetime in the plant. The systems
13 that we actually were studying in that time period are
14 already starting to be ripped out and replaced with
15 newer digital systems.

16 So it is comforting to know that as we get
17 more experience with these systems that their failure
18 appear to be being reduced. The mitigating issue is
19 that their lifetime in the plant tends to be much
20 shorter than previous systems.

21 This is just a quick other effort we're
22 --we've been asked to -- the Committee for Safety of
23 Nuclear Installations is becoming more interested in
24 this area, and they're talking about having a new
25 working group in this area or more international work

NEAL R. GROSS

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

1 in this area.

2 The NRC is also holding discussions about
3 starting an international program in this area,
4 similar to camp or something like that. So we're
5 continuing to work both externally in other industries
6 but also internationally within the nuclear industry.

7 This is just a quick summary of what I
8 said. It's basically a reiteration of the -- what I
9 hoped would be the conclusions.

10 We have various programs in this area.
11 We're looking at various aspects -- data, guidance,
12 failure methods, and reliability. We're working on
13 the development, and you're going to hear more about
14 this from Barry and Carol.

15 The U.S. industry is moving in this
16 direction to say ahead of that. This, of course, is
17 an open debate. We believe that the methodology is
18 such that we can make assessments that are
19 sufficiently mature. Hopefully, by the end of the day
20 you will have more information to agree or disagree
21 with that.

22 There are significant strengths and
23 weaknesses of the current methodology -- what's being
24 used there, as well as the issues that we're
25 proposing. Our future work is going to be looking at

NEAL R. GROSS

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

1 the actual integration type issues, as well as
2 development of testing methodologies.

3 One of the biggest issues, as I think was
4 discussed earlier, is because this has not been used
5 extensively in the nuclear domain, we need to validate
6 the models as we develop them, at least as well as we
7 can based on the available data.

8 Additional data, additional coordination
9 is something that we need to continue to do.

10 MEMBER ROSEN: Are you thinking about
11 ultimately having a pilot with somebody to -- who has
12 an existing plant and PRA and might be willing to at
13 least try to put into a research version of the model
14 -- obviously, not the model they're using for plant,
15 but, you know, put a Rev model out there for research
16 and try to do some digital systems stuff in it?

17 MR. ARNDT: One of -- you'll hear later
18 today what we're doing in our validation work is
19 actually using real nuclear applications in our
20 validations. We did a study on the Calvert Cliffs
21 feedwater system, the actual system that they're
22 using. We're looking at some -- several other
23 programs to test the methods using nuclear-specific
24 applications.

25 The second half of your question is the

1 actual application of that to a regulatory structure,
2 and we're not that far down that path.

3 MEMBER ROSEN: Well, I'm not thinking so
4 much about a regulatory structure. I was thinking
5 about once you get some ways to integrate digital
6 system reliability into PRAs that you think are
7 doable --

8 MR. ARNDT: Right, yes.

9 MEMBER ROSEN: -- to find someone who is
10 willing to work with you --

11 MR. ARNDT: Oh, yes.

12 MEMBER ROSEN: -- in the existing industry
13 to do it.

14 MR. ARNDT: Absolutely.

15 MEMBER ROSEN: Try it, to see what it does
16 to the event trees and the fault trees, to see how
17 hard it is to incorporate it into models in a coherent
18 way, to see what it does to the CDF, depending upon
19 what kind of input parameters you use, to see how it
20 -- it works in terms of if you need to update -- you
21 know, all of the operational --

22 MR. ARNDT: Right.

23 MEMBER ROSEN: -- and implementation
24 issues.

25 MR. ARNDT: Operational issues.

1 MEMBER ROSEN: In other words, take --
2 don't just do the research from an academic point of
3 view. Take it out beyond that to an actually -- if we
4 were to do this, this is the way it would behave in
5 the field.

6 MR. ARNDT: Right. And later in the day
7 when I talk about future projects, that's one of the
8 future projects we have specifically is to do some
9 pilots with particular models in particular PRAs,
10 either ones that we have for other regulatory reasons
11 or doing it ourselves with the information that we
12 currently have, or with --

13 MEMBER ROSEN: I don't know if the SPAR
14 models are a good enough platform for this.

15 MR. ARNDT: No. We have access to actual
16 plant PRAs --

17 MEMBER ROSEN: Right.

18 MR. ARNDT: -- in some cases. And we
19 would use those.

20 MEMBER ROSEN: But maybe you could do it
21 in-house or -- but I would never try to use a plant
22 PRA without talking to the plant's PRA people.

23 MR. ARNDT: That would not be the
24 preferable method, no. That --

25 MEMBER ROSEN: I mean, you can do it.

1 MR. ARNDT: Yes, that is one of our --

2 MEMBER ROSEN: The part of this that I'm
3 aiming at is not just the doability, but the
4 confidence-building measures --

5 MR. ARNDT: Right, exactly.

6 MEMBER ROSEN: -- in the practitioner
7 community, in the nuclear PRA domestic practitioner
8 community.

9 MR. ARNDT: Exactly.

10 Okay. I think that's all I'm going to say
11 for this particular minute. I'm going to turn it over
12 to Barry. What I will -- what I'd like to -- next up
13 on our agenda is Professor Barry Johnson from the
14 University of Virginia. As I discussed earlier, he is
15 leading work in digital systems modeling using the
16 fault injection method. I will let him provide some
17 additional input on his background and get right into
18 the program.

19 MEMBER APOSTOLAKIS: Either you sit down
20 or we'll have to put a mobile microphone on you if you
21 want to stand up. Do you prefer to stand up?

22 DR. JOHNSON: I can do either one. I'd
23 like to stand if it's okay, but I -- I don't have to.
24 I'll sit. That's not a problem.

25 MEMBER APOSTOLAKIS: We're getting you a

NEAL R. GROSS

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

1 microphone.

2 DR. JOHNSON: Not a problem.

3 CHAIRMAN SIEBER: I think it might be over
4 there. You have to turn it on, too. There is a --

5 DR. JOHNSON: Test, test.

6 CHAIRMAN SIEBER: You just swallow the
7 microphone, and that will do it.

8 (Laughter.)

9 DR. JOHNSON: Is this okay?

10 CHAIRMAN SIEBER: Yes.

11 DR. JOHNSON: Okay. Well, I would like to
12 preface my talk with a couple of things. One is just
13 to thank you for the opportunity to be here. I enjoy
14 talking and interacting with groups of this sort. I
15 find I learn more perhaps from you than you learn from
16 me, and I certainly appreciate the opportunity to be
17 here.

18 The second thing is Steve had asked us to
19 give a little bit of our background as a way of a very
20 brief introduction. I started my career in the
21 aviation industry. I worked for Harris Corporation
22 where I designed flight control systems, and, in fact,
23 did the safety assessment for several flight control
24 systems during that part of my career.

25 And, in fact, it was the genesis for many

NEAL R. GROSS

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

1 of the ideas that I've been pursuing in the academic
2 environment for the last 20 years. I joined the
3 University of Virginia in 1984 and have continued
4 research in this area since then, and have come up
5 through the ranks at the university -- 1989, was
6 promoted to Associate Professor, and in '94 to a full
7 Professor. So I've been there since that time.

8 The third comment that I'll make, just as
9 a way of introduction, is I apologize -- I am
10 suffering from a fairly severe cold that has worked
11 its way from my sinuses through my chest. I'm on the
12 tail end of it, but my voice will crack, and so forth,
13 during the course of the conversations, and I
14 apologize for that. I'll try to make sure that I
15 speak as clearly as physically possible at this point.

16 My contact information is on the first
17 chart. Again, please feel free to contact me if you
18 have any questions or comments as we go forward from
19 today.

20 Several things we'd like to cover in the
21 outline that I think Steve had indicated you preferred
22 for these types of presentations. I'll start with
23 some conclusions. The important thing to note about
24 that is that they really are conclusions for this
25 talk. This research is ongoing. We find we almost

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

1 generate more questions than we do answers sometimes,
2 and I think that's a good thing. But, you know, the
3 conclusions will focus on the talk.

4 I'd like to talk a little bit about the
5 objectives of the program that we have, a little bit
6 of background, some of what we see as the challenges,
7 our methodology that we've been working on and that
8 we've applied in several cases, along with the process
9 that that involves. And we have -- we have shown this
10 in some real applications. I'll talk more
11 specifically about them.

12 They are predominantly transportation
13 applications, but there is a lot of similarity between
14 advanced training control systems and some of the
15 reactor control systems that are in place.

16 We've used this in Los Angeles, we've used
17 this in Copenhagen. We're currently using it in New
18 York. We're using it in Illinois. We're using it in
19 Pittsburgh. We have several projects that have gone
20 from cradle to grave with the methodology, at least as
21 the methodology existed at the time that we went
22 through that process.

23 And as a result of that, we've gotten some
24 real hard critical review of it from the safety
25 assessment organization TUV in Germany, as well as

NEAL R. GROSS

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

1 some independent consultants that were hired by Los
2 Angeles for the Metro green line transit system. So
3 there's a lot of good information I think that has
4 come out of that, and then we'll summarize and move
5 forward.

6 I'm one of those people that believes in
7 looking at the integrated hardware-software system.
8 I'm a firm believer in that. I don't think that
9 precludes things that you might do in software alone,
10 or things you might do on the hardware alone.

11 But as Steve has pointed out several
12 times, ultimately the software becomes a collection of
13 bits that get loaded into memory and they get executed
14 by hardware. And the interactions between those two
15 things influence a lot of what happens, and that's
16 where I focused my work is on those interactions.

17 So we have been looking at techniques that
18 can be applied to integrated hardware-software
19 systems, real software running in some cases on real
20 hardware, or real software running on a model of the
21 hardware. And those are two things that will be
22 prevalent in the discussions that we'll talk through.

23 I mentioned the process has been applied.
24 TUV is one of the organizations that spent an
25 incredible amount of time actually looking at this,

NEAL R. GROSS

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

1 and I'll talk about that in a little bit more detail
2 later on. But, you know, we developed at UVA the
3 analysis that was done for that Copenhagen system.

4 There was a set of documents created for
5 each step of that analysis, and the experts at TUV
6 reviewed and critiqued each one of those. And, in
7 fact, they were iteratively developed over the course
8 of a couple of years of that critique.

9 We've talked about -- this has come up a
10 couple of times so far today about assumptions. In
11 both the Los Angeles application and the Copenhagen
12 application, we have an entire document devoted to
13 assumptions. And every assumption is documented,
14 every assumption is discussed, and every assumption is
15 evaluated as to the consequences of that assumption
16 either holding or not holding. It's an important part
17 of the process.

18 Currently, we're looking at new ways of
19 modeling. For example, the issue of COTS has been
20 mentioned. One of the things that we are looking at
21 and that you'll see a little bit later on is, how do
22 I take an application-specific integrated circuit that
23 unbeknownst to me may have a hardware-software system
24 inside it that's executing certain implementation of
25 the protocol that that particular ASIC has provided.

NEAL R. GROSS

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

1 And I may not even know the internals of
2 that. I only know the interface of that. Is there
3 any way that I can model at the interface the things
4 that could happen if something goes wrong inside the
5 chip? And that work is actually being funded by
6 Electricite de France, which is the electric utility
7 EDF in France. And so that work is something that's
8 currently ongoing, as well as additional things that
9 are involving the new statistical models and other
10 types of things.

11 And that really covers some of the COTS
12 work, but the point of this bullet really is that
13 we've, over the years, developed a lot of tools. And
14 one of the things we learned very quickly is nobody
15 really wants to use university tools.

16 Universities don't have very good ways of
17 supporting those tools. Students come and they go.
18 We have a built-in turnover of our workforce every,
19 you know, two to five years, depending upon whether
20 you're dealing with Ph.D. or master's students. So
21 it's difficult to produce tools that are up to quality
22 and have the support necessary to be used in industry.

23 So what we've been doing in the last few
24 years is trying to take the techniques that we've
25 developed and integrate them into commercial tool

1 sets. Simics is one that we've been using recently.
2 We've used the Mentorgraphics tool set, the Cadence
3 tool set, a lot of the system-level design, and, in
4 fact, complete design capabilities in those tool sets.
5 We've tried to integrate our tools into that, and
6 we've had some success in that.

7 And then, lastly, we have started to look
8 not just a rail applications but at nuclear
9 applications. Calvert Cliffs is the most recent, but
10 we also have an objective to be able to look at -- in
11 fact, I'd love to be able to look at one of the three
12 systems that have been generically approved, and to
13 get that into the lab and to be able to do some
14 modeling and simulation and experiments with that.
15 But Calvert Cliffs' digital feedwater control system
16 is the one that we've looked at today.

17 What are the objectives? There are
18 several. And, again, just to focus on a couple of
19 them, we've been looking at safety assessment, and,
20 again, for digital systems. And to me -- I'll show
21 you what I mean by "digital system" in a moment. It's
22 not just hardware and software.

23 It actually involves -- certainly most of
24 the -- well, a lot of the elements are hardware, but
25 real systems involve mechanical components and they

NEAL R. GROSS

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

1 involve sensors and they involve other things that you
2 have to worry about as well, even though we focused
3 mostly on the controller parts, which are, you know,
4 processors and memories and other types of things with
5 software running on those.

6 MEMBER KRESS: When you say -- excuse me.
7 When you say "safety assessment," what exactly do you
8 mean by that?

9 DR. JOHNSON: Essentially, what we mean by
10 that is the -- a process by which I can look at the
11 safety of the system -- and it involves both
12 quantitative and qualitative issues. But most of our
13 work has been driven by an attempt to quantify the
14 safety, to be able to put a probability of occurrence,
15 you know, on an unsafe event.

16 MEMBER KRESS: Okay.

17 DR. JOHNSON: And the use of the execution
18 of this system. That's what we focused on. And by a
19 methodology, it's a -- just a sequence of steps that
20 we go through to try to get to --

21 MEMBER KRESS: I understand what you mean
22 now.

23 DR. JOHNSON: Okay. Modeling simulation
24 and experimental techniques -- one of the points I
25 want to make here is that, you know, sometimes I'm

1 accused of focusing too much on the quantitative side
2 of things, and I believe you need both. I think there
3 are process things you need to do. I think there are,
4 you know, things that you need to have in place that
5 allow you to -- you know, to have a successful
6 development enterprise.

7 But I also believe that there are
8 quantitative things that are important. And, in fact,
9 in the systems we've done in the past, I've learned
10 more by just the process of trying to get to a number
11 than perhaps I learned from the number itself. So I
12 do think both qualitative and quantitative things have
13 to be a part of it, and we've tried -- even though a
14 lot of our work focuses on the quantitative, we've
15 tried very hard to not lose sight of that fact.

16 I've mentioned tools. We've created a
17 bunch of them, and I'll show you some of those over
18 the course of the presentation. But we are trying to
19 use COTS tools and design systems where possible,
20 because ultimately -- and you'll see this at the end
21 of the presentation -- but ultimately the best way for
22 a real safety assessment to be done is for it to start
23 the day you start developing a system, and for it to
24 be an integral part of the design of that system with
25 certain products at various points that can be

NEAL R. GROSS

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

1 reviewed as evidence of what was done at that
2 particular state in the evolution -- or step in the
3 evolution of the system.

4 So that's important, and then
5 demonstrating it. And, you know, again, we've worked
6 with Boeing quite extensively. We've worked with the
7 rail industry extensively -- NASA, nuclear obviously,
8 and some others. Medical is another area that we've
9 been pretty heavily involved in.

10 MR. WHITE: Excuse me, Barry.

11 DR. JOHNSON: Yes.

12 MR. WHITE: I think this is really
13 exciting work. One question that I have is: what
14 size of system have you been able to analyze to date?
15 In other words, do you think you'll ever get to the
16 point where you can actually do a complete reactor I&C
17 system? Or do you think you're probably going to be
18 down in the system level or subsystem level?

19 DR. JOHNSON: There are -- I'll give you
20 a couple of examples. The Los Angeles system that we
21 analyzed was a -- what's called an interlocking, and
22 it -- if you've ever ridden the Washington Metro, we
23 have a station that you stop at, and you can have
24 trains on both sides.

25 Approaching that there are points for

1 trains to cross over track. And then when you leave
2 they can cross over, and that interlocking consisted
3 of six boxes. Each box had two processors in it.
4 Each processor was executing approximately 100,000
5 lines of code. The boxes were all interconnected with
6 a network, and it was -- in that case it was an
7 optical network, but it was a serial optical
8 communications path.

9 And then they also interconnected with
10 sensors that were placed along the track, and then
11 they had an interface with another communications box
12 that was a wireless network that allowed you to
13 communicate to trains and other points that were
14 remote from that system. So that -- that's a rough
15 illustration of complexity that was looked at.

16 In the Copenhagen system, it was actually
17 much more complicated than that. The number of lines
18 of code in that particular system was just a little
19 bit less than a million lines of code that were
20 involved in that. There were on board each of the
21 cars -- were 20 processors, and you have two main
22 pieces of the system.

23 There's what's called an automatic train
24 operation system that actually controls in a
25 driverless fashion all of the starting, stopping,

1 acceleration, velocity control, opening of the doors,
2 and so forth.

3 And then you have something that's called
4 the automatic train protection system, which is
5 somewhat analogous to the reactor protection system
6 that overlooks all of the system, measures certain
7 things, and makes decisions on whether something has
8 gone awry, and then shuts the system down if something
9 has, by using emergency breaking if something has gone
10 wrong.

11 So those are the -- that hopefully gives
12 you a little bit of feel for the type of complexity
13 that we've been looking at. Now, I guess the last
14 example -- the Calvert Cliffs system is a commercial
15 off-the-shelf digital control system, distributed
16 control system.

17 It's an Intel -- actually an AMD version
18 of the Intel 486 processor. It's running, you know,
19 Windows. 3.1 is one of the -- is the operating system
20 that's running at least portions of it. So that's --
21 and then the application is running on top of that.

22 CHAIRMAN SIEBER: And what's the scope of
23 control for that system?

24 DR. JOHNSON: For Calvert Cliffs?

25 CHAIRMAN SIEBER: Yes.

1 DR. JOHNSON: I'll show you a diagram of
2 that a little bit later on. I mean, it's essentially
3 controlling the level of water in a tank, and
4 controlling the valves.

5 CHAIRMAN SIEBER: Is this feedwater?

6 DR. JOHNSON: It is feedwater, yes, sir.

7 CHAIRMAN SIEBER: Okay.

8 DR. JOHNSON: And I -- yes, I have to
9 state right up front I'm not an expert on nuclear
10 systems in terms of the applications, and so forth.
11 I'm a hardware-software guy. I'm an electronics guy.

12 CHAIRMAN SIEBER: I'm familiar with that
13 system.

14 DR. JOHNSON: Okay.

15 CHAIRMAN SIEBER: I'm disappointed that
16 it's using Windows.

17 DR. JOHNSON: It's Windows 3.1, which
18 actually was -- that was one of the difficulties in
19 doing that. I mean, finding a copy of Windows 3.1 or
20 anything associated with it is a --

21 MEMBER KRESS: You can have mine.

22 (Laughter.)

23 MEMBER ROSEN: With all of its software
24 problems. It keeps telling me I've done an illegal
25 operation.

1 CHAIRMAN SIEBER: That's the least of your
2 problems.

3 (Laughter.)

4 DR. JOHNSON: So those are the objectives.
5 Just a couple of points that I want to make with this
6 slide. One is that, you know, these systems are
7 incredibly complicated, and that's one of the things
8 that makes it so difficult. The area that we focus on
9 at UVA is really what's inside the dotted line.

10 I say that simply to point out that, you
11 know, that obviously there are human beings involved
12 in these systems. There are, you know, complex
13 mechanical and civil infrastructures that are involved
14 in these systems. We don't focus on those activities.
15 What we focus on is really the sensors and actuators
16 that make up the control system, analog hardware
17 that's interfacing to those, digital hardware that's
18 interfacing.

19 But predominantly -- and importantly from
20 our standpoint -- is the hardware-software system that
21 is executing the control algorithms and other things
22 that are being used to make the system happen.

23 MEMBER ROSEN: Now, when you say you focus
24 on the -- I think you said dotted line, is what that
25 you said, or --

1 DR. JOHNSON: The two dotted lines.

2 MEMBER ROSEN: -- was it dashed lines?

3 Which is where --

4 DR. JOHNSON: Yes, the two dotted lines.

5 MEMBER ROSEN: -- you're focusing?

6 DR. JOHNSON: I apologize. We focus on
7 what's inside the big box.

8 MEMBER ROSEN: Okay.

9 DR. JOHNSON: And now --

10 MEMBER ROSEN: We had an earlier question
11 -- Jack did -- about the data that Steve was
12 presenting about digital system failures in nuclear
13 plants between the years 1994 and 1998, and whether it
14 was really on the inner box or whether it was within
15 the outer box. And I think we -- we concluded that a
16 lot of the failures in that database were outside the
17 inner box but inside the outer box. In other words,
18 they were in sensors or things like that.

19 DR. JOHNSON: I'm not surprised. I didn't
20 know that, actually, but I'm not surprised based on
21 what we've seen in some of the other -- the other
22 cases.

23 MEMBER ROSEN: Those databases basically
24 just say, "Bang. Everything inside those -- that
25 dashed box, the outer box, is a digital failure." And

1 I'm not sure about what, but maybe.

2 DR. JOHNSON: I mean, the thing that
3 complicates this a little bit even more is -- I mean,
4 this is an oversimplification of it, because sometimes
5 sensors nowadays have embedded processors in them, and
6 a lot of things are going on in there from a hardware-
7 software standpoint. But these are the types of
8 systems that we focus on.

9 The other point I wanted to make with this
10 is just the -- you know, the concept of interfaces.
11 And, you know, when I first started my career one of
12 the things that I did a little bit in was hardware
13 testing. And one of the things that you commonly
14 found was that, you know, you could have a piece of
15 hardware, and it would pass every test you could
16 expose it to.

17 But then when you put it in a system, and
18 it had to interface to other things, it started
19 failing. And it was because of that interface, and
20 the interaction between those components, that created
21 events that you hadn't really anticipated in your test
22 process.

23 And we've actually found that in the
24 hardware-software interface as well. The things that
25 happen in the hardware that exercise features of the

1 software -- that maybe you hadn't completely tested or
2 you hadn't envisioned being exercised in that way, and
3 vice versa. And you end up with some interesting
4 things happening there that you might not have
5 anticipated.

6 So the interfaces are critical, and I
7 think that's --

8 MEMBER ROSEN: Right. And I think your
9 point is it's more complicated even than what you're
10 showing here.

11 DR. JOHNSON: Absolutely.

12 MEMBER ROSEN: And one example is an
13 actuator that goes to a new position under control of
14 the software, sends a signal back to the software,
15 saying, "I have reached the position you sent me to."
16 And now that's -- so you have another feedback loop
17 inside from the actuator circuit back.

18 DR. JOHNSON: That's exactly right. In
19 fact, if you look at -- for example, one of the
20 systems we've looked at are the turbine control
21 system. And they actually use what are called, you
22 know, flux summing actuators.

23 They actually have multiple drives going
24 into them, and then they have an electromagnetic
25 summation process that occurs there. And then there's

NEAL R. GROSS

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

1 feedback from the actuator that goes back into the
2 digital controller, and you compensate, you know,
3 based on, you know, where you think you're driving it
4 versus where it is. And you've got a lot of
5 interactions that are going on there.

6 It is incredibly complicated, and I don't
7 want anybody to -- you know, to misunderstand our work
8 in the sense that, you know, we're not claiming to
9 have solved all the problems. And, you know, we're
10 focusing on the things we feel like we can get a
11 handle on and that we can make contributions to. But
12 it is a complicated system. Even the simple systems
13 are complicated systems.

14 MEMBER ROSEN: Well, I think the important
15 point here is that you've made a contribution just by
16 drawing this chart to me. But I think no one should
17 go away with the understanding that that's the
18 picture. And we do need to have -- when we do the
19 real stuff, we need to have the whole picture, not
20 just a model of the whole picture, which is what this
21 is.

22 DR. JOHNSON: Yes. I understand.

23 MEMBER ROSEN: Because it's as you say,
24 and as I say, somewhat more complicated than this.
25 And those complications can affect the outcome.

1 DR. JOHNSON: Absolutely.

2 MEMBER ROSEN: And the risk

3 DR. JOHNSON: And, again, this is all in
4 background. The other thing that's important that I
5 think is sometimes forgotten in some of these systems
6 is that most of them are what I would call real-time
7 systems, meaning that they have timing requirements.

8 And the timing requirements show up in
9 several different ways. They show up in some time
10 that I must be able to read inputs, calculate outputs,
11 and deliver them. You know, I come from an aviation
12 background where you're doing this process 180 times
13 a second. And if you don't get the right answer in
14 the right amount of time, you might as well not get
15 the right answer.

16 So there are some stringent timing
17 requirements typically. The other place that the
18 timing comes into effect is when an event occurs --
19 and, again, we look at what happens when a fault or
20 some event occurs, and how does your system respond to
21 that.

22 And typically you have some requirement on
23 how quickly you have to be able to respond. You have
24 to be able to identify the problem, remediate it, or
25 mediate it somehow, and reconfigure the system and

NEAL R. GROSS

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

1 keep it running, or shut it down, or do something.

2 And, for example, again, in the aviation
3 industry, you have about 500 milliseconds typically to
4 do a lot of that. And if you don't, then the dynamics
5 of the aircraft are such that you start noticing
6 problems and can get catastrophic results if they're
7 not taken care of quickly.

8 So timing is an issue. And, again, this
9 is another reason that we look at the integrated
10 hardware-softwares, because that integration is -- it
11 can have a big impact on timing, and that's I think an
12 important issue.

13 I've have students, for example, write
14 programs for real-time systems, and then, you know,
15 after we talk about them they go back and write them
16 again. And you can -- you can change performance of
17 those by an order of magnitude, just based on how you
18 do things in writing your software. So it's an
19 important issue.

20 So real time -- complex systems, real-time
21 requirements -- again, this is an oversimplification
22 of it, but I've got just a couple of points here I
23 want to make with this. And Steve actually has made
24 several of these.

25 But the first point -- and this doesn't

NEAL R. GROSS

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

1 attempt to show everything that's involved in the
2 evolution of a system or the design and operation of
3 a system -- but a couple of points that I want to
4 make. I mean, there are things that happen in the
5 operation.

6 Once the system is out there and it's
7 running, there are things that happen that are due to,
8 you know, components just failing. I mean, hardware
9 just dies sometimes. Operators make mistakes. They
10 enter parameters incorrectly or they make wrong
11 decisions. Or external disturbances -- I mean, the
12 biggest problem you have in an airplane is lightning.

13 You know, if you solve the lightning
14 problem, you've solved a lot of your other problems
15 typically in terms of external disturbances. So there
16 are a lot of things that happen.

17 In the development there are a lot of
18 things that happen, and this is just a subset of them.
19 But, you know, you can misunderstand requirements or
20 make mistakes in creating those requirements or have
21 incompleteness in those requirements.

22 One of my colleagues likes to refer to the
23 completeness problem, and that's the way he sums up
24 the whole issue. How do I know that things are
25 complete in terms of understanding whether I've got

1 sufficient requirements and sufficient testing and
2 other types of things?

3 I can make implementation mistakes, and
4 these things can lead to problems in either the
5 hardware or the software or both. You know, for
6 example, Intel will acknowledge that there are 79
7 design defects in the Pentium processor, 39 of which
8 they've chosen to fix. You know, some 40 that they've
9 chosen to ignore, because they occur so infrequently
10 that they are normally not an issue, and we use it
11 successfully every day. But there are design defects
12 in that process.

13 So you can have design defects here. You
14 can have random defects, randomly occurring failures
15 there. You can have design defects here. These can
16 interact with one another. I've actually seen
17 examples of systems where a bug in the software did
18 some things to the hardware, activating things that
19 should not have been activated simultaneously, and
20 actually burned out a portion of the system, creating,
21 in effect, a hardware fault due to the occurrence of
22 a bug that was in the software.

23 So those things can interact with one
24 another. You can also have corruptions in your data
25 structures that make up your system, and these --

NEAL R. GROSS

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

1 again, you can have all of these things leading
2 ultimately to what I call a failure, which some people
3 call a malfunction, but it's fundamentally just a --
4 you know, a non-performance or an incorrect
5 performance of something that the system is supposed
6 to do.

7 MEMBER APOSTOLAKIS: But it seems to me
8 that you are making now a very strong case for looking
9 at software as part of the system and not in
10 isolation.

11 DR. JOHNSON: I am.

12 MEMBER APOSTOLAKIS: So --

13 DR. JOHNSON: I am. I believe that very
14 strongly. I believe that very strongly.

15 MEMBER APOSTOLAKIS: No apologies
16 required. You are doing a great job. But now I come
17 back to my earlier question about ISO 9000, where they
18 talk about mean time to failure. And I'm wondering
19 what that means now in this context, especially in
20 light of your last statement, that the software
21 triggered something in the hardware, and then came
22 back and, you know, there was an interaction there.

23 DR. JOHNSON: Right.

24 MEMBER APOSTOLAKIS: So how -- I mean,
25 what does it mean to talk about mean time to failure

NEAL R. GROSS

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

1 of the software? I can understand maybe talking about
2 the mean time to failure of the whole thing you have
3 there. That might be a concept that would be
4 acceptable.

5 DR. JOHNSON: Right. And that's --

6 MEMBER APOSTOLAKIS: But you are making a
7 very strong case for, you know, looking at the whole
8 thing as an integrated whole, which this agency has
9 been doing for nuclear powerplants now for 30 years.

10 DR. JOHNSON: Right.

11 MEMBER APOSTOLAKIS: Right?

12 DR. JOHNSON: And I do believe that. I
13 mean, I --

14 MEMBER APOSTOLAKIS: I'm sure you are not
15 lying to us, yes.

16 (Laughter.)

17 DR. JOHNSON: I do indeed believe that.

18 MEMBER APOSTOLAKIS: I just wanted to
19 point that out, because this is a question that at
20 least is in my mind.

21 MEMBER ROSEN: Yes. George, I see that
22 exactly as a mean time to failure for this system is
23 when you hit that box on the bottom.

24 MEMBER APOSTOLAKIS: Yes.

25 MEMBER ROSEN: You don't think about what

NEAL R. GROSS

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

1 happens before that.

2 MEMBER APOSTOLAKIS: Yes.

3 MEMBER ROSEN: But by analogy, also, what
4 I think of is a latent defect in a plant system. For
5 instance, someone makes a maintenance error in setting
6 up a motor-operated valve. And -- or, let's say,
7 tightens the packing too much and he's redoing the
8 packing.

9 So, actually, when the valve gets a signal
10 to stroke it won't, because it's one bang. That's a
11 latent defect. Now that is exactly analogous, in my
12 view, to the things on the left side. Someone had to
13 put a requirement -- there's a mistake in the
14 requirements.

15 Maybe there's a file structure that
16 transfers into the processor that the processor wants
17 to have 100 fields filled up, and the processor has
18 120 in it. So when it tries to transfer the data it
19 transfers 100, and it can only transfer 100, it leaves
20 -- it drops 20 bits, and you don't know what -- which
21 20 it's going to drop. So it's, you know, that kind
22 of is a latent defect from a -- coming in from the
23 outside.

24 And so I see those latent defects in a
25 powerplant, the one I described of the valve with the

1 packing, like the one I described in the file. Those
2 are very analogous in my view.

3 MEMBER APOSTOLAKIS: I was intrigued by
4 what you said about Intel. They decided to leave
5 design faults because they figured that those would be
6 triggered under very rare circumstances?

7 DR. JOHNSON: Yes. Those are --

8 MEMBER APOSTOLAKIS: What is rare in their
9 view? Do you know?

10 DR. JOHNSON: You know, probably the most
11 famous example of one that was found by the general
12 public and created an uproar within Intel was actually
13 found by a professor at Lynchburg College who was
14 doing some fairly complicated modeling simulation
15 applications and he started using -- he started
16 noticing that from his two different Intel processors
17 that were running the same software he was getting
18 different results from the floating point
19 calculations, and they were out in very, very, you
20 know, far out digits, you know, to the right of the
21 decimal point.

22 And he started -- that was important to
23 him, and he started asking and inquiring, and it
24 uncovered a flaw that -- or a design defect that was
25 in the floating point unit of the Pentium processor.

1 MEMBER APOSTOLAKIS: So Intel didn't know
2 that?

3 DR. JOHNSON: Intel did not know that.
4 They had not uncovered it with, you know, all of their
5 testing and simulations and all the things that have
6 been done. And, obviously, they had sold millions of
7 Pentium processors that, you know, had that in it, but
8 it was just this particular person was doing something
9 that was exercising the hardware in a specific way
10 that no one else had really done, or either hadn't
11 noticed. And there are a lot of examples of --

12 CHAIRMAN SIEBER: In these instances, you
13 know, the regular commercial user would never run into
14 it because there is no software that's commercially
15 available that uses every feature of a Pentium chip.

16 DR. GUARRO: I can give you an example of
17 a software defect that exists now in Excel. If you go
18 into the beta function and you put a very low value,
19 the alpha parameter you get a 95th percentile higher
20 than the 99 percentile. And it has been there for a
21 long time, to my knowledge, and I don't think anybody
22 worries about it.

23 MEMBER APOSTOLAKIS: Does Microsoft know
24 this?

25 DR. GUARRO: I don't know.

1 CHAIRMAN SIEBER: The question is: does
2 Microsoft care?

3 DR. JOHNSON: Right.

4 (Laughter.)

5 MR. ARNDT: Well, that really goes back to
6 the issue we were discussing earlier. In a lot of
7 cases these are conscious decisions based on the
8 applications that you're doing.

9 DR. JOHNSON: That's right.

10 MR. ARNDT: And in the application that
11 they're interested in it's not an issue for safety or
12 for performance or whatever.

13 MEMBER APOSTOLAKIS: Yes. But the problem
14 that I'm having, though, with that is that it's not so
15 much that, you know, some academic someplace was doing
16 work and found a strange thing that's very rare. It
17 shakes my confidence in the whole enterprise.

18 I mean, if we use this now in safety
19 critical applications, I don't know -- I'm kind of
20 scared, because, you know -- you know the famous
21 saying there are things that we know we don't know,
22 and things we don't know that we don't know. It's the
23 latter part that really scares me.

24 MR. ARNDT: Right. It's a knowledge
25 uncertainty issue.

NEAL R. GROSS

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

1 MEMBER APOSTOLAKIS: Yes, that's right.

2 CHAIRMAN SIEBER: Well, I think that you
3 would have to be carefully considered if you found
4 failure rates for digital systems that were
5 significantly different than the failure rates you get
6 out of analog systems. And then the regulation of it
7 would be easy. You would just write a rule that says
8 don't use digital systems.

9 MEMBER APOSTOLAKIS: But the point is
10 we're talking about the rare application that this
11 professor was doing. But suppose you are in the
12 middle of a severe accident. That's a rare thing, and
13 now you are relying on some software --

14 CHAIRMAN SIEBER: Well, I can give you an
15 example of a mistake I made years ago that took a year
16 and a half to reflect itself, which was a -- basically
17 a routine that directed to a series of tables that had
18 to be solved, and where it went in those tables
19 depended on parameters of -- in the powerplant. And
20 it took a year and a half before it ever got to the
21 combination that took it to a bad table, you know.
22 Once it got there, it never came out.

23 MEMBER ROSEN: What I'm concerned about in
24 your story is that Intel doesn't know what people are
25 going to use the chip for.

1 CHAIRMAN SIEBER: That's right.

2 MEMBER ROSEN: And that someday someone
3 may use it for something that invokes the chip in one
4 of those areas that they didn't fix.

5 DR. JOHNSON: I will not mention the name
6 of the company, but I have a -- there is -- in fact,
7 I had reason to review a supplier agreement not too
8 long ago from a company that makes integrated
9 circuits, and so forth.

10 And one of the things that I was surprised
11 to find in there was a statement that the -- you know,
12 the customer buying that component is warranting that
13 they will not use the integrated circuit in aviation,
14 nuclear, military, or -- there's a long list of
15 applications where, again, as part of the supplier
16 agreement it was -- you were signing up to not using
17 it. So you were, you know, limiting your field of
18 use. And, in fact, if you chose to use it in those
19 arenas, you were accepting liability for anything that
20 might happen there.

21 MEMBER ROSEN: Is that common now?

22 DR. JOHNSON: I don't know how common it
23 is. I -- you know, honestly, I've only had occasion
24 to review a small number of these supplier agreements,
25 so I don't know the answer to that.

1 MEMBER ROSEN: From a regulatory
2 standpoint, I don't know that we would be too thrilled
3 with having -- with licensees that agreed to that sort
4 of thing.

5 CHAIRMAN SIEBER: I'm not sure you can get
6 some chip-makers to pay for the cost of a severe
7 accident at a powerplant.

8 DR. JOHNSON: Okay. The other thing in
9 the way of background that I wanted to just have one
10 slide on is this concept of coverage, because it's
11 really at the heart and soul of what I do. Because,
12 I mean, there -- as you'll see a little bit later on,
13 I mean, there are a couple of issues or questions that
14 you can ask yourself. One is, you know, rate of
15 occurrence of some of these problems.

16 I know we've already talked multiple times
17 about difficulty of being able to assess what that
18 rate is for hardware-software systems, and I -- you
19 know, it is a very, very difficult thing. And that's
20 not what we focus on in our work. What we focus on
21 is: what if something does happen?

22 You know, when something occurs, then how
23 capable is the system of responding to that something?
24 Whether it's a hardware-software defect or some other
25 element of the system. And we use this coverage

NEAL R. GROSS

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

1 estimation concept as part of the work that's done
2 there.

3 Coverage can be broken up into several
4 pieces. We normally lump it into one -- you know, one
5 probability, which is a conditional probability.
6 Given that a fault has occurred, what's the
7 probability that your system is going to correctly
8 detect, locate, isolate, recover from that?

9 And that's this concept of coverage that
10 we talk about, and, in fact, talk about in all of our
11 papers is, you know, what -- given that something
12 occurs, am I going to handle it correctly or
13 incorrectly? And that's really what this concept of
14 coverage is all about.

15 MEMBER APOSTOLAKIS: Well, let me -- when
16 you say "fault occurs" -- let's go to the previous
17 slide if we can. Now, where in your ovals can that
18 fault occur?

19 DR. JOHNSON: It can actually occur -- the
20 fault itself can occur anywhere, actually, in these
21 ovals. I mean, it -- you can have a design fault
22 that's in there from day one as a result of something
23 that you've done in the development process. You can
24 have a random problem occur.

25 On the next chart --

1 MEMBER APOSTOLAKIS: But these are not
2 necessarily faults. I mean, if you -- if the operator
3 does something wrong, would you call that fault?

4 DR. JOHNSON: In the world I come from,
5 which is the fault tolerance or dependability
6 community, that would all be considered a fault.
7 Fault is defined as a physical imperfection or defect
8 or flaw in anything -- hardware, software, whatever it
9 may be -- and it's a defect.

10 MEMBER APOSTOLAKIS: But an external
11 disturbance might be --

12 DR. JOHNSON: Power loss. Loss of power
13 through --

14 MEMBER APOSTOLAKIS: Yes, it doesn't have
15 to be a fault. I mean, it can be some external
16 condition which had not been anticipated by the
17 designer, for example. That wouldn't -- would that be
18 a fault?

19 DR. JOHNSON: It would be -- the external
20 disturbance would be the cause of the fault.

21 MEMBER APOSTOLAKIS: So the fault was not
22 anticipating it.

23 DR. JOHNSON: Right. The fault -- for
24 example, I have a lightning strike. The lightning
25 strike induces hundreds of thousands of amps into a

NEAL R. GROSS

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

1 conductor, and, you know, because I haven't properly
2 designed for that I get an open or a short or
3 something that occurs as a result of that.

4 And now I've got a hardware fault that's
5 in the system due to an external disturbance that
6 occurred. Similarly, with an operator -- an operator
7 -- you know, for example, the -- one example was
8 mentioned here of the space application, where the
9 conversion parameters were entered incorrectly.

10 And to some extent that's a data structure
11 problem. Someone had to enter parameters that were
12 used in that conversion, and they form a database that
13 the hardware and software use, and that's a latent,
14 you know, defect that's in that system that when --
15 when attempted to use you'll have a consequence
16 resulting from that.

17 MEMBER APOSTOLAKIS: So fault can be
18 anywhere, including the hardware.

19 DR. JOHNSON: Absolutely.

20 MEMBER APOSTOLAKIS: Whoa. Okay.

21 DR. JOHNSON: Absolutely.

22 MEMBER APOSTOLAKIS: It's pretty
23 ambitious, though, isn't it?

24 DR. JOHNSON: We have to focus on what we
25 can.

1 MEMBER APOSTOLAKIS: Absolutely.

2 DR. JOHNSON: You know, again, it's a
3 complicated --

4 MEMBER APOSTOLAKIS: Now I understand what
5 you mean.

6 DR. JOHNSON: Now, I even hesitated --

7 MR. WHITE: I'm sorry. Can I ask you a
8 question about the fault coverage?

9 DR. JOHNSON: Absolutely.

10 MR. WHITE: You know, the other
11 possibility here is that the fault occurs, the
12 software -- the system never knows that the fault
13 occurs, so there is no fault detection. But still
14 there are no consequences.

15 DR. JOHNSON: That's right. And we
16 actually -- the community calls those no response
17 faults.

18 MR. WHITE: Ah, thank you.

19 MEMBER APOSTOLAKIS: Or they are latent,
20 right?

21 MEMBER ROSEN: No. Latent fault was one
22 that would -- if you get into the wrong circumstance,
23 like to close, it doesn't close because the packing is
24 too tight.

25 MEMBER APOSTOLAKIS: Well, but these --

NEAL R. GROSS

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

1 MEMBER ROSEN: But as long as it's open
2 and not -- the system runs fine.

3 MEMBER APOSTOLAKIS: But these kinds of
4 faults have the same property. They will be there.
5 You don't know they're there until some circumstances
6 will make the fault -- identify the fault.

7 DR. JOHNSON: And it's -- I mean, part of
8 what's important there is that the way you exercise
9 the system influences that. And, in fact, that's one
10 of the things we found. We've actually -- in some of
11 the systems we've done, we've found bugs in the
12 software that were there from the beginning of time in
13 terms of the system. And they were not discovered
14 until we actually exercised the system in such a way
15 that they were needed -- you know, that the software
16 function that they were in was needed.

17 MEMBER ROSEN: But isn't that the
18 responsibility of the owner, to give -- it has a
19 certain system -- to test it in all its operating
20 modes so that -- so that even though you only use one
21 of the nine modes typically, if you ever switch to one
22 of the other eight modes, you get all kinds of strange
23 things happening that you didn't anticipate. It's
24 your fault for not having tried that during the setup.

25 DR. JOHNSON: And the real difficult

NEAL R. GROSS

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

1 problem there is something I mentioned a few minutes
2 ago -- is there is the completeness problem. It is
3 knowing that you have exercised things in enough of
4 the ways that they will be encountering in the real
5 application to be able to state with any confidence
6 that you've covered those types of scenarios.

7 MEMBER BONACA: But then you -- I mean,
8 can you be sure that you've covered everything?

9 MEMBER ROSEN: You can't.

10 DR. JOHNSON: That's a big issue with
11 digital systems.

12 MEMBER APOSTOLAKIS: In other words, the
13 problem is where it says fault occurs.

14 DR. JOHNSON: That's right.

15 MEMBER APOSTOLAKIS: You have to have an
16 envelope of faults.

17 DR. JOHNSON: And, in fact, the way we
18 approach that is that, you know, because -- I'll give
19 you some examples. But, you know, the envelope that
20 you're referring to is critical, and there are several
21 schools of thought there if you look around the
22 community that does this type of work.

23 One is that you should do things randomly
24 here, that you should randomly inject faults into the
25 system, choosing random times, locations, you know,

NEAL R. GROSS

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

1 characteristics, and other types of things.

2 There are others that -- in fact, we
3 developed a technique that we referred to as malicious
4 faults. We actually derived -- in fact, this -- we
5 have a patent on this, where there's a technique for
6 taking, at the highest level in the system, the
7 algorithm that is going to be executed by that
8 hardware-software system, and then devising or
9 creating from that what we call malicious faults,
10 which are things that could go wrong in the execution
11 of that algorithm.

12 And if they go wrong and are not
13 mitigated, they will cause an unsafe action, and then
14 we inject those into the system and determine what the
15 system does in response to those.

16 So there are multiple schools of thought
17 there, and actually, you know, what we've seen over
18 the years is that you really -- there's a lot -- you
19 really have to do both. You have to do some of the
20 malicious types of things. You have to do random
21 things. You have to do other things as well.

22 MEMBER ROSEN: If it matters.

23 DR. JOHNSON: If it matters.

24 MEMBER ROSEN: I mean, if the coverage --
25 if a fault is -- if a fault's consequences are

NEAL R. GROSS

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

1 important --

2 DR. JOHNSON: Right.

3 MEMBER ROSEN: -- you have high risk.

4 MEMBER APOSTOLAKIS: But you don't know

5 that.

6 DR. JOHNSON: You don't know that.

7 MEMBER APOSTOLAKIS: You don't know that.

8 DR. JOHNSON: Sometimes it is difficult to

9 know that.

10 CHAIRMAN SIEBER: But putting random

11 faults in almost assures that you aren't

12 comprehensive.

13 DR. JOHNSON: Right.

14 MEMBER BONACA: That what?

15 DR. JOHNSON: That's right.

16 MEMBER BONACA: That you're not.

17 CHAIRMAN SIEBER: That you're not.

18 DR. JOHNSON: It gives you some

19 confidence, but it doesn't give you ultimate -- it

20 doesn't give you complete assurance.

21 CHAIRMAN SIEBER: Well, it depends on how

22 long you let it run. And this fault injection --

23 MEMBER BONACA: Either process is --

24 without the process you don't know.

25 MEMBER KRESS: I'm kind of interested in

NEAL R. GROSS

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

1 the details here. How do you inject a fault?

2 DR. JOHNSON: There are several -- in
3 fact, I'll address that actually a little bit later
4 on. There are several ways that you do it. In the --
5 we are -- we look at both simulation-based approaches
6 and physical experiment-based approaches. And if you
7 are talking about a physical experiment, there are,
8 you know, a couple of ways that you can do it
9 typically.

10 You can instrument your system, so that
11 you can actually get access to points where you can,
12 you know, control corruptions. You can insert them,
13 you can control the time that they're there, and
14 things of that sort. You can get access to the
15 software in the memory of the processor, and, you
16 know, cause things to change in terms of the software
17 structure, and so forth.

18 In the simulation environment, you
19 actually have a lot more control over what you can do,
20 because you have access to things that you don't have
21 access to in the physical system. And, again, you
22 have similar types of approaches, though, where you
23 can actually instrument your simulation to allow you
24 to go in and create problems, and then determine how
25 the system responds to those problems.

1 MEMBER KRESS: Is that like inserting a
2 virus?

3 DR. JOHNSON: Well, it's -- certainly you
4 can look at it partly that way, certainly. It's --
5 but if you look at the techniques for fault injection,
6 there are hardware-based techniques, there are
7 software-based techniques, there are simulation-based
8 techniques, and then there are hybrid, which is
9 combinations of those three.

10 MEMBER KRESS: Well, how normally are
11 these faults detected in the system? Are there
12 detections -- are you talking about a self-correcting
13 system there?

14 DR. JOHNSON: These are -- the systems
15 that we deal with are systems that have built-in
16 mechanisms for, you know, detecting and managing
17 faults that occur. And, you know, they may have
18 reconfiguration capabilities. They may have shutdown
19 capabilities.

20 They may have -- you may have one system
21 that's overseeing another system, and you are
22 injecting faults into this system and seeing if the
23 other system actually detects that. So there are a
24 number of different architectures of systems that
25 we've looked at over the years.

NEAL R. GROSS

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

1 MEMBER KRESS: How do they recognize a
2 fault? I'm getting right down to the basics.

3 DR. JOHNSON: Sure. I mean, you have --
4 there are lots of different techniques for doing that.
5 I mean, we -- you know, for example, sometimes you use
6 your redundancy as a way of detecting a fault, so you
7 have voting --

8 MEMBER KRESS: Okay. You're getting
9 voting, and then --

10 DR. JOHNSON: Loading and comparison.

11 MEMBER KRESS: I'd like to see how that
12 would work.

13 DR. JOHNSON: Like, you know, for example,
14 in the Boeing 777 aircraft they have a triplicated
15 architecture. But what they've done is they've
16 actually taken, you know, three different versions of
17 the processor and three different versions of the
18 software running on each of -- you know, so they had
19 nine different processors.

20 So that they have all of the versions of
21 the software running on all of the versions of the
22 processor, and then they have a voting architecture
23 that is used to try to detect disagreements that show
24 up between those different processors. So there are
25 a lot of -- a litany of ways that that's done.

NEAL R. GROSS

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

1 MEMBER KRESS: And I presume there's ways
2 to locate the fault within --

3 DR. JOHNSON: Yes.

4 MEMBER KRESS: -- a software --

5 DR. JOHNSON: Ways to locate faults within
6 systems.

7 MEMBER KRESS: Within systems.

8 DR. JOHNSON: A lot of times, you know,
9 the fault location techniques don't focus on whether
10 it's a hardware problem or a software problem.
11 They're simply focusing -- in fact, they typically
12 focus at what we call the information level, because
13 for you to be able to detect things it has to somehow
14 corrupt a piece of information in your system.

15 And you have to be able to either detect
16 that because it differs from what was expected or it
17 differs from a replica of it.

18 MEMBER APOSTOLAKIS: Now, the word "fault"
19 appears -- you know, fault occurs, and then you have
20 four boxes. Are we talking about one fault? Because
21 you told us earlier that "fault occurs" means some
22 environmental condition. It's not necessarily a
23 fault. I mean, it's -- something happened.

24 DR. JOHNSON: Well, it could be --

25 MEMBER APOSTOLAKIS: And then there may be

1 a fault --

2 DR. JOHNSON: It's not just environmental.

3 MEMBER APOSTOLAKIS: There may be a fault
4 somewhere inside the system --

5 DR. JOHNSON: Absolutely.

6 MEMBER APOSTOLAKIS: -- which is uncovered
7 by that.

8 DR. JOHNSON: Absolutely.

9 MEMBER APOSTOLAKIS: So we are not talking
10 about a single fault.

11 DR. JOHNSON: Not necessarily. I'll show
12 you another diagram that --

13 MEMBER ROSEN: Now, that has -- that fact
14 has enormous consequences for PRA modeling of digital
15 systems.

16 CHAIRMAN SIEBER: Yes. But this chart
17 here is showing a process -- detection, location,
18 isolation, and recovery. And so you're moving to the
19 right through that process for a single fault. Now
20 you may have multiple faults. A single fault may
21 generate other faults.

22 MEMBER APOSTOLAKIS: Or it may not even be
23 a fault.

24 CHAIRMAN SIEBER: Well, an example of that
25 is --

1 MEMBER APOSTOLAKIS: The input may be some
2 abnormal condition. That's not a fault.

3 CHAIRMAN SIEBER: The tuning of a process
4 loop where the equations -- the algorithms that you
5 use don't take into account the harmonics of the
6 system. Okay? And so now you've got some valve
7 that's gone from full open to full closed, back and
8 forth, that's caused basically by the mechanical
9 features of the sensor and the actuator, and the
10 computer is just doing what it was told to do. That's
11 all, however, because it can trip the plant.

12 MEMBER BONACA: Actually, the -- it was
13 mentioned before on the system failures. The Delta 3
14 failure was of that nature. But essentially a control
15 system was overreacted, and it ran the actuator too
16 hard and too long. The actuator lost the hydraulic
17 oil, and eventually failed. So it was a very complex
18 and drawn-out situation. You know, if the flight had
19 been shorter, it would have not -- you would have
20 gotten away with it, but so --

21 CHAIRMAN SIEBER: But the interesting
22 thing about those kinds of faults is that if you don't
23 run the physical plant, you can't test for them.

24 MEMBER BONACA: Right.

25 CHAIRMAN SIEBER: You know, I think there

NEAL R. GROSS

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

1 are some -- some mathematical ways to do it. On the
2 other hand, it's not particularly reliable because you
3 don't know the dynamic parameters with enough
4 certainty to be able to model everything. But that is
5 clearly kind of a fault that can occur that can trip
6 the plant or cause some unsafe actuation.

7 MEMBER KRESS: This discussion brings to
8 mind -- in your fault injection technique, are you
9 injecting one fault at a time? Or can you inject
10 multiple faults when --

11 DR. JOHNSON: There are two things to keep
12 in mind. When we do the fault injection experiments,
13 in the case of simulation-based experiments, we have,
14 you know, the real ones and zeroes that correspond to
15 the software. We're executing that real software. So
16 if there are any defects or faults in the software,
17 we're exercising those faults.

18 And then when we do the injection, we can
19 actually inject, you know, one or hundreds. I mean,
20 we can inject as many as we want to inject,
21 simultaneously or at different times, or for different
22 durations. So we can emulate permanence and
23 transience and things of that sort.

24 MEMBER APOSTOLAKIS: First of all, I'm
25 dying to go Slide 9, because there is a probability --

1 (Laughter.)

2 -- have failure rate. But before I die,
3 what are the C's? $C_D C_L$ is the fractions or --

4 DR. JOHNSON: These are probabilities
5 of -- for example, probability of detection.

6 MEMBER APOSTOLAKIS: How do you know that?

7 DR. JOHNSON: Well, this is what we focus
8 on estimating.

9 MEMBER APOSTOLAKIS: Estimating.

10 DR. JOHNSON: This is what we use the
11 fault injection techniques to try to estimate.

12 MEMBER APOSTOLAKIS: Now, in your fault
13 coverage, as it was discussed a few minutes ago, the
14 real issue -- and you acknowledge that -- is really
15 how do you come with an envelope of faults so that you
16 build up your confidence that what you are doing is
17 very meaningful.

18 I was wondering -- could one use some of
19 the analytical tools that, for example, are used in
20 PRAs, like fault trees or some other method, to go
21 back to your previous slide and -- and develop a model
22 for the hardware-software environment, and maybe that
23 can help you to be a little smarter when you select
24 the faults. Has that been tried?

25 DR. JOHNSON: That's exactly right. In

NEAL R. GROSS

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

1 fact, we have -- one of our publications -- and, in
2 fact, the patent that we have is based on something we
3 call malicious faultless generation.

4 Essentially, what we do is we take the
5 hardware-software execution and we -- we generate
6 essentially a fault tree, but it's a time varying
7 fault tree in the sense that at every step of the
8 execution you have a fault tree of all of the things
9 that could go wrong at that point in the execution
10 that could lead to an incorrect result from that
11 execution.

12 And those things -- not only that, but
13 those things would lead to an unsafe output being
14 delivered to the system, and we call those malicious
15 faults. And we actually, you know, developed some
16 algorithms that allow you to do that automatically,
17 find some of those, and then you can inject those.

18 Now, one of the difficulties we have is
19 that since those are not, you know, randomly-occurring
20 things necessarily, when you start trying to integrate
21 those into a probabilistic model, you have some things
22 that are truly randomly selected. You have some
23 things that are not.

24 And one of the issues that we've been, you
25 know, struggling with quite honestly in looking at

NEAL R. GROSS

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

1 ways to handle is how do I -- how do I integrate some
2 things that are, you know, non-probabilistic with
3 things that are probabilistic and come up with a
4 probabilistic answer.

5 MEMBER APOSTOLAKIS: But it seems to me
6 that this is a general method that can be used in
7 connection with any method that has been developed to
8 identify failure paths.

9 DR. JOHNSON: I think so.

10 MEMBER APOSTOLAKIS: Right?

11 DR. JOHNSON: My hope would be that it
12 could.

13 MEMBER APOSTOLAKIS: Yes. Another
14 critical question here is: when you find a fault,
15 don't you fix it, so that $C_D C_L$, $C_I C_R$, are not constant.

16 DR. JOHNSON: That's correct.

17 MEMBER APOSTOLAKIS: Which is a crucial
18 observation.

19 DR. JOHNSON: That's correct. I mean, and
20 if you think about it from an experimentation
21 standpoint, let's say you do find -- let's say that --
22 you know, let's say that fault location is done by
23 software. And let's say that you run this set of
24 experiments, and you find a bug in your fault location
25 software. I mean, obviously you're going to fix it.

NEAL R. GROSS

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

1 MEMBER APOSTOLAKIS: Unless you are Intel.

2 (Laughter.)

3 DR. JOHNSON: But you're going to fix it.

4 So now the question is, you know -- I mean, that

5 obviously changes your system, and the question is:

6 now what do you do? And, you know, those are --

7 MEMBER APOSTOLAKIS: I mean, any

8 probabilistic calculation now is really up in the air

9 in my mind.

10 DR. JOHNSON: Now, what we've done in the

11 systems that we've done when we've found bugs, you

12 know, we've fixed them, and then we've -- we've, you

13 know, generated another set of experiments. We've

14 repeated the process.

15 The danger you have there is that that can

16 be an iteration that can go on forever, and you've got

17 to know when to stop.

18 CHAIRMAN SIEBER: It sounds like lifetime

19 employment.

20 MR. ARNDT: Well, the saving grace there

21 is the decision point in most cases is: is it this

22 good or better? Or do you fix it? You're driving the

23 system to be --

24 MEMBER APOSTOLAKIS: Well, but the -- I

25 mean, I'm sure Dr. Johnson will come to it, but I've

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 seen other models in the past where, for example, they
2 say, "Okay. It's not as detailed, but maybe if you
3 consider the fault boxes as one box." And so there is
4 a probability P of something going wrong.

5 Then, I ran it many times. I find five
6 errors. I fix them. Well, P is not constant anymore.
7 You can't use the binomial distribution. You can't
8 use any of that. And yet people go ahead and use it.
9 And, I mean, I would rather gain confidence by doing
10 this with a reasonable envelope than try to force a
11 probabilistic model that probably doesn't mean much.

12 But now let's go to Slide 9; there is a
13 failure rate.

14 CHAIRMAN SIEBER: No. Let me take a
15 little timeout here for a second. You're about a
16 third of the way through your presentation, if I count
17 the slides.

18 DR. JOHNSON: And I'm about three-fourths
19 of the way through my time probably, and halfway
20 through --

21 CHAIRMAN SIEBER: Your time will run out
22 in 16 minutes. On the other hand, it seems to me at
23 this point when we move to Slide 9 you're getting into
24 a lot of detail where a break would not be
25 appropriate. Is that true?

1 DR. JOHNSON: Well, we could certainly --

2 CHAIRMAN SIEBER: This would be the slide
3 to break for lunch on, would it not? Or would it?

4 DR. JOHNSON: It would certainly be an
5 appropriate place to break, and George is left
6 hanging.

7 MEMBER APOSTOLAKIS: Yes.

8 CHAIRMAN SIEBER: I did that on purpose.

9 MEMBER APOSTOLAKIS: But let me raise
10 another thing, though. I mean, we -- obviously, Barry
11 will need more than 16 minutes to cover all of this.

12 CHAIRMAN SIEBER: Yes.

13 MEMBER APOSTOLAKIS: Then we have a
14 Maryland presentation scheduled for 1:15. Carol, can
15 you stay later?

16 MS. SMIDTS: Yes, that's fine.

17 MEMBER APOSTOLAKIS: The members will
18 stay, too?

19 MEMBER KRESS: We'll always stay.

20 CHAIRMAN SIEBER: They told me you wanted
21 to work overtime today.

22 MEMBER APOSTOLAKIS: I'm going to have to
23 get out by 4:30 or so, 5:00 at the latest.

24 CHAIRMAN SIEBER: We will finish by 5:00.

25 MR. ARNDT: Yes, I think we're running

NEAL R. GROSS

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

1 something like a half hour late now.

2 MEMBER APOSTOLAKIS: But we're going to
3 lose Dr. Guarro at 3:30, because it's his birthday
4 today. And we are so cruel we don't -- can you move
5 your birthday?

6 (Laughter.)

7 DR. GUARRO: In 20 years --

8 (Laughter.)

9 CHAIRMAN SIEBER: Yes, Steve.

10 MR. ARNDT: I think we're running about a
11 half hour late, maybe slightly more.

12 MEMBER APOSTOLAKIS: more.

13 MR. ARNDT: If we continue to try not to
14 get any later, I think we're going to be okay. But --

15 MEMBER ROSEN: As you can see, there's
16 some interest in the material.

17 MR. ARNDT: Yes, absolutely.

18 MEMBER APOSTOLAKIS: But I would like,
19 though -- I mean, I would hate the idea that Sergio
20 doesn't hear anything from Maryland. So somehow --

21 CHAIRMAN SIEBER: Yes, let's shoot for
22 finishing by 3:30. But I still think now is a good
23 time to break for lunch. Forty-five minutes I think
24 would be sufficient. That will get us started again
25 at quarter to 1:00.

NEAL R. GROSS

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

1 (Whereupon, at 11:59 a.m., the
2 proceedings in the foregoing matter went
3 off the record for a lunch break.)

4 CHAIRMAN SIEBER: Since people have to
5 travel and so forth, I suggest we continue on without
6 a break until we're done.

7 MR. BONACA: Do you want to skip most of
8 figure number 9?

9 CHAIRMAN SIEBER: Yes, let's move to 9.

10 MR. JOHNSON: I guess one question to
11 start here is how much time would you target for me to
12 try to get through the slides? Do you have a stop
13 point that you want to shoot for?

14 CHAIRMAN SIEBER: I think that our crowd
15 is going to dissipate around 3:30.

16 MR. APOSTOLAKIS: We have one more
17 presentation.

18 CHAIRMAN SIEBER: Yes, we have one more
19 presentation. And it is scheduled for --

20 MR. ARNDT: An hour and 15 minutes.

21 CHAIRMAN SIEBER: Yes.

22 MR. ARNDT: I have a short presentation
23 after that.

24 CHAIRMAN SIEBER: Which is what, 20
25 minutes?

NEAL R. GROSS

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

1 MR. ARNDT: It could be a little less.

2 CHAIRMAN SIEBER: Okay. If you could
3 finish by no later than 2:00.

4 MR. JOHNSON: 1:45.

5 CHAIRMAN SIEBER: 1:45, that's perfect.

6 MR. JOHNSON: I'll try to move through as
7 quickly as possible. The point of this slide is, it's
8 a very, very simple model. You know, most of the
9 models that we deal with are considerably more
10 complicated than that, but the point that I wanted to
11 make with this model is that what we look at in these
12 systems is something we call safety, and we have a
13 definition for that that I'll show you on the next
14 slide. But more specifically, we look at something
15 that's known as the steady-state safety.

16 We know that in these systems that there's
17 some rate at which these problems occur. We just
18 don't know how to estimate that rate, nor do we know
19 how to partition it necessarily between hardware and
20 software, so we are looking at systems that are
21 collections of things, and we know there's a rate. We
22 don't know what it is. We're assuming that there's a
23 coverage that's associated with that, based on the
24 definitions that we've had on the previous chart. And
25 what we're focusing on is how do we estimate

NEAL R. GROSS

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

1 probability of being in one of these two states,
2 either the operational state or the failed safe state.

3 Now more specifically, because we don't
4 know these rates, and don't know how to estimate
5 those, at least I don't, we are looking at something
6 that's known as the steady-state safety. In fact, we
7 have several papers that I'd be happy to make
8 available to you that show solutions of these various
9 types of Markov chains for time varying failure rates,
10 time varying coverage factors and so forth. And one
11 of the things that's intriguing about them is that if
12 you look at this property steady-state safety, you
13 know, as you start out, if you assume you start in the
14 operational state and you transition over time, the
15 probability of being in one of those two states,
16 either operational or fail safe is something that will
17 decay to a constant value, and a constant value is
18 what we call the steady-state safety.

19 And you can show for at least all the
20 architectures that we've looked at to-date, that if
21 you look at that steady-state safety, it'll approach
22 a value that's dependent exclusively on the coverage
23 and not on the rate of occurrence of these events, but
24 on your ability to handle them when these events
25 occur. And so most of our work has focused on this

NEAL R. GROSS

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

1 examination of so-called steady-state safety, and
2 we'll see this show up a little bit later on.

3 MR. APOSTOLAKIS: So that's independent of
4 LAMDA?

5 MR. JOHNSON: That's independent of LAMDA.

6 MR. APOSTOLAKIS: But you have assumed
7 that LAMDA is constant.

8 MR. JOHNSON: We've assumed not that it's
9 constant. In fact, we have in one of our publications
10 the time varying failure rate LAMDA, and you do have
11 to make some assumptions about how it varies with
12 time. I mean, you cannot have arbitrary variation
13 with time, but you can have time variation. We've
14 actually looked at several fairly well-known failure
15 rate functions that do have some time varying
16 properties to them, and we can still show a bounding
17 box essentially for the steady-state safety where you
18 can put a bound on it, depending upon exclusively this
19 coverage factor.

20 MR. APOSTOLAKIS: And C is assumed to be
21 constant.

22 MR. JOHNSON: C in this case is assumed to
23 be constant. We've also looked at the time varying
24 coverage, and again if you make certain assumptions
25 about coverage as it varies over time, you can show

NEAL R. GROSS

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

1 some of the same properties with this bounding. In
2 fact, I'd love to have some other folks look at some
3 of these papers and make comments on them.

4 So again, steady-state safety is what we
5 focus on, since we've shown for certain architectures,
6 it depends on coverage. We focus on how we estimate
7 that coverage, and that's really the focus of the
8 research that we do.

9 Now the challenge, obviously - we've
10 already talked about this a lot, but I did want to
11 make a couple of comments on this, is that software
12 and hardware are not independent entities. The
13 software executes on a hardware platform. One of the
14 interesting things that we found in some of the
15 systems that we've looked at is that a lot of your
16 software oftentimes is developed to handle problems
17 that occur in your hardware, your fault detection,
18 fault management.

19 In fact, we did a survey and looked at
20 both aviation and railroad. We didn't look at nuclear
21 in that case, but we found that in the systems that we
22 looked at, that 80 percent of the software typically
23 was for fault management purposes, or the management
24 of events that would occur in the life of the system.
25 And one of the interesting things in some of the

NEAL R. GROSS

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

1 systems we've done, we've actually found that there
2 are -- we've actually found bugs in software, and the
3 software regimes were there for the detection and
4 management of faults that occurred in hardware, but
5 they were not -- those defects in the software were
6 not made visible until you actually exercised it in
7 the way that it was designed to be exercised in the
8 fields.

9 So this introduces some interesting things
10 where you could have now a fault in the software that
11 would never be a problem if you didn't get a fault in
12 the hardware, or you can have a fault to the hardware
13 that wouldn't be a problem if you didn't have a fault
14 in the software. But the existence of both there can
15 be difficult. So this lack of independence, again, is
16 a focal point.

17 Now a little bit about our methodology.
18 There's a fairly complicated or fairly extensive
19 document that describes all of this, but I guess what
20 I tried to do is to put some of this into a fairly
21 straightforward diagram. I mean again, the types of
22 things we focus on, steady-state safety is the primary
23 one that we look at. We do analytical models. We've
24 actually looked at Markov, and Petri Nets, and fault
25 trees, and dynamic fault trees, and all the ones 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 we've been able to find out there in terms of
2 analytical models. And we've actually done models
3 based on all of them to-date. And from those
4 analytical models, again for steady-state safety,
5 coverage is the key parameter. And then the question,
6 obviously, is how do I estimate that coverage?

7 And we've looked across a spectrum of
8 possibilities there focusing -- really most of our
9 work focuses on the three blocks to the right here,
10 where we create physical prototypes, and we do
11 experimentation on those prototypes. We create
12 simulation models and do experimentation with the
13 simulation models. And by experimentation, I mean
14 fault injection.

15 We have statistical models that allow us
16 to look at the data that we derived from these
17 experiments, and we use that information to estimate
18 predominantly this coverage parameter. That's the
19 primary parameter that we're focused on.

20 MR. GUARRO: I'm just wondering, for those
21 situations that we were discussing or envisioning
22 before in which essentially you may have a design
23 problem in the software, how would the coverage
24 question be posed, because it seems to me that if you
25 have a design issue, you normally would inspect

NEAL R. GROSS

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

1 coverage with that. In other words, if you're
2 encountering a situation that has not been clearly
3 anticipated, unless you have some catch-all type of
4 provisions that are devised in a way that -- hopes to
5 catch unforeseen things. I'm just curious, is there
6 something that addresses that in your approach?

7 MR. JOHNSON: Typically, in most of the
8 systems that we look at, the way that they attempt to
9 address those types of design defects in the design is
10 through diversity, so you have a system that is
11 controlling the turbine, and then you have a system
12 that's overseeing that control, and they are diverse
13 systems. And you're attempting to overcome some of
14 that. A design flaw that could occur in the system
15 that's doing the control by a diverse implementation
16 that hopefully doesn't have those.

17 MR. GUARRO: Okay. I understand, but in
18 terms of your attempt to estimate the degree of
19 coverage that you have, how do you address those type
20 of -- I guess you're trying to develop a C condition
21 or probability of coverage.

22 MR. JOHNSON: You're trying to encapsulate
23 within that coverage both the design and the randomly
24 occurring faults that can occur. And you're
25 attempting to do that by really two mechanisms. One

NEAL R. GROSS

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

1 is the type - in fact, we talked about it earlier -
2 the envelope of faults that you inject, you're
3 attempting to address certain types of design faults
4 in that injection process. Now the difficulty there
5 is how do I model those, how do I represent those?
6 And we don't have a solution to that yet, although
7 it's something we are working on.

8 The other thing that you're doing though
9 is in this experimentation that you're doing, you're
10 exercising the real system, so the design faults that
11 are in the software and the design faults that are in
12 the hardware, you're exercising those as part of the
13 experimentation. And your objective is to try to
14 uncover some of these design faults, and use the
15 information on the number of those that you're
16 uncovering as a means of estimating the probability
17 that there may be design faults remaining in that
18 system.

19 And in the systems we've addressed so far,
20 we have, indeed, uncovered design faults by the
21 experimentation. I'll show you some of those systems
22 in a moment.

23 MR. APOSTOLAKIS: But there is a
24 fundamental assumption behind it though, that these
25 faults that remain and the faults that you are

NEAL R. GROSS

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

1 encountering are exchangeable in some way, and that
2 may not be the case. Maybe there is a single design,
3 there is a design that affects something under certain
4 conditions or under different accident conditions you
5 have something else. This is a pretty strong
6 assumption.

7 MR. JOHNSON: What do you mean by
8 "exchangeable"?

9 MR. APOSTOLAKIS: They come from the same
10 population, and that the order of appearance does not
11 -- in other words, there are four design faults there.
12 If I capture two of them, then I can say something
13 about the remaining two because they are essentially
14 from the same process.

15 MR. JOHNSON: Yes.

16 MR. APOSTOLAKIS: But that may not be the
17 case.

18 MR. JOHNSON: That's an excellent point.
19 That is an assumption that's being made.

20 MR. APOSTOLAKIS: A pretty strong
21 assumption.

22 MR. JOHNSON: It is. And it's one we
23 would like to figure out ways to be able to overcome
24 that.

25 MR. APOSTOLAKIS: I know it's an extremely

NEAL R. GROSS

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

1 difficult problem. And come to think of it, I mean
2 even for the hardware, we don't have any acceptable
3 models for design.

4 MR. JOHNSON: No. And in fact, if you can
5 think about how hardware is designed today, I mean
6 hardware design and software design have become almost
7 indistinguishable, because the way you design hardware
8 is you write a software program that describes the
9 functionalities that you want, and then you use
10 another incredibly complicated piece of software that
11 automatically synthesizes an implementation of that
12 hardware. So your hardware and software design
13 processes have become almost indistinguishable, and
14 the types of problems you create in software, you have
15 the potential to also create similar types of problems
16 in hardware.

17 MR. APOSTOLAKIS: That's right.

18 MR. JOHNSON: It's an interesting paradigm
19 that has come about as a result of the way that we
20 design systems.

21 MR. APOSTOLAKIS: But I think this is
22 really something that bothers me about - not your work
23 only, but in general - attempts to quantify the
24 probability. This assumption that all the design
25 faults are exchangeable is an extremely strong

1 assumption, and that implies the assumption that you
2 can have a failure rate or a constant probability of
3 failure, so it's not quite valid. Now what to do, I
4 don't know. I don't think anybody knows, but we have
5 to acknowledge that we're making some pretty strong
6 assumptions.

7 MR. JOHNSON: I agree with you, and I
8 think it is -- I agree with two things that you said,
9 two that pop out.

10 MR. APOSTOLAKIS: Yes.

11 MR. JOHNSON: One is that it is a strong
12 assumption, and obviously, an assumption that's being
13 made not only in my work, but around the world.

14 MR. APOSTOLAKIS: No, I know.

15 MR. JOHNSON: And the second thing is that
16 it's -- I'm not aware of anybody that has a solution
17 to that.

18 MR. APOSTOLAKIS: I am not either.

19 MR. JOHNSON: And, in fact, I think
20 someone would be quite famous once they find such a
21 solution. It's a hard problem.

22 MR. APOSTOLAKIS: It is a very hard
23 problem.

24 MR. JOHNSON: A very hard problem.

25 The other point - this is a little bit of

NEAL R. GROSS

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

1 a cluttered slide. I apologize for that, but I guess
2 the point that I want to make with this is a couple of
3 things. One is that systems are made up of lots of
4 different things, basic circuit elements, basic logic.
5 You know, typically when you look at systems, you look
6 at them from an architecture all the way down to
7 detail circuit level. And there are several things
8 that are important here. I mean, the whole concept of
9 defense in depth normally is that you're going to put
10 protection mechanisms in at different levels of the
11 system, different layers of the system so that if one
12 thing misses a problem, another thing has the ability
13 to catch that problem. And some of those are not part
14 of the electronic system. They may be mechanical
15 things that you've done, or containment buildings that
16 you've put in place and other types of things, but
17 there are layers of protection.

18 Those layers are subject to design faults
19 because you may have made mistakes in the creation of
20 those protection mechanisms in each of these layers,
21 as well as the function, basic functions. You also
22 have things that just happen, and the random events
23 that occur in the failure of hardware and so forth,
24 and the point of this diagram -- I mean, really when
25 you're talking about designing systems, your objective

1 is to eliminate a problem, either a design fault or a
2 randomly occurring fault that can somehow make it all
3 the way through your protection mechanisms and create
4 a failure.

5 The other point of this chart is that from
6 an analysis standpoint, those are the ones you'd love
7 to be able to find because again, that would be a
8 tremendous insight into the system.

9 Now the other point on the right-hand side
10 of this is that the modeling that we've done - and
11 I'll start at the lower levels because this is
12 important, because when you're looking at a lot of
13 systems nowadays, you don't have access to this
14 information. Part of it's because the way we design
15 hardware nowadays, and even software. You know, you
16 can specify a digital filter in Netlab and synthesize
17 C codes that will implement that, so you may not know
18 a lot about some of these lower levels. So one of the
19 aspects of our research is that what we're trying to
20 do is we are trying to look at these lower levels, so
21 hopefully people in industry don't have to. So we're
22 trying to use the results of the analysis that we do
23 at low levels of hardware and software to try to
24 characterize the elements at higher levels of
25 abstraction, so that that characterization can then 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 by people, and not necessarily require them to go
2 down to these lower levels of detail.

3 The way we've approached the analysis of
4 these systems is that we've done all of this. We've
5 done the higher levels, and we've done the lower
6 levels, and we've used information from these lower
7 levels - in the hardware world they call this back
8 annotation, where you try to extract information from
9 those lower levels and better characterize your model
10 at the higher levels. And what that's leading to,
11 hopefully, in the work that we're doing is a couple of
12 things.

13 Actually, let me hold that thought for a
14 second because it's not the next chart. It's the one
15 after that, that points that out. But first, in this
16 -- particularly these couple of blocks, what we've
17 done is to develop modeling schemes that allow this
18 integrated model. So, for example, we look not only
19 at the actual code levels of modeling these systems,
20 but we look at higher levels, as well, so we can
21 create data flow representations of the algorithms
22 that you're going to run on your computer, and have a
23 way of interfacing that high level description of your
24 system to a high level description of a hardware
25 element. So that, for example, imagine that as you're

NEAL R. GROSS

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

1 simulating this, you have a function that needs to use
2 hardware resources in order to execute, and you don't
3 necessarily know the details of the hardware, but you
4 can characterize potentially the timing and the other
5 fetch and executive processes that you have to go to
6 function, so that there are two points with this.

7 One is that, we do have some models that
8 we've created that are actual bits representing the
9 code running on gate level models of the processors,
10 but we also look at higher levels where you have much
11 more abstract representations of your software and
12 algorithms running on much more abstract
13 representations of your hardware. So the concept of
14 integrated hardware/software modeling is intended to
15 span all of those levels of that diagram I had on the
16 previous chart. So that's part of what the integrated
17 modeling is all about.

18 And then the second thing, the point that
19 I was making earlier is trying to characterize these
20 things. You know, we talked about hardware synthesis
21 a second ago. I mean, for example, suppose that a
22 synthesis program creates an application specific to
23 integrated circuit, and as part of that application
24 specific integrated circuit, it synthesized a little
25 processor and a little memory, and put bits or state

NEAL R. GROSS

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

1 information in that memory that now caused that little
2 processor to, in effect, be embedded in that ASIC.
3 Now is that ASIC now a hardware element, or is it now
4 a hardware/software element? And my argument that it
5 effectively has become a hardware/software element
6 because it has programmable features associated with
7 it, even though it's one-time programmable. The
8 synthesis routines created a program effectively that
9 defines the function of that piece of hardware.

10 So what we're attempting to do, and again
11 we don't have time to go into all of the details, but
12 the attempt here is what I call interface modeling.
13 The idea is to be able to model using state machines,
14 the interface between this device and the outside
15 world, and be able to characterize the things that
16 that can do at the interface when something goes wrong
17 internally, independent of whether it's hardware only
18 or whether it's a mixture of hardware and software.

19 This we can very quickly -- several times
20 we've talked about peer review. And in my world, the
21 key publications that we go to are the IEEE
22 Transactions on Reliability or the IEEE Transactions
23 in general from someone in an electrical engineering
24 department, transactions on computers and transactions
25 on reliability. I've listed just some of the key

NEAL R. GROSS

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

1 publications over the last few years that look at some
2 of the modeling techniques, some of the parameter
3 estimation techniques, statistical models and others,
4 so that's just for reference more than anything else.

5 MR. APOSTOLAKIS: The "IEEE Transactions
6 on Software Engineering" --

7 MR. JOHNSON: "IEEE Transactions on
8 Software Engineering", I personally have not published
9 there, but that's one of the major publications, as
10 well. And there are conferences and so forth, as
11 well.

12 MR. APOSTOLAKIS: Have you ever had a
13 reviewer say you're working with rates that's
14 unacceptable, reject. Since there is so much
15 controversy out there, do you occasionally get the guy
16 who just rejects it outright because you dare talk
17 about the failure rate?

18 MR. JOHNSON: Occasionally, you will get
19 a reviewer that just rejects it outright and doesn't
20 tell you why, but I've not had that particular --

21 MR. ROSEN: It's Tuesday, and I feel like
22 rejecting it.

23 CHAIRMAN SIEBER: That's the way I would
24 read it.

25 MR. JOHNSON: Those are just, again, some

NEAL R. GROSS

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

1 examples of some of the work that we've done. The
2 other thing - again, Steve had indicated that we
3 should put in some things about who's looking at this,
4 and the peer review and other things as more of the
5 examples.

6 As I mentioned earlier, the theoretical
7 foundation for the work that we do was really created
8 when I was at Harris, and I applied the very
9 preliminary ideas to a flight control system that I
10 was working on as part of the team at Harris. Also,
11 one of the products of our modeling and our research
12 is modeling and simulation tools. ADEPT which stands
13 for Advanced Design Environment Prototype Tool, was
14 the first place that we implemented these ideas in a
15 tool set. This was actually funded by NSF and DARPA
16 and NASA, and so that's -- ADEPT was integrated into
17 the metrographics tool set. That was the basis that
18 we used for the ADEPT tool set.

19 ROBUST was the second in our line of tools
20 that was funded by the U.S. Air Force, and we've been
21 -- again, I'm only talking about my particular piece
22 of the center today, but my work has been funded since
23 1984 continuously by all of the organizations that are
24 listed there. And my students that have come out, and
25 the papers that have been peer reviewed, the patent

NEAL R. GROSS

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

1 and so forth, and I've been fortunate enough to be
2 named an IEEE Fellow for the contributions that I've
3 made in this area, so other people have looked at it.
4 And I think that was really the point of this.

5 Applications - I've mentioned several of
6 these, but I wanted to give you a few more specifics.
7 The Los Angeles Metro Green Line was a transit
8 application that we've talked about. We developed a
9 model that had the actual software, the real ones and
10 zeros executing on a model of the hardware. We created
11 results for more than 10 billion experiments, using
12 some techniques that we developed for not just running
13 experiments, but helping you avoid running experiments
14 that were not going to teach you anything. And also
15 running experiments that were meaningful, so there
16 were some 10 billion experiments that were created.

17 We actually uncovered three software
18 design faults in the system. This was a system, this
19 was a software system that had been in the field for
20 almost ten years at 150 different installations, and
21 it was software that was developed using all the right
22 processes, and all the things that were -- and this
23 was an ISO certified house and everything else, and we
24 found three bugs in that software. And that software
25 was updated and revised and so forth as a result of

NEAL R. GROSS

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

1 that.

2 The California Public Utility Commission
3 hired an outside consulting firm to review all of the
4 documents that we created as part of the analysis and
5 to sign-off on those.

6 Copenhagen was very similar, a more
7 complicated system. We did both simulation modeling,
8 as well as physical experimentation, including some
9 gate level things of a modern 32-bit processor. We
10 actually uncovered one software design fault in that
11 particular case, and all of this was actually approved
12 by TUV in Germany.

13 We're currently doing Calvert Cliffs, New
14 York City, CSX, a mag lev system in Pittsburgh, and
15 Illinois Department of Transportation system as well,
16 so those are currently ongoing activities.

17 MR. WHITE: Excuse me, Barry. I would
18 assume that all these systems are very reliable
19 normally, so I think an interesting point to be made
20 here is that you've been able to work with systems
21 where the reliability is already pretty significant,
22 as we would hope would be the case in a nuclear
23 situation.

24 MR. JOHNSON: Absolutely.

25 MR. WHITE: But one of the issues is how

1 do you do an analysis for a very reliable -- a system
2 design to be very reliable, and it would seem to me
3 that you're on track, but if you had any numbers for
4 reliability for any of these systems, it would be
5 interesting. I don't know if you'd be able to divulge
6 any of that or not.

7 MR. JOHNSON: These are -- I can't -- the
8 only thing I can tell you there is that the
9 requirements, what they were shooting for is almost
10 identical to what the aviation industry and others
11 have been promoting over the years; that they're
12 looking at 10 to the minus - anywhere from 10 to the
13 minus 7, to 10 to the minus 9 probability of unsafe
14 event occurring over a life, over a period of time.
15 So those are the types of numbers that they're
16 targeting.

17 I think in all of these cases, again we
18 produce numbers, but I think in all of these cases it
19 really was looked upon as the final number coming out
20 of the analysis was not as important as the analysis
21 itself, and what was demonstrated or learned as a
22 result of doing that analysis.

23 MR. APOSTOLAKIS: Which is what people say
24 about risk assessment.

25 MR. ROSEN: That's what he said all along.

1 MR. JOHNSON: Absolutely.

2 MR. ROSEN: But 10 to the minus 7 or 9 are
3 so low that one has to wonder what do you think about
4 uncertainty for that?

5 MR. JOHNSON: Well, actually, I think
6 that's a huge issue. It's a research issue that needs
7 to addressed, is an uncertainty assessment - because
8 you've got uncertainty in the models, you've got
9 inaccuracies and uncertainty in the models and
10 parameters, and the estimation and so forth.

11 We've actually done -- some of the
12 statistical models are based on some uncertainty
13 principles that are used so that you can at least get
14 an understanding of how much confidence you might have
15 in some of the estimates you're getting out of the
16 model.

17 MR. ROSEN: But if you're saying those
18 kind of very low numbers, you need to be saying
19 something like we think it's between 10 to the minus
20 7 and minus 9, and probably at least an order of
21 magnitude one way or the other, whatever. But you
22 fixed a number in there. The real number is probably
23 within an order of magnitude either way, but you have
24 to say some -- give some decision maker some feel for
25 how sure you are of the result.

NEAL R. GROSS

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

1 MR. JOHNSON: I mean you really have to
2 really understand that issue. I mean, I've been
3 amazed at some results that I've seen published where
4 the accuracy of the computers that they were running
5 these models on wasn't as accurate as the results that
6 they were presenting. You really have to understand
7 those issues, and it is an important problem.

8 MR. APOSTOLAKIS: Was the process for
9 developing all of these systems controlled, or was it
10 as controlled as the nuclear?

11 MR. JOHNSON: Very, very heavily. Very
12 heavily controlled. I mean, they have a very, very
13 rigid process for developing requirements and
14 reviewing those requirements, and developing
15 specifications, and the whole process of -- for both
16 the hardware and the software, very rigid.

17 MR. APOSTOLAKIS: And these systems have
18 been tested before you did your analysis?

19 MR. JOHNSON: Yes.

20 MR. APOSTOLAKIS: And they still haven't
21 found design faults.

22 MR. JOHNSON: Yes. And one of the
23 reasons, and most of these cases, the design faults
24 were the scenario that I had illustrated earlier,
25 where it was never a problem until you had a fault

NEAL R. GROSS

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

1 occur somewhere else in the system. And the
2 combination of the two became now visible. And the
3 reality is that in the field they just had never
4 encountered those situations, nor did they encounter
5 them in the testing process.

6 MR. APOSTOLAKIS: Somewhere else in the
7 system was hardware?

8 MR. JOHNSON: Yes, in this case it was.
9 These were -- in fact, in three of the four that I
10 mentioned here, they were bugs in the software that
11 were only revealed when a certain type of fault in the
12 hardware occurred. Now these software routines were
13 software routines designed to manage the occurrence of
14 faults that could occur both in hardware and software.

15 MR. ROSEN: Doesn't that say that you can
16 test it until you're blue in the face, but that as the
17 system ages and the hardware ages and some of the
18 stuff begins to -- you begin to see some premature
19 failures of something on the cards, that that failure
20 of something on the cards then creates a circumstance
21 in which you'll see a software fault.

22 MR. JOHNSON: Certainly. This data is
23 pointing exactly to that.

24 MR. ROSEN: But that has operation
25 notifications.

1 MR. JOHNSON: It does.

2 MR. ROSEN: One of them is that maybe a
3 strategy to avoid that is to trade-out, as my
4 colleague Dr. Kress says, trade-out cards on a planned
5 cycle as the system matures. Now that has some of its
6 own problems because you can introduce premature
7 failures in the new cards, but at least you're
8 renewing the system rather than just letting all the
9 cards age in time.

10 MR. JOHNSON: I think there are some - and
11 I haven't looked at it any, but I think there are some
12 operational issues that can be addressed perhaps more
13 effectively as a result of some of the things we're
14 learning from the research that's being done. I agree
15 with that.

16 What I wanted to do in just a few
17 remaining slides is just show you a couple of quick
18 things about the Calvert Cliffs system. I won't go
19 into a lot of detail, but again, since we are
20 concerned with nuclear applications here, I just
21 wanted to make sure that you knew we are in the
22 process of working on this one. And actually, have
23 pretty much finished it.

24 One of the things that we're going to be
25 preparing as a report for this year is what I'm

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 calling a Lessons Learned Report, where we're going to
2 essentially talk about some of the things that we
3 learned as a result of applying this to the digital
4 feed on our control system. But this is the system,
5 and again I'm not an expert on nuclear, but
6 essentially it's controlling the water level and the
7 flow of water in and out of the tank, steam
8 generation.

9 MR. ROSEN: Just for interest, it's called
10 a steam generator.

11 MR. JOHNSON: Oh, okay. It's an important
12 part of the process, right?

13 MR. ROSEN: Oh, yes, it's pretty
14 important.

15 MR. APOSTOLAKIS: A minor detail.

16 MR. JOHNSON: Yes. The control system was
17 completely replicated in our lab at UVA, and you'll
18 see a photograph of this. We have two controllers -
19 not a very good photo - PID controllers. We have an
20 experiment control station, which is where we were
21 essentially simulating - I hate to use the word
22 "simulating" in this case, because you're not really
23 simulating the plant, but we're emulating it.
24 Essentially what we were doing is applying from this
25 control station a set of test sequences that were --

NEAL R. GROSS

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

1 there were 23 of them that they used to test the
2 system in their own lab at Baltimore Gas and Electric
3 before they would actually put anything into the
4 field. So it was a sequence of inputs and expected
5 outputs that were being driven on this system, and
6 then our experimentation - the physical part of the
7 experimentation all occurred in this system, so it's
8 a complete replica of what's in the plant, except that
9 obviously we don't have a power plant. We're
10 emulating that.

11 We did develop - this happens to be a
12 dynamic fault tree. And again, I won't go into the
13 specifics of it, but this is a dynamic fault tree of
14 the digital feedwater control system, where we
15 represented several things. The key feature of the
16 dynamic fault tree is the ability to represent
17 reconfiguration and coverage-related matters, so we
18 have -- and this is described in our documents. I'd
19 be happy to make those documents available to you.

20 If you look at just the controller portion
21 of that, there's an equivalent Markov model that you
22 could derive. Again, this is documented as well, but
23 it's very simple because you have two units. You can
24 have both of them working. You can one working, you
25 can have a repair occur during that operation period,

NEAL 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 you can have an unsafe or safe failure of that
2 system.

3 DR. KRESS: Would you call MU a fraction
4 of that that went from two to one and made it back
5 before an unsafe condition --

6 MR. JOHNSON: It's a repair rate but it's
7 exactly that concept, where you have both units
8 working. One of them fails and shut downs, and some
9 time later you'll have it either automatically or
10 physically repaired and brought back on-line, so
11 you're going to have both of them up and running.

12 DR. KRESS: Before an unsafe condition --

13 MR. JOHNSON: Before an unsafe conditions
14 could occur.

15 MR. APOSTOLAKIS: But again, there's an
16 assumption here --

17 MR. JOHNSON: It's a fraction.

18 DR. KRESS: I think it's a fraction.

19 MR. APOSTOLAKIS: All these things rest on
20 the assumption that they are constant, C is
21 constant --

22 DR. KRESS: Yes.

23 MR. APOSTOLAKIS: Otherwise, a Markov
24 model would be --

25 MR. JOHNSON: Again, you can consider time

1 variations and so forth, but this particular case
2 obviously is based on constants.

3 MR. APOSTOLAKIS: So this is a Markov
4 model for what?

5 MR. JOHNSON: This is a Markov model for
6 the two controllers, just the master and the backup
7 controller. It's actually a subset of the fault tree
8 that I showed you earlier.

9 MR. APOSTOLAKIS: Yes.

10 DR. KRESS: These are independent
11 redundant controllers.

12 MR. JOHNSON: Yes. Now if you look at the
13 solutions, I'm going to show both the MTTUF -- let me
14 make a couple of points about this. You know, we
15 don't -- again, because of the -- you know, we don't
16 have a good way of estimating that LAMDA. We don't
17 focus on this piece of it, and this is really -- it's
18 meantime to first unsafe failure, so it's the
19 occurrence of the first unsafe failure.

20 The steady-state safety, though, depends
21 on a couple of the coverage parameters. One that's
22 gained by having these two units compare amongst
23 themselves, and the other that's gained by diagnostics
24 that are running on each of the two units.

25 MR. APOSTOLAKIS: But there is a reason

NEAL R. GROSS

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

1 for that, and the reason is that if you go back to
2 your transition diagram, you're assuming the same
3 LAMDA for both controllers, and they're failing
4 independently.

5 MR. JOHNSON: Yes.

6 MR. APOSTOLAKIS: There is absolutely no
7 coupling because you see from --

8 MR. JOHNSON: They are assumed to be
9 independent.

10 MR. APOSTOLAKIS: Yes.

11 MR. JOHNSON: That's exactly right.

12 MR. APOSTOLAKIS: That's why LAMDA cancels
13 that. Now is that a reasonable thing to do? I don't
14 know.

15 DR. KRESS: Of course, you don't have a MU
16 in there either, so I presume you're --

17 MR. JOHNSON: Yes. The mean time to the
18 first unsafe failure --

19 DR. KRESS: The first unsafe --

20 MR. APOSTOLAKIS: Because MU takes you
21 from one to 200.

22 MR. JOHNSON: That's right.

23 DR. KRESS: No, no.

24 MR. JOHNSON: Now we have -- that's one of
25 the things -- I mean, the paper that I've referenced

NEAL R. GROSS

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

1 here actually looks at more complicated architectures
2 and some of the more complicated models, so there are
3 -- you do have the ability to look at some of these
4 more complicated issues, but it's not addressed in
5 this particular model.

6 DR. KRESS: You have to -- to get this
7 mean time you start out with determining what the
8 failure frequency is.

9 MR. JOHNSON: That's right.

10 DR. KRESS: And they've gone over that.

11 MR. JOHNSON: That's right. And that's
12 why we don't -- again, I show this for reference only.
13 We have not focused on this metric because of the
14 difficulties with estimating this LAMDA.

15 DR. KRESS: But you do get the frequency.

16 MR. JOHNSON: You'd like to have that,
17 certainly.

18 DR. KRESS: You know, this is equivalent
19 to the frequency.

20 MR. JOHNSON: Yes.

21 MR. APOSTOLAKIS: Now I don't know, Sergio
22 and Jim, you have seen more data than I have. Is the
23 assumption that the controllers fail independently a
24 reasonable one, and that they both have the same
25 LAMDA, or could be there some common cause failure?

NEAL R. GROSS

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

1 MR. WHITE: Well, there certainly could be
2 some common cause failure, and I'm sure Barry is aware
3 of that. And I guess it would be interesting to see,
4 and maybe you've addressed it in your paper, what
5 happens if you assume certain degrees of dependence.
6 So how does that affect your results?

7 MR. JOHNSON: We have looked at that.

8 DR. KRESS: You could actually have two
9 controllers out at different LAMDA.

10 MR. JOHNSON: Absolutely.

11 DR. KRESS: That's a complicated --

12 MR. JOHNSON: The results get more
13 complicated.

14 MR. APOSTOLAKIS: But then the result
15 would not be independent of LAMDA, which is your
16 objective.

17 MR. JOHNSON: This would still be
18 independent of LAMDA.

19 MR. APOSTOLAKIS: Would it be?

20 MR. JOHNSON: Yes. Even if the LAMDAs
21 were different you can -- in fact, we've done a
22 generic model where you've got differing LAMDAs --

23 MR. APOSTOLAKIS: So what this is, this is
24 the probability of being in the unsafe state?

25 MR. JOHNSON: This is the steady-state

NEAL R. GROSS

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

1 solution of the safety expression. Safety is the
2 probability of being in either the operational or the
3 fail-safe state.

4 MR. APOSTOLAKIS: So this is safety.

5 MR. JOHNSON: This is the steady-state
6 solution to that particular probability. This is --

7 MR. APOSTOLAKIS: Either in one, or two,
8 or what? I mean, if we go to the previous diagram,
9 which state is that?

10 MR. JOHNSON: It's one or two or the FS
11 state.

12 MR. APOSTOLAKIS: One of the three.

13 MR. JOHNSON: One of the three. That's
14 right. And, in fact, if you look -- if you ignore
15 repair of a system, you know, if you look as time goes
16 towards infinity, what you're going to find is that
17 the probability of being in one of those three states
18 is going to approach a constant value. It'll approach
19 a limit, and that limit is what the steady-state
20 safety is.

21 MR. ROSEN: And that's dependent mostly on
22 the coverage. Is that right?

23 MR. JOHNSON: Yes.

24 MR. APOSTOLAKIS: Only on the coverage.

25 MR. JOHNSON: Only on the coverage.

1 MR. ROSEN: Only on the coverage.

2 MR. WHITE: Okay. Now I have to ask a
3 question I was hoping I wouldn't. The limit as time
4 goes to infinity, that always catches my interest, and
5 that kind of analysis is very useful if you're just
6 trying to get passed a problem and you can do that
7 simplification. I would presume that the times we're
8 talking about are really long compared to other things
9 you're worried about, or not - if they're really short
10 compared to -- so my question is, how limiting an
11 assumption is that if you're trying to estimate a
12 failure rate of a digital system?

13 MR. JOHNSON: Well, if you're looking at
14 the -- again, if you think about the safety expression
15 that we would find early on, and the safety function,
16 what you can show is that this limit is a worst case.
17 I mean, it is because your safety function will decay
18 from -- you know, if you think of safety as the
19 probability of being either operational or fail-safe,
20 it will actually decay from starting point of one to
21 this bound.

22 MR. WHITE: Okay. I don't want to take up
23 the Subcommittee's time, and I'm sure you've thought
24 about this, but there are some cases where that may
25 not be the limiting case. A limiting case - and I may

NEAL R. GROSS

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

1 be wrong. It may be that if the system continues to
2 operate the way you would expect it to, that is worse
3 than if it were to fail immediately, if it's going to
4 fail later on. And I just don't know. It hurts my
5 head to think about it, so I didn't know if you'd gone
6 through that kind of reasoning in any --

7 MR. JOHNSON: We have. We've thought
8 about that. We don't have any results to show on
9 that, but we actually have looked at that quite a bit.
10 There are other things that you can do. When you do
11 start to look at some of the time variations of the
12 parameters and other types of things, you can still
13 find bounds, but they're not -- the bound is not
14 necessarily identical to the steady-state solution.
15 There are some things that show up like that,
16 depending upon repair issues and other types of
17 things, but you can still find a bound that's
18 dependent upon the coverage factors.

19 DR. KRESS: Isn't the PRA likely to use
20 the upper expression?

21 MR. JOHNSON: I'm sorry?

22 DR. KRESS: For use in a PRA, wouldn't you
23 just stick with the upper expression?

24 MR. JOHNSON: I guess my --

25 MR. APOSTOLAKIS: Why isn't one minus this

1 the probability of interest to us?

2 MR. ARNDT: That's the most important
3 parameter.

4 MR. APOSTOLAKIS: But the failure be
5 independent of the rate of challenges? I have
6 difficulty understanding that.

7 MR. JOHNSON: Isn't the probability of
8 failure upon demand? Really, I mean, one minus this
9 would be the probability failure on demand. But
10 again, it's a bound. It's not the actual probability.

11 MR. APOSTOLAKIS: But this is a continuous
12 controlling -- we're controlling the feedwater level
13 continuously, so I should have a failure rate at any
14 time, shouldn't I?

15 MR. JOHNSON: If it's a digital system,
16 you may not. Well, what's continuous and what's --

17 MR. APOSTOLAKIS: What does it demand
18 then?

19 MR. WHITE: In the digital world, that
20 also hurts my head.

21 MR. APOSTOLAKIS: No, but the model itself
22 has a rate of challenges λ , which then disappears.

23 MR. JOHNSON: That's right. Right. And
24 again, it disappears because you're looking at the
25 probability and its limit. If you look at the

1 probabilities at any instant of time, they depend on
2 LAMDA. But if you look at the limit as time gets
3 large, then it will decay. And essentially, your
4 variables that depend upon LAMDA are eliminated from
5 the expressions, because again it's a bound. I mean,
6 if you think -- the simplest example is where you have
7 -- safety might be your coverage plus a term that is
8 exponentially dependent upon time. And as time gets
9 large, the exponential term disappears, and that term
10 goes to zero. And what you're finding in the safety
11 function is that there are some terms that disappear,
12 and there are some terms that remain.

13 In the architectures we've looked at
14 today, the terms that remain are dependent upon the
15 coverage and nothing else.

16 MR. APOSTOLAKIS: Let's go back to 22 for
17 a second. The rate at which I visit the FU state from
18 two or from one depends on LAMDA. Right? LAMDA is
19 there. The rate at which I go into FU depends on
20 LAMDA. Then the steady-state probability of being at
21 FU is independent of LAMDA. That's interesting. I
22 guess you have carried out the calculations.

23 MR. JOHNSON: I'll be happy to show them
24 to you.

25 MR. APOSTOLAKIS: Yes, I'd like to see

1 that.

2 MR. ROSEN: Remind me again, what's cease
3 of S?

4 MR. JOHNSON: Cease of S is a coverage
5 factor but it is specifically the coverage that's
6 provided by diagnostics that are running on a single
7 processor unit. We use the term Simplex, so you have
8 two ways of detecting problems in the system. One is
9 you have comparisons that you're making, and then you
10 have others that are diagnostics that are being run in
11 real time to try to assess the health of the system.
12 That's cease of S.

13 MR. APOSTOLAKIS: There's another --

14 MR. ROSEN: So if you go to your resulting
15 S of SS expression, explain to me what S of SS is
16 that's equal to coverage.

17 MR. JOHNSON: No. S of SS is the
18 probability of --

19 MR. ROSEN: Well, no. Let's go across the
20 equation. It's equal to the coverage times one minus
21 the Simplex.

22 MR. JOHNSON: Right.

23 MR. ROSEN: Times the Simplex squared.

24 MR. JOHNSON: What this is really showing
25 you is that you have a couple of ways of handling

1 problems. Okay? If you detect something by your
2 comparison mechanisms, and you do not detect it by
3 your Simplex or diagnostic mechanisms, then you'll
4 still fail in a safe manner.

5 MR. ROSEN: Okay. That's the term that
6 represents --

7 MR. JOHNSON: If you detect it in both
8 processors using their detection mechanisms, you'll
9 also fail in the safe manner. The case where you will
10 not fail in the safe manner is where you have a
11 problem that is undetected by the unit that's bad, and
12 it's undetected by the comparison mechanisms. So what
13 this is showing you, and again, it's a simple case,
14 but you've got two contributors to the probability of
15 being safe. You detect the problem with your
16 comparisons, and you don't detect it with your
17 diagnostics, or you detect it with both units
18 detecting it via diagnostics.

19 MR. ROSEN: In your diagnostics.

20 MR. JOHNSON: And those are the conditions
21 that lead to a safe failure.

22 MR. ROSEN: I'm sure that will be very
23 helpful after I think about it.

24 MR. APOSTOLAKIS: Let me give you an
25 interpretation of this. Let's go back to the diagram.

1 The diagram is critical here. The states FS and FU
2 are what are called in Markov analysis absorbing
3 states.

4 MR. JOHNSON: They are indeed.

5 MR. APOSTOLAKIS: Once you enter, you
6 cannot get out. If you enter one, you can always get
7 out through -- right?

8 MR. ROSEN: Right.

9 MR. APOSTOLAKIS: So the probability is
10 one that if you wait long enough, you will end up in
11 one of the absorbing states. Right?

12 MR. ROSEN: Right.

13 MR. APOSTOLAKIS: Because you can never
14 get out. The probability is one. I think what the
15 expression that Barry showed us is, is it splits the
16 probability of one between FS and FU, and it says this
17 fraction of time you will be in FS.

18 MR. JOHNSON: That's right.

19 MR. APOSTOLAKIS: And then one minus that
20 is the fraction of time you will be in FU.

21 MR. ROSEN: Yes.

22 MR. JOHNSON: That's right.

23 MR. APOSTOLAKIS: But it is not what you
24 call a safe thing. I am safe as long as I am in one
25 or two, not in FS. FS is a spurious failure.

NEAL R. GROSS

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

1 MR. JOHNSON: No, FS is a safe failure in
2 the sense that --

3 MR. APOSTOLAKIS: Yes, it's a safe
4 failure, but it's a failure.

5 MR. JOHNSON: For example, in the case of
6 --

7 MR. APOSTOLAKIS: What I want is, I want
8 to be in one and two.

9 MR. JOHNSON: Oh, absolutely. Absolutely.

10 MR. APOSTOLAKIS: And that probability you
11 don't have.

12 MR. JOHNSON: No.

13 MR. ROSEN: But that's an operational
14 view.

15 MR. APOSTOLAKIS: But that's what I want.

16 MR. ROSEN: No, no. I think the safety
17 view is what we -- you could think about it in both
18 spaces. Think about it in safety space. All we
19 really care about is that this thing be safe. Then
20 you don't care about LAMDA, because you're satisfied
21 if you're in one, two, or FS. Even if you fail, the
22 system is shutdown, the main feedwater pumps trip, the
23 reactor goes into shutdown and you're safe.

24 DR. KRESS: You can learn something about
25 one and two by the frequencies of these failures.

NEAL R. GROSS

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

1 MR. APOSTOLAKIS: But then I think it's
2 the fraction of time that of the given failures, you
3 will be in FS.

4 MR. JOHNSON: Oh, yes. That's exactly
5 right.

6 MR. APOSTOLAKIS: So it's a conditional
7 thing.

8 MR. JOHNSON: It is.

9 MR. APOSTOLAKIS: It's conditional on
10 knowing LAMDA.

11 MR. JOHNSON: Coverage by definition is
12 conditional.

13 MR. APOSTOLAKIS: Yes, it's conditional.

14 MR. JOHNSON: It is conditional.

15 MR. APOSTOLAKIS: So you cannot take this
16 and put it directly in a PRA, because it's conditional
17 on the coverage.

18 MR. JOHNSON: It is, indeed, conditional.

19 MR. APOSTOLAKIS: Even the coverage. I
20 know that eventually I will be either in FS or in FU,
21 and what that is telling us is the fraction of times
22 you will be in FS is the expression I'm giving you.

23 DR. KRESS: Yes. And then it's going to
24 go on further --

25 MR. APOSTOLAKIS: And it makes sense.

1 DR. KRESS: It's going on further to tell
2 us how you can use fault injection to get these
3 coverages.

4 MR. ROSEN: But he hasn't explained yet
5 how to do it in PRA space.

6 MR. APOSTOLAKIS: Because he's not a PRA
7 man.

8 (Simultaneous speech.)

9 CHAIRMAN SIEBER: Why don't we continue
10 on.

11 MR. JOHNSON: Okay. The fault injections
12 that we've applied to this digital feedwater control
13 system, we've actually done two different approaches.
14 And I'll show you the software-based approach in a
15 second, a simulation-based approach. We've done both
16 software and simulation, software being where, you
17 know, again as the system is executing we're able to
18 insert corruptions into the system in the physical
19 prototype. And then the simulation-based is obviously
20 a simulation.

21 We actually have a scheme that we've
22 developed that uses interrupts in the operating system
23 to do this injection during the execution, so you can
24 think of as the system is running along, you have a
25 brief interrupt that then is your saboteur is the term

1 that's used in the literature quite often, where you
2 then can go in and do various types of corruptions
3 based on the models that you've got, and then allow
4 the system to continue from that point.

5 DR. KRESS: Have you got that automated so
6 you don't have to sit there and type something in?

7 MR. JOHNSON: Yes, we do. We have -- we
8 didn't for a long time, and so my automation was
9 undergraduate students that --

10 (Laughter.)

11 MR. JOHNSON: We have automated much of
12 that now. And then the simulation-based part of it is
13 we've actually migrated this into a COTS tool that's
14 called Simics to allow us to do some simulations.
15 I'll show you a little bit of that in a moment. In
16 fact, this is the Simics.

17 The main point that I wanted to show with
18 this is that where we talked about the entire system
19 and our goal is to be able to model the plant or to
20 get -- we're not going to model the plant, but to get
21 a model of the plant, and have a model of the plant
22 that can be interacting with our model of the system
23 that's controlling the plant. So that, for example,
24 what we've done so far is for the GE turbine
25 controller, we've got a very simple model of the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 plant. We have the -- it happens to be an Intel 386
2 processor with operating system and application code
3 running on that simulation model with interfaces then
4 between this part of the simulation and the digital
5 feedwater control system in the physical prototype.
6 This is all done in physical hardware and software
7 implemented in the lab. This is done by a very simple
8 input/output relationship.

9 In the GE gas turbine controller, this is
10 a completely simulated hardware/software simulation,
11 and then this is a simulated plant model. The
12 objective is to be able to have these fault injection
13 experiments done in an environment where you're
14 actually interacting with a model of the plant that
15 that's going to be interacting with in the real world.
16 And again, this framework allows you to do that, and
17 actually we've done it. And that's built on a COTS
18 tool call settings.

19 Now I guess the last slide, just one
20 comment. I actually debated on whether to put this in
21 here, but I put it in here for the following reason -
22 because I do think that the ideal place to do a lot of
23 the things that we've done and are doing is in the
24 design process. I mean, if you go look at some of the
25 things that are done, there are a lot of people that

NEAL R. GROSS

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

1 design the system and then step back and say how do I
2 make it reliable, or how do I make it safe. And I
3 think that's not the right way to do it. I think the
4 design for safety ought to be an integral part of the
5 design process, and the assessments that we do should
6 really be an integral part of the design process. So
7 that from the very beginning of the system, the
8 simulation environment, which is what I'm calling the
9 virtual prototype - actually, this is taken from the
10 program we did with DARVA where some of these
11 techniques were developed. The program is called
12 Rapid Prototyping of Application-Specific Signal
13 Processors, but the intent was to have a virtual
14 prototype that as you go from start to finish in the
15 hardware/software design process, including
16 integrating and testing, that would all be done in a
17 simulation environment prior to building anything.
18 And all of the fault simulations, simulation-based and
19 so forth that is done in what we developed can be a
20 part of that process.

21 The point of this chart is not that we're
22 there, but the point of the chart is that this is
23 where we would like to go from the standpoint of some
24 of the product of the research so that you've got the
25 ability to integrate some of these things into 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 design process, and you can evolve this assessment as
2 you're evolving the design.

3 MR. ROSEN: It may interest you to know,
4 and I'm sure you do, that this Committee and me
5 personally, are very supportive and insistent even on
6 the use of PRA in the design process.

7 MR. JOHNSON: Yes.

8 MR. ROSEN: Not as an afterthought to
9 evaluate how good did the design come out, but as a
10 first principal thing. First you set down the system
11 definitions and functions, and then you do the PRA
12 first, the first PRA. Then you do a little more
13 detail, a little detailed design, then you rev up your
14 PRA until -- and use your PRA to say, you know,
15 instead of having three of those things there, we
16 really need a more full tolerant kind of thing. Here
17 we need a separate system, more diverse, and I can
18 change these split fractions and get a better answer
19 here. And basically going out like this using your
20 PRA tools until you get to the final design. What
21 you're suggesting now for the software aspects of this
22 is exactly the same thing.

23 MR. JOHNSON: Exactly.

24 MR. ROSEN: And I applaud that.

25 MR. JOHNSON: Exactly. I believe that

1 from the bottom of my heart, that's the right way to
2 do it.

3 DR. KRESS: Now in his iterative process,
4 the ideal is to get the risk down to a level that you
5 accept, and not only to get the risk down to sort of
6 minimize the uncertainties, and to spread the risk out
7 in design in defense-in-depth over a variety of
8 things.

9 MR. JOHNSON: Yes.

10 DR. KRESS: What would be your equivalent
11 to these objectives for the software and hardware?

12 MR. JOHNSON: You know, I think to -- I
13 mean, to some extent I think it's very similar,
14 because I think there are -- you know, as you begin to
15 create a system from a functional standpoint, there
16 are going to be functions even in your software that
17 are going to be more critical than others, because
18 they are going to be -- you know, a good example of
19 that is in the case -- in the GE system that we were
20 working on they use a voting technique. So they go
21 out and they sample a bunch of inputs, and then they
22 come together in each of the units, then uses a
23 software that does a vote across these multiple inputs
24 that they've collected. And if you think about it,
25 you can envision that that voting process may very

NEAL R. GROSS

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

1 well be more critical than some of the other processes
2 that are out there. And if you could understand that
3 from the beginning, that might determine where you put
4 that routine in terms of mapping it to a specific
5 processor. It might determine the level of scrutiny
6 that you apply to that routine in terms of the test
7 and evaluation, and other things that you might do.
8 So I think it's very similar. It's just at a
9 different level.

10 DR. KRESS: The objective would be to end
11 up with the hardware/software, the end that meets the
12 functional requirements at a high reliability level.

13 MR. JOHNSON: Yes.

14 DR. KRESS: Something like that.

15 MR. JOHNSON: I guess I should point out,
16 this is -- I mentioned the DARPA project, which is
17 where some of these concepts were initiated, but they
18 also were further evolved with a project that I did
19 with Boeing, so the objective -- Boeing's objective
20 was exactly what I was describing in terms of the
21 development of aircraft.

22 I am finally at the end. I appreciate
23 your patience, and I appreciate the dialogue and the
24 interaction. As I expected, I learned a lot. I hope
25 you got some information that will be of value to you.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 This repeats what we started with, working on the
2 safety assessment process, integrated
3 hardware/software. We've done it multiple times, not
4 trying to imply that it's in any way finalized, but
5 we've at least had some real experiences with it. And
6 we're continuing to work both in terms of the models,
7 as well as the tools that we're evolving. So again,
8 thank you. Appreciate your time.

9 CHAIRMAN SIEBER: Thank you. And I guess,
10 Steve, we're ready now --

11 MR. APOSTOLAKIS: The chairman insists on
12 no breaks.

13 CHAIRMAN SIEBER: Yes.

14 MR. APOSTOLAKIS: We're doing so well.

15 CHAIRMAN SIEBER: Pardon?

16 MR. APOSTOLAKIS: We're doing so well.

17 CHAIRMAN SIEBER: I think we should not
18 take a break.

19 MR. APOSTOLAKIS: Okay.

20 CHAIRMAN SIEBER: Because people have to
21 leave, and I want them to get as much of the
22 presentations as they can.

23 DR. KRESS: You're the chairman.

24 CHAIRMAN SIEBER: If you have an emergency
25 arising though you may attend to it.

NEAL R. GROSS

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

1 DR. KRESS: You have to raise your hand.

2 MR. ROSEN: The criteria will be you
3 should not make medical history here.

4 CHAIRMAN SIEBER: Or any kind of history.

5 MR. ARNDT: Okay. As I mentioned earlier,
6 another one of our programs is with the University of
7 Maryland. The principal investigator of that project
8 is Professor Carol Smidts. She'll make some self-
9 introduction, as well.

10 MS. SMIDTS: My name is Carol Smidts. I'm
11 an Associate Professor at the University of Maryland
12 in the Center for Reliability Engineering, the
13 Department of Mechanical Engineering. I graduated
14 from the University of Brussels with a Ph.D. in
15 Engineering Physics. My research interests are in
16 probabalistic risk assessment and software reliability
17 modeling.

18 The work I will present this afternoon is
19 essentially geared towards using software engineering
20 to predict software quality or reliability. So what
21 my presentation wants to introduce a method that we
22 have devolved to bring software engineering measures
23 to actually estimates of reliability, and we have
24 piloted this method on small applications which we'll
25 talk about in the presentation.

NEAL R. GROSS

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

1 The results of the method at this point
2 are promising, and the method itself is in that
3 paralleling the review process for software, which is
4 the current process which is used by the NRC staff, so
5 we believe that then it should be straightforward to
6 implement.

7 Work is currently ongoing. We're
8 performing work on the actual nuclear application or
9 we're planning to do that, to actually validate the
10 method on the larger scale application of high
11 reliability, and specific to the nuclear field. So
12 this is to reiterate.

13 When we started the project, the project
14 was geared essentially towards review, and helping the
15 review process to provide somewhat of a systematic
16 framework. Basically, the software developer who
17 comes to the NRC staff and is trying to get the
18 license approved for their system has to go through a
19 process of software development which is characterized
20 in the branch technical position 14, and this is
21 geared at developing plans, developing things such as
22 software maintenance plans, some development plan, and
23 also products, requirements, design, code, test
24 results, and things of that nature.

25 Now the reviewer at NRC then has to look

1 at this information, and from there infer whether or
2 not the application should be accepted, so there is no
3 quantitative measurement going on in that process
4 really. Plus, at this point, the measurements that
5 the licensee wishes to provide can do anything, as we
6 discussed this morning.

7 So project history - we actually inherited
8 this project from Lawrence Livermore National
9 Laboratory. We started in 1996, and what Lawrence
10 Livermore did is actually identify the first set of
11 measures, software engineering measures that they
12 believed were relevant to reliability. We then
13 performed an expert opinion study to try to rank these
14 measurements, and we performed a small scale
15 validation study in 2001. And we're currently
16 enlarged in the large scale validation study.

17 So Steve trapped me into doing this slide,
18 and I'm still wondering why I did it. So here what
19 I'm showing is what I understand to be the
20 contributions that we believe we can at this point
21 assess if we were to use the reliability estimates
22 we're producing. So if you look at this event
23 sequence diagram representation, what we're trying to
24 show is what we believe are all the contributors of
25 software, or contributors related to software, so at

1 the very top of the diagram, what we do have --

2 MR. APOSTOLAKIS: You've got a pointer
3 there. Can you use it?

4 MS. SMIDTS: Sure. So what we do have
5 here is whether or not the support platform functions
6 correctly. So this is actually the work that Barry
7 concentrates on, which is to look at support platform
8 degradation. And this is cases where the support
9 platform actually functions correctly. And then what
10 we do have is that the software gets inputs from
11 sensors or humans and things like that, and this input
12 needs to be characterized. We call it operational
13 profiles sometimes. It's actually really the
14 definition of the input. The software executes, and
15 there's a delay of execution of the software depending
16 on the input which we, at this point, do not
17 characterize. No environment measurements actually
18 look at that.

19 Then there is an assessment whether or not
20 the behavior that is specified in the requirements is
21 actually implemented, and that is what we're looking
22 at - whether the behavior leads to a safe condition.
23 And some of our measures actually look at that. And
24 then let's assume that indeed the requirements are
25 followed, well, it is also possible that the output

NEAL R. GROSS

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

1 still doesn't match what is the output required by the
2 next component in the process, and we do not
3 explicitly look at this. So I think this explains a
4 little bit the context of what we do.

5 So here is our work. We look at software
6 engineering measures, and try to create subsets of
7 measures which can then be related to reliability. We
8 may be able to create only one such subset, or we may
9 be able to create several such subsets. If that's the
10 case, it will be possible in the future to imagine
11 that we could use another uncertainty framework to
12 actually create better estimates for the reliability,
13 so for these blocks here.

14 MR. ROSEN: George, you should be thrilled
15 at this point.

16 MR. APOSTOLAKIS: I can't control myself.

17 MR. ROSEN: Besides that.

18 MR. ARNDT: Well, what's important to
19 recognize is this is a method to help us quantify, to
20 make the software review process more quantifiable.
21 And it also has the opportunity to tell us something
22 about the reliability.

23 MS. SMIDTS: Okay. So what is the idea
24 behind this research? In other words, why would we
25 want to look at software engineering measures, and how

NEAL R. GROSS

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

1 can we possibly relate them to software reliability?

2 Well, basically software reliability is
3 determined by the characteristics of the product, so
4 the software, and the characteristics of the
5 operational environment which I call the input.

6 Now the product characteristics are
7 actually determined by characteristics of the project,
8 such as the type of application, and characteristics
9 of the development environment, such as the skill
10 level of the people involved in the development, or
11 such as the schedule pressures and things like that.

12 Now these characteristics are actually
13 measured by software engineering measures which apply
14 to all of these elements. So in essence, software
15 engineering measures are actually determining software
16 reliability.

17 MR. APOSTOLAKIS: Wait. I don't
18 understand the last bullet. How does that follow from
19 the --

20 MS. SMIDTS: So what I said is that
21 basically the reliability of the product is determined
22 by the product itself, how it is, actually the
23 functions in the product, the logic in the product and
24 so forth and so on. And it's also determined by the
25 development in the operational environment, how that

NEAL R. GROSS

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

1 product is executed. So the features of the product
2 are influenced not immediately but indirectly by the
3 project characteristics and the development
4 characteristics.

5 MR. APOSTOLAKIS: Software engineering
6 measures, what are these?

7 MS. SMIDTS: Those can be many types of
8 things, such as, for instance, the logic complexity of
9 a module, the number of lines of code in a module. It
10 could be things like the number of requirements. The
11 fact that requirements are traceable to the system,
12 the software requirements are traceable to the system,
13 and so forth and so on, there is a very large number
14 of such measures.

15 MR. APOSTOLAKIS: But this is an
16 assumption really. I mean, why is the number of lines
17 determining the software reliability? It depends on
18 how you wrote it.

19 MR. ARNDT: Right. There's a whole body
20 of research associated with what things, how many
21 errors or how many problems you have in software, and
22 then you come out with the size of the code, the
23 complexity of the code, the amount of times you change
24 the code, all sorts of different kinds of issues.
25 Many of those are measured for one reason or another.

NEAL R. GROSS

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

1 We're trying to understand the quality of the code, or
2 we're trying to improve the efficiency of the code,
3 trying to do a quality process in the development of
4 the software or whatever. There have been measures
5 that are used for various reasons.

6 MR. APOSTOLAKIS: So what doesn't follow
7 though is that they determine the reliability. They
8 influence the reliability. They are indirect measures
9 of the reliability, but they do not determine the
10 reliability.

11 CHAIRMAN SIEBER: No, they don't. But you
12 have to interpret some of that too. For example, it
13 sort of follows to me anyway, the more lines of code,
14 the more chances for mistakes.

15 MS. SMIDTS: Right.

16 MR. ROSEN: Well, it's not linear.

17 MR. APOSTOLAKIS: No, because I may have
18 a million reviews.

19 CHAIRMAN SIEBER: Yes.

20 MS. SMIDTS: So that's why you would want
21 then to combine that other measurement, which tells
22 you how many measurements, I mean, how many --

23 MR. APOSTOLAKIS: What matters is the
24 whole process.

25 MS. SMIDTS: Right. So you would want to

1 get all these measurements together, and together they
2 actually should give you a pretty good --

3 MR. APOSTOLAKIS: That's the whole point
4 of controlling the process.

5 MS. SMIDTS: Right. Right.

6 CHAIRMAN SIEBER: But if you set out to
7 minimize the lines of code, you may be simplifying the
8 algorithms to the point where you don't get very good
9 answers, and so there are a lot of conflicting kinds
10 of things here. I think the best thing to do is hire
11 the smartest person you can to do the programming.

12 MS. SMIDTS: If they are too smart, then
13 the code is really difficult to maintain.

14 CHAIRMAN SIEBER: Yes, I know about that.
15 Smart, not tricky.

16 MS. SMIDTS: So the idea here was to
17 postulate the existence of subsets of measures that
18 could help us determine reliability. Now since we
19 don't know what those subsets are, and we don't know
20 what are the models that need the subsets to
21 reliability, what we wanted to do was to be able to
22 rank these subsets since NRC staff would actually get
23 several measurements, and they would have to determine
24 whether these sets of measures are actually going to
25 product good estimates of reliability. Do they help

NEAL R. GROSS

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

1 us identify what the reliability of the product is, or
2 is the set of measurements insufficient?

3 So basically, we can't rank these sets.
4 So the idea is that we decided to start by ranking
5 individual measures with respect to reliability, and
6 hoping that by obtaining these rankings, we would be
7 able to actually build sets that would lead us to top
8 reliability prediction systems, that's how we call
9 them.

10 Now to rank the measures, and I should --

11 MR. GUARRO: Carol, I'm sorry. You're
12 saying you set out to rank individual measures?

13 MS. SMIDTS: Yes.

14 MR. GUARRO: Okay. Well, you probably
15 guess what the next comment is; which is, it seems
16 that there would be very strong combinatorial effects,
17 in the sense combination actually, not combinatorial,
18 combination effects so that depending on environment
19 and situations, the relative ranking of measures could
20 change from one situation to another. Have you
21 thought about that?

22 MS. SMIDTS: Well, that's what I would
23 have thought too, but as you will see, the results of
24 the experts don't really seem to indicate that. I
25 mean, we were trying to take experts which were coming

NEAL R. GROSS

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

1 from very diverse backgrounds to try to cover the most
2 generic of cases. We took people from the
3 telecommunications industry, from financial industry,
4 from aerospace and nuclear, and so forth and so on, to
5 try to cover all the possible aspects.

6 MR. GUARRO: Well, I'll give you an
7 example in which you could force the number of lines
8 of code down to the point where you generate logical
9 errors. And I know of situations in which at least
10 you could run into that type of problem when you're --
11 for reasons of efficiency. There's a certain type of
12 processor that don't accept a lot of lines of code.

13 MS. SMIDTS: Okay.

14 MR. GUARRO: And again, I'm conditioned by
15 this bit system experience where we still use because
16 of space qualification issues. We use processors that
17 are, in terms of technology, they're 25 years ago.

18 CHAIRMAN SIEBER: Z-80s.

19 MR. GUARRO: Right. Also, in certain
20 languages are line of code intensive and certain
21 languages are not.

22 MS. SMIDTS: Right. So if were to look at
23 the lines of code that these people created, probably
24 you would see that other measurements would show that,
25 such as - I'm thinking about cyclimatic complexity,

1 which show that the logic has become very complicated,
2 so you would have --

3 MR. GUARRO: Yes, but I mean that's the
4 point.

5 MS. SMIDTS: Right.

6 MR. GUARRO: You're in an environment
7 which now, you know, if you're in a free environment
8 where the lines of code are just left completed
9 unconstrained, well, then probably yes, there you will
10 find that the more lines of codes that people want to
11 right, the more errors they may produce. But in an
12 environment in which the lines of codes are
13 constrained, now that factor, that particular metric
14 is not free to influence the reliability as it in
15 others. So something else flips ahead of it. So what
16 I'm saying, if you're ranking one-by-one
17 independently, you might not see these combined
18 effects.

19 MS. SMIDTS: You wouldn't. You wouldn't
20 see the combined effects. Yes, because we are ranking
21 them one-by-one. Right. So another -- well, one of
22 the things we could do in the future is to try
23 actually to rank them by several factors, but we
24 haven't done that.

25 MR. GUARRO: Well, I guess one way of

1 saying that is that the issue perhaps looked at
2 different sets of environments in which the
3 combinations of factors act in different ways.

4 MS. SMIDTS: Differently, yes.

5 MR. ARNDT: And one of the reasons we're
6 trying to do pilot studies in various applications,
7 particularly the nuclear domain dependent application
8 for that very reason. We want to be able to valid the
9 methodology in the kind of environment that we're
10 interested in.

11 MS. SMIDTS: Okay. So this part of the
12 slide that actually shows the criteria that we
13 selected for the ranking of the measures, so one of
14 the criteria is actually the relevance to reliability
15 of the measurement. The other criteria try to assess
16 the internal validity of the measure, so what we have
17 here is, for instance, how costful the measurement is,
18 what is the benefit of having this measurement to the
19 organization. Has this measure been validated
20 extensively by the scientific community, has there
21 been much experience, industrial experience with this
22 measure. Here, what is the level of credibility of
23 the measure; in other words, does it actually assess
24 the goal of the measure, and finally if this measure
25 is repeatable or not. In other words, if performed

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 repeatedly by different individuals, do we get the
2 same measurement.

3 MR. APOSTOLAKIS: These overlap a lot,
4 don't they? I mean, the degree of credibility depends
5 on everything else, and the validation - V depends on
6 R. The more people use it, the more validated it is,
7 isn't it?

8 MS. SMIDTS: Right, but this the
9 validation really by the scientific community. Here
10 we would look at the industrial experience, so you may
11 have a lot of validation from us, from the scientific
12 community and nobody is ever using this measure.

13 Repeatability actually is really in the
14 way the measure is being defined. Now we find that
15 some measures like lines of code have a very low
16 degree of repeatability, but they're used throughout
17 industry largely.

18 MR. APOSTOLAKIS: Repeatability. What is
19 repeatability again?

20 MS. SMIDTS: Repeatability is the fact
21 that you can make a measurement - if you and I make
22 the same measurement, do we get the same result. And
23 a lot of the --

24 MR. APOSTOLAKIS: You said something about
25 the number of lines of code.

NEAL R. GROSS

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

1 MS. SMIDTS: Right.

2 MR. APOSTOLAKIS: What kind of measurement
3 would that be, just the number of lines?

4 MS. SMIDTS: Right.

5 MR. APOSTOLAKIS: Do you disagree?

6 MS. SMIDTS: Yes.

7 MR. APOSTOLAKIS: Why would we disagree?

8 MS. SMIDTS: Because there are multiple
9 definitions of the line of code to start with, so
10 actually one of the problems that is in this field, my
11 experience with this field now is that most of the
12 measures are very readily defined. Repeatability is
13 the real problem.

14 So this is the ranking process that we
15 actually followed. So the first step in our work was
16 to actually narrow down the set of measures that
17 Lawrence Livermore had identified to 30 measures.
18 Actually, in the set that Lawrence Livermore had
19 prepared, there were things that actually were not
20 measures, but techniques, things that were models and
21 not measures either, so we narrowed that down, and
22 then restricted to a set of Perti because we were
23 gearing up for expert opinion elicitation. And we
24 thought our experts would not be able to rank more
25 than 30 measures. So step two was expert

NEAL R. GROSS

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

1 identification.

2 Now why did we perform this? We tried to
3 look in the literature to see whether or not there
4 would be some data that would allow us to rank the
5 measurements on our own. And actually, it's very
6 difficult to find any relevant data. The data may be
7 there, but it's usually proprietary and companies will
8 not share it, so the only way we thought we could
9 actually approach this problem is by expert opinion
10 elicitation.

11 So we identified a set of 10 experts, and
12 I'll show you the name of the experts in the next
13 slide. We defined the criteria specifically, and
14 identified levels for the criteria. So for instance,
15 for the experience criteria we had five levels, from
16 a case where there was absolutely no experience with
17 the measure, to cases where hundreds of companies had
18 used the measure.

19 So in the next slide, we also design a
20 questionnaire which we sent to the experts. The
21 experts sent us their ranking back, and then we held
22 a workshop to actually look at, and the experts
23 actually explained their ranking. We also had
24 interviews with the experts after the workshop to
25 follow-up on some of their results.

NEAL R. GROSS

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

1 We had left intentionally a door open in
2 the sense that we allowed experts to identify what we
3 call missing measures, so if they believed we had
4 missed some important measurements, they actually
5 indicated that.

6 The next step, we aggregated the opinions
7 of those experts using utility fields, and this
8 framework, the utility field framework has a number of
9 parameters, such as the weights of each of the ranking
10 criteria and so forth and so on. We performed a
11 sensitivity analysis to see whether or not within
12 bounds that we thought were acceptable or reasonable,
13 whether the rankings would be actually modified. Then
14 we analyzed the results.

15 So here are the experts. They were
16 selected out of a set of 30 initial candidates, and we
17 see the backgrounds of those experts. It's industry,
18 academia mix, some have actual experience both in the
19 industry and the academia. And here are the areas in
20 which they actually -- the domains in which they work.
21 All experts have knowledge with critical systems, with
22 actually software reliability, and software
23 measurement.

24 Here is the set of measures which we
25 considered initially, and here are the results of the

NEAL R. GROSS

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

1 ranking. Actually, the experts provided rates for
2 each of the measures in different phases of the
3 development life-cycle. So a rate of zero essentially
4 means that the measure is worthless, and a rate of one
5 means that the measure is actually excellent.

6 As you see in the requirements phase, we
7 have very little measures available because some of
8 the measures become defined only in the later phases
9 of the life-cycle, by testing all the measures
10 available.

11 MR. APOSTOLAKIS: Are these -- you had
12 what, 12 experts?

13 MS. SMIDTS: Ten.

14 MR. APOSTOLAKIS: Ten. So if I look at
15 completeness requirements, you say .41 - don't tell me
16 all 10 said .41. So how did you come up with .41?
17 What is the dispersion?

18 MS. SMIDTS: The dispersion - do you
19 remember, Ming, what is the dispersion, because I
20 don't remember. How much dispersion --

21 MR. APOSTOLAKIS: You have to come to the
22 microphone if you want to speak, and say who you are.

23 CHAIRMAN SIEBER: For the record.

24 MR. LI: I'm Ming Li. I'm the post doc
25 researcher for Dr. Smidts. And this research actually

NEAL R. GROSS

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

1 is my Ph.D. topic. I have been working on it for over
2 six years. And I found the number of repeats of that
3 measure should be around four to six out of ten
4 experts.

5 MS. SMIDTS: No, that's not the question.
6 The question was, was there a lot of dispersion in the
7 rating of the experts.

8 MR. LI: Oh, okay. Fine. Well, since we
9 ranked using the latter scale, and if converting to
10 zero to one, I would say 30 percent around. We didn't
11 calculate that rigorously and have the statistics, but
12 I will say it's around from -- let's say from letter
13 D to letter B, something like that.

14 MR. APOSTOLAKIS: Let me understand. What
15 exactly did you ask the expert to give you regarding
16 completeness?

17 MR. LI: Well, for each measure - do you
18 want to continue?

19 MS. SMIDTS: Yes. So for each measure, we
20 asked them to tell us for each of the ranking criteria
21 what was the level of that particular ranking
22 criterion.

23 MR. APOSTOLAKIS: On a scale of what?

24 MS. SMIDTS: So the scales are -- they go
25 from letter -- let's say there are five levels, so

NEAL R. GROSS

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

1 from letter A to E.

2 MR. APOSTOLAKIS: And then you converted
3 it to a number.

4 MS. SMIDTS: Right. So what we did is
5 actually, because we weren't sure that the conversion
6 would not change the numbers which, of course, it
7 does. It changes the number, but we wanted to verify
8 whether or not the ratings remained correlated, so we
9 performed a sensitivity analysis later on that.

10 MR. APOSTOLAKIS: So in terms of the
11 letters then, for a particular one, what did they give
12 you? Did you have a situation where somebody gave an
13 A, somebody gave an E, another guy gave a C - it was
14 all over the map?

15 MS. SMIDTS: We had cases like that.

16 MR. APOSTOLAKIS: So what does that tell
17 you?

18 MS. SMIDTS: That there was, in that case,
19 indetermination between the different cases. But most
20 of the cases were not like that.

21 MR. APOSTOLAKIS: They were like what?

22 MS. SMIDTS: One letter grade probably.

23 MR. APOSTOLAKIS: From all ten of them?

24 MS. SMIDTS: From all ten of them. No, I
25 mean maybe most of them were A, and then some gave B.

1 So I --

2 MR. APOSTOLAKIS: Remarkable.

3 MS. SMIDTS: I didn't study the -- I don't
4 have in mind the actual variations of the experts.
5 But it wasn't outrageous, like you would assume that
6 -- I mean, it wasn't like you had a person gave E, and
7 then everybody else -- and then one gave D, and two
8 gave C, and then one gave A. It wasn't that bad.

9 MR. APOSTOLAKIS: And then you converted
10 the letter scale to a numerical scale using what?

11 MS. SMIDTS: We actually did that using
12 different curves. And what we did is we actually
13 performed a sensitivity analysis on the different --
14 we varied the curves, the transformation.

15 MR. APOSTOLAKIS: Now when you use
16 additive, you really have to make sure that the
17 measures are independent. I mean, there is an
18 implication of remarkable accuracy when you say .15.
19 And it seems to me that some sort of statement of
20 uncertainty would be required there.

21 MS. SMIDTS: Okay.

22 MR. GUARRO: Now when you're saying you
23 used these curves, you adopted actually one curve for
24 all the measures, or depending which measure you were
25 dealing with, you used a different curve?

NEAL R. GROSS

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

1 MS. SMIDTS: So we used one curve for all
2 the measures, and then we looked at the rating at that
3 point. Then we used another curve for all the
4 measures, and what we were trying to do is to see
5 whether or not the ratings were correlated for these
6 different curves. And we did that for all these
7 different curves. And then since we were looking at
8 an aggregation framework which was additive, so we had
9 different weights for the different criteria, and we
10 varied the weights. So these are the sensitivity
11 analysis schemes we looked at, those different
12 weights.

13 MR. APOSTOLAKIS: So these are weights
14 that you show there?

15 MS. SMIDTS: Right. Here.

16 MR. APOSTOLAKIS: Yes, and these are your
17 weights.

18 MS. SMIDTS: This is the first -- these
19 are my weights.

20 MR. APOSTOLAKIS: These are your weights,
21 not the experts'.

22 MS. SMIDTS: They're not the experts', no.

23 MR. APOSTOLAKIS: Why didn't you ask the
24 experts to also tell you relative importance --

25 MS. SMIDTS: I asked them to give me 30

NEAL R. GROSS

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

1 measures, and for these 30 measures, I had how many
2 criteria - seven criteria, and I had four phases of
3 the life-cycle. So I didn't ask them the weight.

4 MR. APOSTOLAKIS: So what is it that we
5 learn from this, Carol? Can you tell us what the
6 conclusion from all this is?

7 MS. SMIDTS: Yes. I mean, my conclusion
8 is the actual measurements which are important are
9 relevant, and the others which are not.

10 MR. APOSTOLAKIS: So which are they?

11 MS. SMIDTS: Okay. So these are for the
12 different phases of the life-cycle, the best
13 indicators of reliability. Now some of them are
14 obvious, of course, like failure rate. Now here we
15 have code defect Ansically, which is surprising, but
16 the experts considered that there is a lot of
17 experience with this measure, and this measure
18 actually measures the flaws in the code, the defects,
19 so it is relevant to reliability.

20 MR. APOSTOLAKIS: It measures the defects?

21 MS. SMIDTS: Yes.

22 MR. APOSTOLAKIS: So you know how many
23 there are?

24 MS. SMIDTS: That's what the measure gives
25 you.

1 MR. APOSTOLAKIS: Then what do you do, you
2 say --

3 MS. SMIDTS: That's the defects found.

4 MR. APOSTOLAKIS: Oh, these are defects
5 found. And why is the --

6 MS. SMIDTS: Because actually they
7 normalize it to the lines of code. But the measure
8 itself, you have to understand, the measure is not on
9 the number of defects per line of code. It's also the
10 location of the defects found, the nature of the
11 defect, the type of the defect, so it's all the
12 information that was relevant to that defect, and
13 identified in inspection.

14 MR. APOSTOLAKIS: So again, there is an
15 implication as I was saying earlier to Barry, that
16 these defects that you found are exchangeable with the
17 ones you have not found. And that's a pretty strong
18 assumption.

19 MS. SMIDTS: Well, found is defect found.
20 If you have several inspectors that inspect at the
21 same time, you have some models, and I haven't done
22 that. I haven't pushed the research to that point
23 yet, but if you have multiple inspectors inspecting,
24 you can actually calculate through some statistical
25 models to recapture models. You can calculate the

NEAL R. GROSS

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

1 number of defects remaining.

2 MR. APOSTOLAKIS: No. That's where I
3 disagree.

4 MS. SMIDTS: You do disagree.

5 MR. APOSTOLAKIS: They all assume that
6 these things -- I suggest we --

7 MS. SMIDTS: Homogeneous.

8 MR. APOSTOLAKIS: Yes. Not exchangeable.

9 MS. SMIDTS: Homogeneous, yes, in that
10 sense.

11 MR. APOSTOLAKIS: Yes.

12 MS. SMIDTS: Yes. The only thing it gives
13 you then is a first order estimate of what the number
14 of defects remaining may be.

15 MR. APOSTOLAKIS: Sure. I mean, if I find
16 lots of defects, I form an opinion about the process.

17 MS. SMIDTS: Right.

18 MR. APOSTOLAKIS: Right. I say, you know,
19 these guys really didn't know what they were doing.

20 MS. SMIDTS: Right.

21 MR. APOSTOLAKIS: But presumably, you
22 never do that in a strictly controlled process, I
23 hope.

24 MS. SMIDTS: Well, that's what you
25 believe.

NEAL R. GROSS

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

1 MR. APOSTOLAKIS: Yes, well, I can only
2 believe what I believe.

3 MR. WHITE: Excuse me, Carol. The
4 coverage factor rate says third most important in the
5 testing phase. Is that correct?

6 MS. SMIDTS: Right. In the sense that
7 that measurement you can get at this point only during
8 the testing, because what you do is you actually
9 inject flaws and you measure whether or not it can
10 recover from the flaw. So it becomes important on
11 event, because it becomes available on the event.

12 MR. WHITE: Okay. What is fault number
13 days?

14 MS. SMIDTS: Fault number days I think is
15 actually the number of days that the fault remained in
16 the application. Is that correct?

17 MR. WHITE: But how do you note that under
18 the requirements? Say under requirements column, I
19 see fault number days as rank number 5.

20 MS. SMIDTS: Right.

21 MR. WHITE: What does that mean?

22 MS. SMIDTS: So it would be, let's assume
23 we start the development process, and then how much
24 time did it take for us to detect the critical fault.

25 MR. ARNDT: After it was put into the

NEAL R. GROSS

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

1 process.

2 MR. WHITE: Yes. Thank you.

3 MS. SMIDTS: Yes.

4 MR. GUARRO: Can you elaborate on the
5 definition of the design defect in implementation
6 versus design fault in the design phase?

7 MS. SMIDTS: Yes. So design defect
8 density is actually in the same type of code defect
9 density. It's the same type of measure. Design
10 defect density is actually assessed with respect to
11 the number of lines of design, so this would be with
12 respect to - let's assume you have a design document,
13 and you actually measure the number of lines of
14 design. And you would actually then calculate --

15 MR. GUARRO: Okay. But essentially,
16 defect for you is any variation from requirements?

17 MS. SMIDTS: Or it could be problems in
18 the requirements.

19 MR. GUARRO: Okay.

20 MS. SMIDTS: Inconsistent, incorrect,
21 ambiguous, anything.

22 MR. GUARRO: Okay. I understand that. So
23 now in the design column, what is a fault, and how is
24 it different from a defect?

25 MS. SMIDTS: Okay. So a defect, if I

NEAL R. GROSS

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

1 remember correctly, is something that you identify by
2 inspection.

3 MR. GUARRO: I understand the difference
4 between defect and fault in the execution, so to
5 speak. Fault is as executed, defect is just there.
6 It may not be called upon. Am I interpreting it
7 correct?

8 MS. SMIDTS: Yes.

9 MR. GUARRO: In other words, a defect is
10 a latent fault, but is not an active fault.

11 MS. SMIDTS: Right.

12 MR. GUARRO: So I'm trying to understand
13 what fault means in the design column, because in the
14 design phase you will not know if something is being
15 executed or not, so it's really a defect, isn't it?

16 MS. SMIDTS: Yes. However, you may have
17 let's say a simulation at the design level which would
18 allow you to infer that you have actually some kind of
19 a failure, so if you're --

20 MR. GUARRO: Yes. But you're not using a
21 reoperational profile --

22 MS. SMIDTS: No, we're not.

23 MR. GUARRO: -- so it's really speculation
24 whether that is a defect or a fault. You see what I'm
25 driving at? I don't --

NEAL R. GROSS

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

1 MS. SMIDTS: However, you have -- I mean,
2 you're right because you're not in the real
3 environment. But in the sense that you know whether
4 or not this would create a failure, it is your
5 assessment, of course. Yes.

6 MR. GUARRO: Because you're using a
7 postulated profile.

8 MS. SMIDTS: Right.

9 MR. GUARRO: And a postulated code itself,
10 because you're still in the design.

11 MS. SMIDTS: Right.

12 MR. GUARRO: Okay.

13 MS. SMIDTS: So you have the -- yes.

14 MR. GUARRO: I'm just trying to understand
15 the definition.

16 MS. SMIDTS: No problem. So here are the
17 missing measures that were identified by the experts.
18 Actually, the missing measures identified were the
19 first four ones. And actually when we started, we
20 were not considering OO projects or OO software,
21 object-oriented software, because at that point there
22 was little experience with object-oriented for safety-
23 critical systems, so the experts recommended that we
24 add a category of measurements which would capture
25 object-oriented programming. So this is actually what

NEAL R. GROSS

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

1 we did here, we added those measurements for that.

2 The first one that they recommended was
3 the coverage -- I mean, one of the first ones was the
4 coverage factor for fault architectures. Then that of
5 a full function point for real time systems. They
6 believe that full function point was more relevant to
7 real time systems than function point, which is
8 another measure that we have.

9 CHAIRMAN SIEBER: Which number of
10 children, fourth from the bottom?

11 MS. SMIDTS: The number of children I
12 think is when you have a parent class, and the number
13 of derived classes from that parent class. Okay. So
14 this is the result of our sensitivity analysis, and
15 what we -- I think we looked at 100 and something
16 sensitivity analysis variations. And of those, you
17 see that most of the variations are actually with a
18 correlation coefficient, which is superior to .9,
19 which is very encouraging in those results.

20 Okay. So now the hardware we are trying
21 to actually validate our method, so we performed a
22 validation on small scale studies. So this is the
23 method which we applied. The first part, of course,
24 is the selection of the application. We took an
25 application which was a small control system, which

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 was real time in that sense. It was pertinent to what
2 the NRC types of applications are.

3 In the next step, we were looking at which
4 measures to actually select for the validation. And
5 we considered a limited number of measures due to the
6 small scale of the validation study. We took measures
7 which were highly ranked measures, which were ranked
8 medium, and measures which were ranked low to see
9 whether or not we could see actually whether the
10 predictions were actually following that trend.

11 MR. ARNDT: This was also because we
12 wanted to gain information on whether or not the
13 licensee comes in with a ranking, be it high, medium,
14 or low, or what amount of credibility they assigned to
15 that.

16 MS. SMIDTS: Right. So in the third step,
17 we performed the reliability assessment. So what
18 happens is that we split our research team in two
19 components. One component actually was performing
20 measurements, and trying based on those measurements
21 to predict reliability. And another part that the
22 team considered to be a team that knew what the ideal
23 behavior should be, so they actually had what we call
24 the Oracle, the perfect behavior, or assumed perfect
25 behavior.

1 Now in the fourth step, what we did is we
2 actually tried to construct those reliability
3 prediction systems. In other words, we tried to
4 bridge what we knew the measures for reliability. In
5 step five, we performed measurements and analysis.
6 And in step six, our results of peer review.

7 So here are the small scale systems that
8 we considered. The first -- so this is personal
9 access control system to enter in a building. The
10 first system was devolved by industry. It was
11 devolved following the Capability Maturity Model, and
12 that particular company at the time was rated at level
13 4, and they were asked to perform this development at
14 level 4. This was actually -- we used the system in
15 another study that was sponsored by NSA, so the code
16 was devolved in C++, and the reliability of that
17 application is .92 per demand, around .92 per demand.
18 So it's not a very high reliability system. It's a
19 low-medium reliability.

20 DR. KRESS: When it was unreliable, refuse
21 access to somebody that should have been --

22 MS. SMIDTS: Let in.

23 DR. KRESS: Or let somebody in they
24 shouldn't have.

25 MS. SMIDTS: Right. Right. So then since

NEAL R. GROSS

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

1 we wanted to see whether or not we could use what we
2 had devolved on a more reliable application, we
3 actually asked West Virginia University to develop
4 another version of this same system, again in C++.
5 And here, the reliability is much higher with this
6 system. It's .999 per demand. This work was
7 sponsored by NASA. So the measures which we are using
8 in the validation were these, two high-ranked, two
9 medium, two low.

10 SPEAKER: Before you leave the slide,
11 should I draw any kind of conclusion from the fact
12 that you had a CMM level 4 that was reliability of .92
13 per demand? And if so, what would that conclusion be?

14 MS. SMIDTS: The conclusion would be that
15 you cannot trust that you cannot trust a CMM level to
16 tell you what is the reliability of the application.
17 And now if you want to probe further, I can tell you
18 that this is because there are no real measurements
19 which are required by CMM. It's a process without
20 actual final measurement.

21 MR. ARNDT: There have been several
22 studies related to the CMM process and its ability to
23 predict the quality in the software. And there's
24 been a lot of controversy associated with it,
25 obviously because it's an important issue,

NEAL R. GROSS

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

1 particularly in military software development. And
2 many of those studies have shown various issues, in my
3 opinion the most important of which are for classes of
4 software. You get a good prediction, you narrow it
5 down to single codes with reliability or the validity
6 of that becomes more difficult as you might think.
7 Also, as the code size shrinks, like sometimes in say
8 the critical real time systems, the validity of CMM as
9 a predictor of quality goes --

10 MS. SMIDTS: Yes.

11 MR. ARNDT: That's one of the many reasons
12 that SEI, Software Engineering Institution, has looked
13 at individual code, individual measures for
14 individuals or small teams, as opposed to whole
15 companies, which are more applicable to smaller codes.

16 MR. GUARRO: Carol, this may be a silly
17 question, but why mean time to failure was included as
18 something to test? I mean, it's essentially a
19 parameter that defines reliability so, of course, it
20 will be highly correlated with reliability.

21 MS. SMIDTS: Yes, you're right. So
22 actually what we did is that in the second study,
23 PACS-2, we took it off.

24 MR. GUARRO: Okay.

25 MR. APOSTOLAKIS: It's not the true mean

NEAL R. GROSS

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

1 time to failure, is it?

2 MS. SMIDTS: It's not the true.

3 MR. APOSTOLAKIS: So somebody estimates
4 it, so it makes sense.

5 MR. GUARRO: But it's essentially the only
6 measure that you have out of your system that tells
7 you what the reliability may be.

8 MS. SMIDTS: Yes. So I've been going back
9 and forth because, I mean, for the first study what we
10 did is that the team that was performing the
11 measurement calculated the mean time to failure. And
12 the team which had the Oracle, calculated the failure
13 rate. Now they're not the same perception of the
14 system, yes.

15 MR. GUARRO: Yes. Okay.

16 MS. SMIDTS: Okay. So this is the
17 environment that we used to perform the reliability
18 assessment, so using this Oracle. So what we do is we
19 start actually from the requirements, and the team
20 develops, analyzes the requirements and devolves a
21 finite fake machine that represents the behavior of
22 that system.

23 Then if you put that in some test
24 generation tool, such as the Test Master Tool, well,
25 you can automatically generate test cases, and those

NEAL R. GROSS

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

1 test cases are run automatically by a test execution
2 tool which is not WNRRunner, but WinRunner, so that
3 allows us to run a very large number of tests
4 automatically actually. And the failure/success is
5 captured also automatically.

6 MR. APOSTOLAKIS: So this is your
7 approach, these boxes?

8 MS. SMIDTS: This is -- so what we -- what
9 I was saying is what we did is we split out team in
10 two parts. One part was measuring and was trying to
11 assess reliability, and the other part was supposedly
12 the Oracle. And that team defined this, so this
13 represents the Oracle and the testing using this
14 perfect image of what the system should be. So then
15 what we do is we try to compare the results.

16 MR. APOSTOLAKIS: Did you at any time
17 actually look at the process that the NRC has blessed
18 for the development of software? This is your
19 approach. Right?

20 MS. SMIDTS: Right.

21 MR. APOSTOLAKIS: Did you look at that?

22 MS. SMIDTS: I looked at the process. I
23 read the documents which are related to that. No,
24 this is just a process to assess what the reliability,
25 the true supposedly reliability of the application is.

NEAL R. GROSS

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

1 MR. APOSTOLAKIS: But I thought what you
2 were trying to do was to ultimately go - maybe I was
3 wrong - go through the process that the NRC staff has
4 established and say based on whatever I have learned,
5 if you really follow this process you end up with a
6 reliability of such and such.

7 MS. SMIDTS: Right.

8 MR. APOSTOLAKIS: Isn't that what you --

9 MR. ARNDT: Not quite. What the idea is,
10 is to -- the process that the licensees need to follow
11 is laid out. What's laid out is how we're going to
12 review their process.

13 MR. APOSTOLAKIS: Yes, I agree with you.

14 MR. ARNDT: What we're trying to do is
15 inform our review of their process by adding a
16 quantity of measures.

17 MR. APOSTOLAKIS: Yes, but they will
18 follow the process that you have in your SRP.

19 MR. ARNDT: Right.

20 MR. APOSTOLAKIS: So at some point you
21 could take these insights, apply them to that process.

22 MR. ARNDT: Right. What we're trying to
23 do is update the process, our review process so that
24 we look at things that are the most important to final
25 system reliability. And this is designed to find out

NEAL R. GROSS

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

1 if there are measures that are going to help us do
2 that.

3 MR. APOSTOLAKIS: Now are there any
4 measures -- I mean, from Professor Johnson's
5 presentation, we learned that in some of the errors
6 that he caught, there were hardware/software
7 interactions. Are any of the 30 measures addressing
8 that?

9 MS. SMIDTS: That was the coverage factor,
10 actually. So that one actually --

11 MR. APOSTOLAKIS: The coverage factor is
12 the same as his coverage factor, and that's the only
13 one.

14 MS. SMIDTS: There are others -- let's say
15 there are others that probably look at it indirectly,
16 such as, if you look at requirement traceability, what
17 requirements traceability does is look at whether the
18 software requirements are traceable throughout the
19 development of software. But also, if the software
20 requirements are traceable upstream to the system.

21 MR. APOSTOLAKIS: Yes. I have a couple of
22 examples in my mind of actual failures, and I'm
23 wondering how this approach relates to that. There
24 was a case that I read some time ago where the pilot
25 in a fighter plane commanded the software to raise the

NEAL R. GROSS

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

1 landing gear while the plane was on the ground, and it
2 went down. And then, of course, they realized that
3 the software should have an interlock of some sort
4 that said if you're on the ground, don't do that.

5 CHAIRMAN SIEBER: Or get a new pilot would
6 be good too.

7 MR. APOSTOLAKIS: Now that is a
8 requirements problem, is it not?

9 MS. SMIDTS: Yes.

10 MR. APOSTOLAKIS: Would your approach find
11 anything like that?

12 MS. SMIDTS: Well, normally in the
13 requirements they should actually define what are the
14 range of correct inputs in different situations.

15 MR. APOSTOLAKIS: Right. But in this case
16 there was an incorrect situation, I guess.

17 MS. SMIDTS: Right. So all --

18 MR. APOSTOLAKIS: So would you find that?

19 MS. SMIDTS: Well, in the case you're not
20 in the range of correct input, you should have
21 specified behavior for inputs that are not within that
22 range. If such are not defined, there is a problem in
23 the requirements.

24 MR. APOSTOLAKIS: And I know there is a
25 problem.

NEAL R. GROSS

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

1 MS. SMIDTS: Okay.

2 MR. APOSTOLAKIS: The question is whether
3 your method would find that problem.

4 MS. SMIDTS: Right, because you would have
5 --

6 MR. APOSTOLAKIS: How would you find it?

7 MS. SMIDTS: You would have normally a
8 measurement that would tell you that the requirements
9 are incomplete, because that range of parameters
10 outside the correct range is not considered.

11 MR. APOSTOLAKIS: Which measure of the
12 therapy would do that?

13 MS. SMIDTS: Well, requirements
14 completeness, for instance.

15 MR. APOSTOLAKIS: Requirements
16 completeness. Yes, it's easy to talk about
17 requirements completeness but somebody has to actually
18 evaluate it.

19 MS. SMIDTS: Right.

20 DR. KRESS: You have to have a complete
21 set of requirements.

22 MR. APOSTOLAKIS: Right. And I think
23 that's what part of the problem is, isn't it? That
24 you need somebody with an imagination, in this case
25 maybe it doesn't take much imagination but it does,

NEAL R. GROSS

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

1 that would say you need this. So I don't know whether
2 any formal methods, or any of this, or even what Barry
3 is doing, whether it would find something. I don't
4 know.

5 MS. SMIDTS: So actually, to go back to
6 one of the first slides I have is that actually you
7 have to create those input conditions depending on the
8 sequence in which you are, you need to assess what is
9 the set of input conditions that that software is
10 going to seek.

11 MR. APOSTOLAKIS: And I agree with you.
12 And it seems to me this is the real issue we're facing
13 in the nuclear industry. Right? The software may get
14 some inputs that command you to do something that is
15 inappropriate for that particular context. And that,
16 it seems to me, is more a matter of technical
17 knowledge on the part of the designer than anything
18 else.

19 MR. ROSEN: You got hold of a very good
20 point I think, George. Let's take some real
21 operational circumstances, for example. Let's take a
22 case, a plant I know where three trains of central
23 cooling water should never all be out of service at
24 once.

25 MR. APOSTOLAKIS: Exactly.

1 MR. ROSEN: And let's say this plant was
2 digitally controlled, and one could give a command to
3 the software to take out a train of central cooling
4 water. And then one could go to the next train, to B
5 Train. Let's say you did it to A, and then go to B
6 and do the same, and they would accept the second
7 command too. But when you went to the third train --

8 MR. APOSTOLAKIS: Should refuse.

9 MR. ROSEN: -- it would refuse to take out
10 the train, so that's the third train, because the
11 other two are out. You have to put one back before
12 you can this one out. Now that should be a
13 requirement in the requirement software.

14 MR. APOSTOLAKIS: And my question is
15 whether the methods we've been discussing here from
16 Virginia and Maryland, if the designer had made the
17 mistake and allowed all three to be out, would any of
18 these match this? Again, this is not -- don't take me
19 wrong. I'm not actually criticizing you. I'm
20 addressing what I think is the real issue in nuclear
21 safety.

22 MR. ROSEN: I understand, but I don't
23 think you can ascribe that to the software. I think
24 the software --

25 MR. APOSTOLAKIS: It's a design, the

1 design of the software.

2 MR. ROSEN: The designer of the plant has
3 to work with the designer of the software to say
4 amongst all the thousands of other things he wants the
5 software to do --

6 MR. APOSTOLAKIS: I want you to do that
7 one.

8 MR. ROSEN: -- I want for the central
9 cooling water never to be take out three trains at
10 once.

11 MR. APOSTOLAKIS: That's right.

12 MR. ROSEN: And this will not allow an
13 operator to do one, two, three, or the software to
14 make a fault in which it automatically takes out all
15 three. If it tries to do that, or even succeeds to do
16 that, there's a fault error message. There's an error
17 message pops up immediately, and the software takes
18 another algorithm and puts one of the trains back in
19 service, or something like that.

20 MS. SMIDTS: So that actually should be
21 specified in the system requirements.

22 MR. APOSTOLAKIS: I agree. What should
23 have been done is clear. Whether you catch it is the
24 issue.

25 DR. KRESS: It's just like the PRA

1 completeness issue.

2 MS. SMIDTS: Right.

3 DR. KRESS: If you're incomplete, you're
4 not ever going to find it until something happens and
5 you say oh, I should have had that in my PRA too.

6 MS. SMIDTS: Right.

7 DR. KRESS: This is the same way. You
8 will never find it with any of these messages, and you
9 can't hope to.

10 CHAIRMAN SIEBER: No, you can't ask
11 software to --

12 DR. KRESS: You can't ask it to do that.

13 MR. GUARRO: That is true, but the
14 question is, for example, if there are ways of
15 analyzing the interactions between hardware and
16 software that help identifying situations in which key
17 requirements have not been identified.

18 MS. SMIDTS: And the answer is that in any
19 reliability assessment we do, be it based on measures
20 or anything, one of the primary issue is to
21 characterize the input space, because once you
22 characterize the input space, you will be able to
23 trigger conditions that may not be represented in your
24 software model.

25 MR. GUARRO: Exactly. I think that's the

NEAL R. GROSS

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

1 key point, whether there are ways to generate the sets
2 of input conditions in a way that essentially probes
3 the design of the integrated system. It's the same
4 type of story of the example we were discussing
5 before, the one that I'm familiar with because it
6 comes from this basis and environment. That was not
7 a software problem specifically, because if you
8 hotwired their own parameter value into an analog
9 controller, it would have caused exactly the same
10 failure.

11 MR. ROSEN: Damage the valve are you
12 talking about?

13 MR. GUARRO: Well, the overreactive launch
14 vehicle control system that ran the system out of
15 hydraulic fluid. And that's a particularly tricky
16 one, but there are things of that nature that if you
17 have some orderly way of verifying the requirements
18 and looking at the spatial requirements, I think it
19 can help you think in the right direction. I don't
20 think that there is any particular silver bullet that
21 automatically says okay, here are your missing key
22 requirements. Unless you look at the hardware and
23 software together, you're not even triggered to think
24 in that direction, so I think that's the key thing
25 too.

1 DR. KRESS: I was wondering if the
2 University of Virginia processed moving from the left
3 to the right, iterating with a simulated system would
4 uncover something like that. You would ask -- at
5 every point along the line you would ask your system
6 if the plant has some sort of unacceptable failure,
7 what conditions would make it lead to that. That
8 might be one of the things you have to pick up.

9 MR. APOSTOLAKIS: Still though, if you
10 went there with a mindset that when I command it to
11 raise the landing gear it has to do it, without ever
12 thinking that if I'm on the ground I shouldn't allow
13 it, then you probably convince yourself, even with
14 this approach that it's okay.

15 DR. KRESS: I think you --

16 MR. APOSTOLAKIS: It comes down to
17 technical --

18 MR. ARNDT: The basis you're going to have
19 to have, as we discussed earlier in the day, a
20 detailed understanding of what you're trying to
21 accomplish in the system.

22 MR. ROSEN: And knowledge of the system
23 itself, whether it's an airplane that wants to crash
24 itself on the ground, or a Delta rocket with a
25 hydraulic control system, or in a central cooling

NEAL R. GROSS

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

1 water system that can't have all three systems out at
2 once. And nuclear, aerospace and airplane requires an
3 initial definition of the system requirements by the
4 engineer, not of the software but of the engineer of
5 the system.

6 MR. APOSTOLAKIS: Exactly.

7 MR. ROSEN: And then once those
8 requirements are set down, then it becomes the job of
9 the software engineers to accurately translate them.
10 But absent having the system requirements from the
11 engineers of the system, the software process is
12 doomed to start with.

13 MR. APOSTOLAKIS: I'd like to come back to
14 the various measures that you have evaluated. If we
15 all agree that this is really a major, if not the
16 major problem with software requirement specification,
17 are we creating a false sense of security by looking
18 at things like number of lines, density of faults.
19 That's where the action is. Shouldn't we be focusing
20 on this issue? Like, for example, I don't think you
21 have a project on formal methods.

22 MR. ARNDT: We have a small project that's
23 part of the --

24 MR. APOSTOLAKIS: Now these guys claim
25 that they check for internal consistency. Now again,

NEAL R. GROSS

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

1 if internal consistency means I want to raise the
2 landing gear and I always do it, then that doesn't
3 help.

4 MS. SMIDTS: No, it doesn't.

5 MR. APOSTOLAKIS: It doesn't help me
6 either.

7 MS. SMIDTS: No.

8 MR. APOSTOLAKIS: Why should I care about
9 what you do, Carol?

10 MS. SMIDTS: Well, you should because I
11 look at the combination of the input conditions. I
12 force you to actually look at the input conditions,
13 because you cannot create a reliability estimate if
14 you don't define the input conditions.

15 MR. APOSTOLAKIS: Absolutely agree with
16 that.

17 MS. SMIDTS: I cannot --

18 MR. APOSTOLAKIS: But which of your
19 measures deals with that?

20 MS. SMIDTS: The measures themselves, the
21 30 that are there don't.

22 MR. APOSTOLAKIS: Are doomed.

23 MS. SMIDTS: So I have to add measures to
24 my set to actually get that.

25 MR. APOSTOLAKIS: Well, now you're

NEAL R. GROSS

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

1 talking. I would really love to see those measures.

2 MR. WHITE: But what about your measure of
3 review inspections and walk-throughs? So my question
4 is, and I think what we found on the panel was, if
5 these reviews inspections and walk-throughs are done
6 by the equivalent of plant engineers, that's good.

7 MS. SMIDTS: Yes.

8 MR. WHITE: But if it's done by a bunch of
9 software engineers, then you're going to get into the
10 same problem because you're going to miss these other
11 -- so which of these did you mean in reviews
12 inspections and walk-throughs?

13 MS. SMIDTS: Is that the one in the
14 requirements phase?

15 MR. WHITE: That's one of the pre-selected
16 30 measures.

17 MS. SMIDTS: Okay. Those are done at
18 different phases of the life-cycle, typically by
19 different groups of individuals. So if you're early
20 in the life-cycle requirements phase, you will have
21 plant engineers in that group. You will have user
22 representatives in that group.

23 MR. ROSEN: That's the key, that the user
24 representatives get on board I think the day the
25 contract is signed for the new system. The very first

NEAL R. GROSS

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

1 person after the project manager who is assigned, the
2 project manager picks up the phone and calls the
3 equivalent of a plant engineer and says put yourself
4 on an airplane and be here at 8:00 Monday morning.
5 We're starting the design of the new whatever.
6 Airplane, space system - because it's his input that's
7 crucial for almost everything you do from that point
8 on.

9 MR. APOSTOLAKIS: I would suggest -- maybe
10 you're already thinking about it, Steve, that you have
11 somebody, a group or whatever, think about this issue
12 of requirements. What is it that we can learn from
13 the existing literature on faults that have been
14 found, and what can be done about it? I agree with
15 Sergio and Tom, that it's an issue of completeness and
16 our brains cannot handle issue of completeness in a
17 sense that we can prove that something is complete.
18 But as Sergio says, there might be ways that can
19 guide, that would enhance the probability that you
20 will identify something in the process. It seems to
21 me that's so important that it certain -- that doesn't
22 mean you can do this at the expense of this or
23 something else, but it's such an important thing that
24 it seems to me by itself should be a task.

25 I've looked at a number of these things,

NEAL R. GROSS

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

1 and it's not really the fault of the software, it's
2 the system. The guy who designed the whole thing that
3 either didn't foresee something, or didn't know
4 enough, or whatever.

5 MR. ROSEN: Had never flown an airplane
6 like that or something like that.

7 MR. APOSTOLAKIS: Yes.

8 MR. ROSEN: But the minute you put someone
9 on the team who has flown an airplane like that and
10 his life depended on it, he will tell you his life's
11 anecdotes in very brief time, and you'll make sure you
12 don't make those mistakes at least again.

13 CHAIRMAN SIEBER: I don't want to
14 interrupt but there are 13 slides in 10 minutes.

15 MR. APOSTOLAKIS: Ten minutes, 35 minutes.

16 MS. SMIDTS: Okay.

17 CHAIRMAN SIEBER: No, we're going to let
18 Steve also talk.

19 MR. APOSTOLAKIS: Steve can talk after
20 3:30. I'm here.

21 CHAIRMAN SIEBER: I will encourage -- you
22 may even want to pick out the best of your slides --

23 MR. APOSTOLAKIS: The best of the best.

24 MS. SMIDTS: Okay. So --

25 MR. APOSTOLAKIS: And the most legible.

NEAL R. GROSS

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

1 MS. SMIDTS: Okay. So one of the things
2 I wanted to say though is that I know you insist a lot
3 on requirements, but do not forget that there are a
4 lot of implementation errors also. So this is -- I
5 have 10 minutes? Okay.

6 CHAIRMAN SIEBER: You're skipping the
7 interesting part.

8 MS. SMIDTS: Okay.

9 MR. APOSTOLAKIS: When challenged, she
10 responds.

11 MS. SMIDTS: So here are the results -- so
12 these are -- so what I skipped is actually the
13 building of the prediction system from the different
14 measures. So what you can see is actually for PACS-1
15 on the left-hand side, you have the values which are
16 obtained for the different measurements, so this is by
17 the measurement team. And here you have the predicted
18 probability of success by each of those measurements.

19 We're using in this box here - what you do
20 have is the actual correct evaluated probability of
21 success of the system. So here is just the relative
22 error for the different predictions.

23 MR. ARNDT: Predicted relative error.

24 MS. SMIDTS: Right. Predict relative
25 error? No, the actual relative error for each of

NEAL R. GROSS

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

1 these. So here is the original rankings of the
2 experts, and here is actually the rankings that we
3 obtained based on validation. So some of the results
4 we get is that as you see the high-ranked measures
5 produce the best estimates, medium-ranked measures
6 product not as good estimate. And, of course, low-
7 ranked measures produce actually relatively bad
8 estimates.

9 So the same thing -- so this is another
10 thing I wanted to show you, is that the method that we
11 use for validation is actually reviewed by these four
12 experts. These people were pretty familiar with our
13 research earlier because they had participated in the
14 expert opinion elicitation. They didn't flag any
15 major significant problems with the --

16 MR. APOSTOLAKIS: Where is Michael Lyu
17 now?

18 MS. SMIDTS: He's in Hong Kong, University
19 of Hong Kong. Okay. So here the study carried out
20 for the second application, so here is the reliability
21 estimation, and here again is the rankings obtained
22 based on expert opinion. And here again, the rankings
23 based on the validation. Here the predictions from
24 the different measures, I mean reliability prediction
25 sets.

NEAL R. GROSS

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

1 MR. APOSTOLAKIS: What is number one?

2 MS. SMIDTS: We took it out. We took the
3 mean time to failure out from this study.

4 DR. KRESS: Now if you had, I say looked
5 at the dispersion of the predictions, would that have
6 changed your opinion?

7 MS. SMIDTS: From the experts you mean.

8 DR. KRESS: Yes. You might have had a
9 bigger dispersion for some of these than others, and
10 it might change your opinion of which ones --

11 MS. SMIDTS: Are actually --

12 DR. KRESS: Right.

13 MS. SMIDTS: Yes, that's a possibility.
14 I'll consider that definitely. Okay. So here are
15 some of the publications that relate directly to this
16 work. The expert opinion study was actually published
17 in Transactions and Software Engineering, and here is
18 some other publication. What we use actually, the
19 predictions to reduce the amount of testing. This is
20 some other things that can be used for it, that can
21 serve as some prior estimates. And we can reduce the
22 amount of tests that needs to be performed on an
23 application.

24 So our current research is to look at an
25 actual system for the nuclear industry, and we have

1 picked the STAR system, which is used at Oconee. And
2 this is the Safety STAR System, reactor protection
3 system.

4 We've also extended the number of
5 measurements we're going to look at so this is now a
6 total of 12 out of the 30 measures. And we're going
7 to consider the different phases of the life-cycle
8 requirements design coding and testing, and see what
9 those different phases tell us about the reliability,
10 and what we can extract from that.

11 MR. ROSEN: What did you say, it was done
12 at Oconee?

13 MS. SMIDTS: The STAR system. It's a
14 digital system used for the reactor protection system.

15 MR. ROSEN: Okay. It's a new digital
16 system for Oconee.

17 MS. SMIDTS: Right. So we'll continue
18 working on the improvements for those reliability
19 prediction systems. And one, of course, of the major
20 problems is getting defects, and what to do about
21 them.

22 So as a summary, the summary just repeats
23 in the same way that Barry had, we have the summary
24 slide repeat the conclusion slide that was the second
25 slide of our presentation. So we worked on a method

NEAL R. GROSS

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

1 to use software engineering measures for predicting
2 reliability. The results of the method so far as
3 promising.

4 We think the method can be used in the
5 current review method, and the work is going on on a
6 nuclear application, large OCS.

7 CHAIRMAN SIEBER: Are there any questions
8 that anybody would have?

9 MR. WHITE: That haven't been asked
10 already.

11 CHAIRMAN SIEBER: Right.

12 MR. GUARRO: What is the time frame for
13 carrying out your next validation?

14 MS. SMIDTS: I think that we have two
15 years. Is that correct? Yes. We started in
16 December, so we just started actually.

17 CHAIRMAN SIEBER: Well, thank you,
18 Professor Smidts.

19 MS. SMIDTS: Thank you.

20 CHAIRMAN SIEBER: That was a very good
21 presentation, and we appreciate your coming here.

22 MS. SMIDTS: Thank you.

23 CHAIRMAN SIEBER: Steve, I think you have
24 -- in fact, you finished early by two minutes.

25 MR. APOSTOLAKIS: Steve, you are repeating

NEAL R. GROSS

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

1 yourself here. You're describing ongoing problems.
2 We've done that.

3 MR. ARNDT: Then I'll work through it very
4 quickly.

5 MR. APOSTOLAKIS: Why don't you go through
6 the slides that you like.

7 MR. ARNDT: I will go through the slides
8 I like.

9 MR. OVERLAND: I've been in and out
10 randomly, and every time I come in you're giving him
11 a hard time.

12 CHAIRMAN SIEBER: You should have been
13 here the whole time. Let's let him make his
14 presentation here.

15 MR. ARNDT: Okay. What I want to do is
16 talk a little bit about future things, particularly
17 things I haven't talked about before. Some of these
18 things we have talked about before, and I'll just give
19 them 20 seconds of time. I'd also like to talk about
20 some things that we're planning on doing, and based on
21 our input from this and other inputs we may revise
22 that.

23 Continuing new research is planned, with
24 basically trying to investigate different aspects of
25 the assessment process. If you recall from my

NEAL R. GROSS

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

1 introductory comments, we're trying to do several
2 things. We're trying to improve the current process,
3 we're trying to make it more qualitative - I'm sorry,
4 more quantitative. I'll get it. And we're trying to
5 work toward the ability to do real risk assessment of
6 this area.

7 We're trying to provide tools and guidance
8 to NRR so they can do better assessments. And we're
9 trying to coordinate this both internally, both
10 between the PRA groups and I&C groups, as well as in
11 various international and national groups in the
12 nuclear area.

13 As Barry mentioned, this new work is going
14 to be on one of the three generically approved
15 platforms that actually work on COTS software, and
16 continue to develop this as a potential independent
17 assessment methodology.

18 As Carol mentioned, she's starting to work
19 on a large-scale application, full life-cycle so we
20 can actually look at all the life-cycle areas, both to
21 assess what's most important in the review, and also
22 to give us some more quantitative measures.

23 DR. KRESS: You've done this one time
24 expert opinion ranking.

25 MR. ARNDT: That's correct.

1 DR. KRESS: So we've got that.

2 MR. ARNDT: Yes.

3 DR. KRESS: And one thing you might want
4 to think about is the dispersion, but do you plan some
5 sort of update as you accumulate data as you go
6 through these things?

7 MR. ARNDT: Part of the process of all
8 this is research program planning both for what
9 programs are we going to do, what we're going to try
10 to accomplish in those programs and things like that.
11 And that's part of the research planning you'll hear
12 about in a couple of months. But also, it's
13 continually reassessing both the methodologies and new
14 methodologies as they become available.

15 One of the biggest challenges in this area
16 is not only is the technology changing, but the
17 ability to assess things is changing. So you'll
18 notice that in the BNL work, in Barry's work, he did
19 an assessment, in BNL's work - they did an assessment.
20 And talk about some of the future work, we're also
21 going to probably do an assessment. The idea is to
22 update that issue.

23 In the case of Carol's ranking, you'll
24 notice that the file cases basically validated the
25 experts' opinions so I don't think that's necessary to

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 the point, but the larger-scale study demonstrates the
2 things that give us better predictions of reliability
3 in nuclear-specific applications not working out the
4 same way, then we'll probably do an update.

5 DR. KRESS: Yes. Well, it's quite a bit
6 more lines of code. You might expect some --

7 MR. ARNDT: Right. It's a different
8 domain, although there are similarities. I mean, it's
9 a real time system, it's a no-go kind of system and
10 kind of things, but it's different and we would expect
11 some differences.

12 MR. APOSTOLAKIS: I thought this morning
13 you told us that BNL will think about methods for
14 including software in the PRA.

15 MR. ARNDT: Yes.

16 MR. APOSTOLAKIS: The first bullet here
17 seems to say that they have already decided to use a
18 Markov model?

19 MR. ARNDT: It says one of the things
20 they're looking at, development of a process, Markov
21 model, one of the three platforms to identify the
22 splitting analysis need to support individual
23 features. What we're talking about doing is having
24 them do that analysis at that level.

25 MR. APOSTOLAKIS: I must say I'm a little

NEAL R. GROSS

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

1 cool to the whole idea. Markov model means you have
2 transition rates, and to get anything useful out of
3 it, you have to assume they are constant, and that
4 justifies that. So I would expect them to start with
5 that and think about whether it's appropriate to use
6 a Markov model or something else.

7 MR. ARNDT: Okay. That's why we're
8 discussing future plans with you. That's the whole
9 point.

10 MR. APOSTOLAKIS: No, I'm not questioning
11 this, but I'm a little surprised because the
12 impression I got in the morning was that they would
13 essentially have free-hand to look at what's available
14 and try to put things together. And now this says oh,
15 no, no, no, they have already decided to use a Markov
16 model.

17 MR. ARNDT: Continue review of the
18 database, particularly in conjunction with other
19 database work, and look at some of the quantitative
20 methods for assessing software reliability in
21 conjunction with the other software.

22 This work I want to highlight, even though
23 I know the Committee is not overly thrilled with
24 Halden's work in the past, one of the areas that they
25 specialize in is the Bayesian Belief Network 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 combining qualitative and quantitative data, where
2 they've also done extensive work in formal methods.
3 That's one of the areas that they are probably going
4 to present in the May meeting which I will be
5 attending, and we will assess whether or not we want
6 to include that in this continuing work with them.
7 They're one of the leaders in the European nuclear
8 community for formal methods.

9 MR. GUARRO: Steve, with respect to the
10 database review, I would just suggest that the horizon
11 is kept wide so that you look at some of these
12 egregious type of examples of failures that have been
13 pretty catastrophic, and those are not very many. And
14 you look at them from the point of view of kind of a
15 case study to see what needs to be learned from them.
16 It's not a matter of how many happened and how many
17 trials.

18 MR. ARNDT: Right.

19 MR. GUARRO: It's just a matter of what
20 really happened.

21 MR. ARNDT: Right. And I didn't mention
22 it when I was talking about, but that's one of the
23 specific goals of the international nuclear database,
24 is not so much to come up with reliability data, but
25 it's to understand what the failures are telling us,

NEAL R. GROSS

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

1 both from a specific individual failure analysis, and
2 a trending kind of statement, the COMPSIS
3 International Database Program is looking at that for
4 smaller events where we actually had nuclear-specific
5 data.

6 MR. ROSEN: What I would have wished you
7 had said in response to Sergio's comment was that you
8 would look at the known failures, the most egregious
9 examples.

10 MR. ARNDT: Yes.

11 MR. ROSEN: And that you would derive from
12 them the generic implications to the nuclear program
13 from that.

14 MR. ARNDT: Yes. Absolutely. And that's
15 one of the things that you'll see in the BNL report.
16 But we need to do that more.

17 We plan on having a new project that's
18 going to look at specifically looking at what kind of
19 models work best in current generation PRAs. The
20 project is specifically looking at the risk importance
21 issues, what is most important in putting a system
22 into a model, and what are the practicality issues
23 associated with trying to put a Markov model, a
24 dynamic fault treaty, or the various issues. This
25 project is specifically designed for that analysis.

NEAL R. GROSS

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

1 MR. APOSTOLAKIS: Now we just said a few
2 minutes ago that the completeness of the requirements
3 is extremely important, so it seems to me it should be
4 -- the next you talk to us, I would suggest that there
5 is a separate bullet for that.

6 MR. ARNDT: Okay.

7 MR. APOSTOLAKIS: It's really so
8 important. And if you look at all these events that
9 have occurred, you will see that there was a problem
10 with the requirements.

11 MR. ROSEN: And I think ultimately you go
12 to what are the regulatory requirements for developing
13 digital software. And some place in those regulatory
14 requirements there should be an embodiment of the
15 principle that the user is embedded in the process
16 from a very early point and continues throughout.

17 MR. ARNDT: There is a specific
18 requirement, specific regulatory review guidance on
19 requirements. I just don't remember the exact
20 phraseology and level of detail.

21 MR. ROSEN: For that specific requirement,
22 for the user input from very early-on and continuing
23 throughout the life-cycle of the development?

24 MR. ARNDT: The requirements, and who
25 needs to specify them, and how they need to be

1 followed and things like that. I don't remember the
2 level of detail.

3 MR. ROSEN: Well, I think I just told you
4 what I would want to see. It's the result of
5 listening to this discussion, but also a career, a
6 lifetime in doing, not software but doing design work,
7 knowing how systems work, and knowing how to get to a
8 good answer.

9 MR. ARNDT: Another effort that's going to
10 be ongoing is the review of the draft EPRI report,
11 which proposes a risk-informed approach to a
12 particular software issue; that is the defense-in-
13 depth requirement, diversity requirements. So that is
14 going to be one of our efforts in the near future.

15 And as I mentioned, we don't know this to
16 be the case, but it could be the first step in the
17 industry's push to use risk-informed ideas in digital
18 system submittals.

19 There is a little bit of work that's going
20 to be ongoing in the reactor program, particularly
21 trying to develop information to support the risk-
22 informed regulatory approaches that Mary is working
23 on, and also to try and understand better the kinds of
24 issues in software that can have potential issues in
25 pre-application and application. Some of these you

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 raised when you looked at the ACR-700 software.

2 You asked Carol when her next program
3 should be complete. That's going to be in early FY06
4 for some of the work that we talked about, that's been
5 published already. We're going to have an additional
6 report on the small-scale validation. It's going to
7 be published this year so that that work could be
8 folded into any regulatory guidance document we
9 develop.

10 As I mentioned, Barry's new program which
11 hopefully will be one of the generic platforms should
12 be completed in late '05. The first products of the
13 new research program should be ready in '05. The
14 database work is ongoing, and the guidance review
15 depending upon what response we get from industry and
16 various other things should be completed in '05.

17 MR. APOSTOLAKIS: Well, you said you are
18 developing a plan, a research plan.

19 MR. ARNDT: Yes. We're updating our
20 research plan basically.

21 MR. APOSTOLAKIS: So that plan will have
22 new tasks or projects and so on, because from what
23 you're presenting, you're pretty busy already well
24 into 2006.

25 MR. ARNDT: In this area, yes. It will

1 not just be this program, but it will be all the rest
2 of the I&C programs, the emerging technology and other
3 programs, as well.

4 CHAIRMAN SIEBER: There's some pretty
5 basic stuff still in the basic program.

6 MR. ARNDT: Yes. And one of the areas is
7 systems aspects, things like operating systems and
8 design reviews and things like that, which we've
9 touched on as it affects these kinds of things from
10 this presentation.

11 MR. APOSTOLAKIS: We heard years ago when
12 we were reviewing the SRP that the Canadians when they
13 licensed - which one was it, Pickering? No, another
14 one. Darlington. They used a mixture of formal
15 methods and testing, and all that stuff. Are you
16 familiar with all that?

17 MR. ARNDT: Yes. We've looked at that, as
18 well as several other countries' reviews, like the
19 review that was done for Sizewell, and for Choose-
20 B, and some of the ABWR work and things like that. And
21 that's actually part of a product that's going to be
22 published here in a month or two on Lessons Learned
23 from evolutionary reactors.

24 MR. APOSTOLAKIS: One interesting thing
25 that is related to what we were saying earlier from

NEAL R. GROSS

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

1 the Canadians, is that they didn't really use formal
2 methods, but they borrowed what they thought was
3 appropriate. And one of the things they borrowed was
4 some tables where the requirements are specified in a
5 formal language, and maybe that helps. What Sergio
6 said earlier, you know, it enhances their ability to
7 catch problems with the requirements if you do that.
8 Because, as you know, if you use a formal language,
9 then there is no two ways about it. I mean, either
10 you're precise or you're not.

11 MR. ARNDT: It helps, like a lot of other
12 things.

13 MR. APOSTOLAKIS: Yes.

14 MR. ARNDT: And least once you've done
15 your system work, you're software requirements are
16 very tight. We still don't have as much of the system
17 issues solved, but it doesn't certainly more formalize
18 the software requirements.

19 CHAIRMAN SIEBER: Okay.

20 MR. ARNDT: And this is just a quick some
21 of the things we're doing to keep up with current
22 work. We've talked about this, a major meeting this
23 year - this is the joint IA, EA, NEA Maryland project
24 to look at validation and verification. There's going
25 to be a meeting in Istanbul. COMPSIS where work

NEAL R. GROSS

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

1 through our contractors to stay in touch with other
2 industries and things like that, and of course
3 standard professional things that we try and do.

4 CHAIRMAN SIEBER: Very good.

5 MR. ARNDT: And again, we're continuing
6 our work. We're continuing future work to look at
7 different aspects. The goal is always to provide
8 tools and guidance to NRR. Okay. Mr. Chairman.

9 CHAIRMAN SIEBER: Yes.

10 MR. APOSTOLAKIS: You stood up and we're
11 finished.

12 CHAIRMAN SIEBER: We have one of our
13 guests that has to leave. I thought it would be nice
14 to say goodbye.

15 MR. APOSTOLAKIS: I was wondering where
16 there was a correlation.

17 CHAIRMAN SIEBER: And our Designated
18 Federal Official stood up too. I'm not sure what that
19 means.

20 MR. SYKES: You're still in control.

21 CHAIRMAN SIEBER: Well, I think that's
22 what I want to do. What we will do with the
23 information that we received today, which is very good
24 presentations all down the line is, I will make a
25 report to the Full Committee in April. And what I

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 would like to do now is just go around the room and
2 take a little bit of time for you to give me your
3 opinion of what you've heard today, and suggestions as
4 to what should be in my April report. And, George,
5 why don't you start.

6 MR. APOSTOLAKIS: Well, I'm still not sure
7 that we're addressing the real issues that are
8 important to us, granulating nuclear power. Perhaps
9 if we had seen some actual failures that involved
10 software and then seen some methods, how these
11 methods, for example, that were presented were
12 consistent or would have found these things in
13 advance, I would feel much better.

14 CHAIRMAN SIEBER: Yes.

15 MR. APOSTOLAKIS: At this time, I'm still
16 not sure we're on the right path, so I am willing to
17 be convinced, but I'm not sure that we're really
18 focusing on what's really important to this agency.

19 CHAIRMAN SIEBER: Okay.

20 MR. APOSTOLAKIS: Okay.

21 CHAIRMAN SIEBER: Just as a comment to
22 that, I've asked these same questions on other
23 occasions, and there is no audit data in the U.S.
24 Nuclear Industry on digital I&C because there aren't
25 very many systems. The systems that are there are

NEAL R. GROSS

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

1 really sub-systems, and relatively rudimentary
2 systems. There is some European data, but the major
3 data really comes from other industries. For example,
4 the steel mill accident where they dumped a ladle of
5 steel in the middle of the floor. That was a digital
6 I&C problem, as I understand it, and that information
7 wasn't presented. It is available, but right now
8 other than aerospace and commercial aviation, and some
9 process industries, like chemicals and petroleum,
10 there isn't a lot of data out there.

11 I'm not sure where you go though when you
12 assess what it is this agency should do to assure the
13 integrity of the software systems, lacking that kind
14 of data. And you may want to speak to that.

15 MR. ARNDT: Well, there are several
16 issues, and most of them were brought up during the
17 course of the meeting. One is that that whole issue
18 is what do we need to do to assess the safety and to
19 ensure the safety of the digital systems as they're
20 implemented. One thing that we could do, as Dr. Rosen
21 mentioned, is to set a particular high threshold
22 requirement that if you're going to do it, you need to
23 do it this way.

24 CHAIRMAN SIEBER: Yes, I sort of agree
25 with that.

1 MR. ARNDT: And that's fine. Another
2 thing we can do is to update our review methods and
3 technology to try and better handle, so when presented
4 with analysis we can make a more informed decision as
5 to whether or not it's acceptable or not, going at the
6 same issue from a slightly different perspective.

7 In trying to develop tools and methods for
8 our colleagues at NRR to do their current assessments,
9 that's what we're currently trying to do. The issue
10 I think that Professor Apostolakis is getting to is,
11 are the things that we are doing either in the reviews
12 that NRR is doing, or the research that we are doing
13 really attacking issues that are going to make a
14 significant difference in the likelihood of a problem.
15 And that's a tough thing to get at.

16 CHAIRMAN SIEBER: Yes.

17 MR. ARNDT: And I think we are doing that.
18 We may not have articulated it as well as we would
19 like. There are certainly things that we can do more
20 in that area.

21 MR. APOSTOLAKIS: Going back to the issue
22 of data - you know, there have been some really
23 spectacular failures, like the Ariane failure and so
24 on. And there are some minor, like the one I
25 mentioned with the fighter plane and so on. It would

1 be very enlightening, I think, to look at those and
2 maybe categorize them in some way, maybe say that this
3 thing will never happen in a nuclear plant, but this
4 other thing might. And then get a basis from which we
5 will start focusing on what's important, a combination
6 of the failure experience and theory. We seem to be
7 jumping into things like, you know, the density of
8 faults. I mean, why is that important? On what basis
9 is that important, because somebody used it?

10 This is where I get lost. Why are we
11 doing certain things, and what's the basis for those,
12 and how relevant are they to nuclear reactor
13 regulation?

14 MR. ARNDT: I think it's important that
15 you bring that up because it provides us a background
16 on future interactions.

17 MR. APOSTOLAKIS: Absolutely.

18 MR. ARNDT: Things that we need to try and
19 do to inform the committee better.

20 MR. APOSTOLAKIS: I want you to succeed,
21 Steve. I really want you to succeed. Don't think I
22 -- but I have to give you my honest opinion now.

23 MR. ARNDT: That's why we're here.

24 MR. APOSTOLAKIS: I'm not sure we're
25 fitting the right places.

NEAL R. GROSS

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

1 MR. ARNDT: That's why we're here.

2 CHAIRMAN SIEBER: Jim.

3 MR. WHITE: Thank you. I'll be brief.
4 Steve, you opened the meeting saying you'd like to be
5 prepared to answer the questions that you expect to be
6 asked about how NRC will do risk assessment. It would
7 help me if you could give us a little scorecard, what
8 are the questions you expect to be addressed, and then
9 lay out your programs to show how you are, and the
10 progress you would expect. Just kind of put it all
11 into context for us.

12 One thing that we learned on the National
13 Academy Study is we've got a lot to learn from the
14 software engineering practitioner community, and I'm
15 glad to see that you are really trying to get engaged
16 with those folks.

17 The other thing that we - and that's a
18 really big positive. The other thing we did learn,
19 however, and I know this is controversial, but it's
20 the design of safety assessment rigor in those
21 industries seemed to pale in comparison to what we're
22 expected to do in the nuclear industry. And it seems
23 to me that you're going to have to forge new -- you're
24 going to have to blaze new territory to make that
25 happen, and so good luck on all 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 There is the issue of data, and it looks
2 like you're trying to go out and get the data. And
3 that's going to be a continuing challenge.

4 With respect to the software community, I
5 think you saw today how hard it is for some of us to
6 understand what they're trying to tell us. We know
7 that they're trying to tell us something that's really
8 important, and we're trying to grasp what it is. And
9 it's not always so obvious to us.

10 I see that you're beginning to, and maybe
11 you always have, pay attention to IEC standards, which
12 is one thing that we'd recommended. And I'm just
13 about done.

14 I think it's really excellent that Barry
15 Johnson with your funding is looking at large systems
16 with very high reliability, because trying to assess
17 the probability of failure of a very high reliability
18 system is difficult, as you know better than I do, so
19 I'm glad that you're doing that. And it seems to me
20 that one of the big questions is going to be
21 uncertainty, and how do we handle uncertainty. And I
22 think we have some models from our PRA on the thermal
23 hydraulic-type accidents, how we might do that. That
24 concludes my comments. Thank you.

25 CHAIRMAN SIEBER: Thank you. I presume

NEAL R. GROSS

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

1 you'll provide us with something in writing?

2 MR. WHITE: Yes.

3 CHAIRMAN SIEBER: Thank you.

4 MR. WHITE: When do you need that?

5 CHAIRMAN SIEBER: Actually, it would have
6 been handy yesterday. Tom.

7 DR. KRESS: I was glad to hear Jim mention
8 the word uncertainty, because as everybody knows, it's
9 my hobbyhorse, so I want to agree with that comment.
10 I also want to say, I thought today's presentations
11 were superb. It was much better -- a lot better than
12 we're used to, and wanting to thank the speakers and
13 everybody.

14 I think this research has some very bold
15 proactive elements that are badly needed, and I'm
16 really glad to see something like this being done.
17 And I applaud the effort. It looks like the program
18 is well-conceived, and the various parts of it
19 actually fit together nicely or complimentary, and
20 each one of them appear to me to be needed for this.

21 That said, I have following other
22 thoughts. Like George, I think more is needed to
23 justify the use of the Markov model. Now I'm not as
24 skeptical that it can't be used, as George appears to
25 be, but I think -- I haven't seen the real

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 justification for it yet. It wasn't presented to us
2 today, and I think something needs -- you're going to
3 get asked this question over and over, and I think
4 something needs to be done about that.

5 I think you need some early thinking on
6 what your acceptance criteria are going to be for when
7 you actually get ready to stick a PRA model of digital
8 systems in. When is it good enough, and what are the
9 acceptance criteria? And these need to be ready to
10 think about the uncertainty and the reliability
11 numbers you get, and the defense-in-depth issues. And
12 0174 may have some in there, but I'm not sure.

13 I'm glad to hear that the fault injection
14 method can use injection of multiple faults
15 simultaneously. I hope to see more of that, because
16 I think that might be important.

17 I was also very glad to hear you are
18 seeking some international programs in this area, and
19 I really urge you to continue that. And you might
20 even work on trying to get the industry involved,
21 through EPRI or NEI.

22 I share George's thought that we might
23 want to think about how to approach the business of
24 the initial requirements. On the PRA completeness
25 issue, you just have to think about it, and think

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 about it, and get enough people, experts to look at it
2 and see if you've covered everything. And maybe you
3 haven't, and maybe you have, and you're never going to
4 know until something happens that you didn't think
5 about. But perhaps if we give it some more thought,
6 it might be helpful.

7 In the University of Maryland expert
8 opinions, I still think you need to look at the
9 dispersion and factor that into your ranking some way.
10 And I think you need to think about how to update the
11 rankings as you go along, as you get new information.
12 So that's all I have.

13 CHAIRMAN SIEBER: Okay. Thanks. Steve.

14 MR. ROSEN: Well, I learned a lot today,
15 and I thought the presentations were very good. Of
16 course, it was easy for me to learn a lot because I
17 didn't know very much to start, but I thought the
18 presentations were very interesting, very useful.

19 With regard to the University of
20 Virginia's programs, the one on developing an
21 integrated digital system assessment method that the
22 staff can use is, think crucial, along the lines of
23 your comment, Steve, that if you're going to do it,
24 you need to do it this way. It's a very valuable
25 thing for the industry to have the staff's idea 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 front of them, how this process should be done. They
2 may do it another way, but they'll certainly check the
3 way they do it against your methods, because they
4 don't want to be surprised when they come in here.

5 With regard to the modeling, risk
6 modeling, I think it's very, very good idea to push
7 the research to figure out what the most effective
8 method is for including digital system modeling in
9 PRAs. It's always been a worry of mine, but I didn't
10 really face it directly in my career because there
11 wasn't that much digital stuff in the plant. We just
12 assumed the failure of the reactor protection system
13 as an initiating event. Its frequency was tiny, but
14 it was there, and then we tried to figure out what the
15 most effective method is. The consequences are very
16 large, the frequency was tiny, but it wasn't very
17 instructive to do that. We need something much
18 better. I'm glad to see that you're focusing on that.
19 We'll be very interested in the results of how one
20 does that.

21 I'm also glad to see that at Maryland, I
22 guess it is - maybe no, I'm not sure - maybe you can
23 help me with this, but that the first products of the
24 new research will be pilot models integrated into
25 current plant PRAs. Is that Maryland or Virginia?

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. ARNDT: That's going to be the new
2 project we're starting this year.

3 MR. ROSEN: That's the new project. At
4 Maryland or at Virginia? Don't know yet.

5 MR. ARNDT: We haven't decided yet.

6 MR. ROSEN: Okay. That's why it's so
7 unclear. But whoever does it, how one does it will be
8 of great interest to me, and I'll be thinking about
9 it, having been a practitioner or manager of
10 practitioners at one point in my career. Could we
11 really do it, could we back-fit it to an existing
12 plant? These plants now, the ones I'm familiar with
13 are 20 years old, let's say, sure to be relicensed,
14 sure to have digital systems incorporated in before
15 the end of their operating terms. And so the people
16 who I know will be faced with the problem of
17 integrating into the PRA model, these new systems, and
18 doing it in a way that preserves the integrity of the
19 existing model and results. And so I'll be very
20 interested in how that's done.

21 So those are my comments. I thought, as
22 I said, I learned a lot and I'm hopeful for the
23 future.

24 CHAIRMAN SIEBER: Okay. Thank you. I
25 agree that the presentations today were excellent, and

1 I thank the speakers for coming in and making those
2 presentations, and informing us as to what they're
3 doing.

4 I'd sort of like to step back just for a
5 second and look at the overall scheme of what it is
6 we're trying to do. Really what you're preparing to
7 do is to write SERs that will approve the use of
8 digital I&C systems in nuclear power plants. And if
9 you're going to do that on a risk-basis, which I think
10 is the way to do it, then you have to decide what your
11 goal, your safety goal is, and what methods either the
12 staff will use, or the applicant will use in order to
13 establish whether or not they meet that goal. And I
14 think that that has to be pretty prescriptive in order
15 to do that, and I would see that as part of regulatory
16 guidance of one sort or another. And that's a project
17 that you ought to be actively engaged in finding that.

18 Now what kind of systems are proposed is
19 irrelevant, except to the extent that different system
20 architectures have an influence on how risky the
21 system really is. And so you won't be dictating to
22 vendors what the system functional requirements will
23 be, or what is architecture, either software or
24 hardware design should be. On the other hand, you're
25 setting up a performance standard that they ought 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 meet. And if you do it in a consistent way, I think
2 it's fair across the board, and there is a real basis
3 then to write an SER that says basically there's no
4 substantial risk to the public when these systems are
5 employed.

6 I think that I would put some additional
7 direction into developing that framework. How is it
8 that we're going to approve the systems? And you've
9 already done it with three systems, and I'm not
10 exactly sure how you do that.

11 DR. KRESS: Engineering judgment.

12 CHAIRMAN SIEBER: Well, it goes beyond
13 that. You know, I bought a computer -- I buy a
14 computer about every 18 months for some reason or
15 other, because they turn obsolete like you wouldn't
16 believe. They're either too small or what have you,
17 and so let's say combustion engineering comes out with
18 a digital I&C system. That becomes obsolete pretty
19 fast. And if you're still using 8086s and 486s, and
20 Windows 3.1, I think there's a problem there.

21 You know, it's like your thermal
22 hydraulics programs, they're relegated to operate on
23 some ancient main frame that it becomes difficult to
24 continue to operate some of these design and
25 analytical codes because you've got to maintain some

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 old, decrepit, antique of a machine for which it was
2 approved. And so there has to be a way to be flexible
3 enough to allow the manufacturers to be able to change
4 processors and some of the architecture inside the
5 machine. Every time you change processors, you're
6 changing the instruction set, because there is an
7 instruction set that goes with a Pentium IV or what
8 have you. And it makes a difference as to what chip
9 you have as to how the operating system performs, so
10 it seems to me that there's an area that needs some
11 attention too. How do you accommodate people's desire
12 to upgrade systems and still establish the fact that
13 that SER applies, or do you have to start from scratch
14 every time somebody wants to change a chip.

15 DR. KRESS: 5059.

16 CHAIRMAN SIEBER: Right. 1.174.

17 MR. ROSEN: Well, that's an
18 extraordinarily good point. We've got two factors
19 operating, and they're going in opposite directions.
20 The life-cycle of computers is going down, and the
21 life-cycle of plants is going up.

22 MR. APOSTOLAKIS: Somewhere they meet.

23 MR. ROSEN: In third space maybe.

24 CHAIRMAN SIEBER: When they're going like
25 this I don't think they meet. That's one of the

NEAL R. GROSS

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

1 problems. But in any event, those are some of the
2 thoughts that I had when I was preparing for this, and
3 hoping would be answered. And I'm still hoping.
4 Okay. But I think that that's -- if I were doing it,
5 that's where I would put a little more emphasis, is to
6 figure out what I'm going to do with the applications
7 when they come in.

8 And so with that, anybody else have any
9 comments or any comments from our guests? Well if
10 not, then I would take this time to adjourn the
11 meeting. Thank you all very much.

12 (Whereupon, the proceedings in the above-
13 entitled matter went off the record at 3:52 p.m.)
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

Plant Operations Subcommittee

Docket Number: n/a

Location: Rockville, MD

were held as herein appears, and that this is the original transcript thereof for the file of the United States Nuclear Regulatory Commission taken by me and, thereafter reduced to typewriting by me or under the direction of the court reporting company, and that the transcript is a true and accurate record of the foregoing proceedings.



Eric Hendrixson
Official Reporter
Neal R. Gross & Co., Inc.

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

(202) 234-4433

www.nealrgross.com



United States Nuclear Regulatory Commission

**ADVISORY COMMITTEE ON REACTOR
SAFEGUARDS PLANT OPERATIONS
SUBCOMMITTEE MEETING ON
DIGITAL INSTRUMENTATION AND CONTROL**

March 26, 2004

Division of Engineering Technology
Office of Nuclear Regulatory Research



United States Nuclear Regulatory Commission

SCHEDULE

| | |
|--|-------------------------|
| Opening Remarks | 8:30-8:35AM |
| Overview of Digital I&C Research Program, State-of-the-Art in Digital System Reliability, Modeling and PRA Modeling Program | 8:35-10:00AM |
| Break | 10:00-10:15AM |
| Overview of Digital I&C Research Program, State-of-the-Art in Digital System Reliability, Modeling and PRA Modeling Program (Continued) | 10:15-10:45AM |
| Digital Systems Modeling Using Fault Injection Methods | 10:45AM-12:15 PM |
| Lunch | 12:15-1:15 PM |
| Software Reliability Modeling | 1:15-2:30 PM |
| Staff Plans for Digital Reliability Models | 2:30-2:50 PM |
| General Discussion and Adjourn | 2:50-3:00 PM |



United States Nuclear Regulatory Commission

Overview of Digital I&C Research Program, State-of-the-Art in Digital System Reliability Modeling and PRA Modeling Program

Steven A. Arndt

(saa@nrc.gov, 301-415-6502)

Division of Engineering Technology
Office of Nuclear Regulatory Research

March 26, 2004



United States Nuclear Regulatory Commission

OVERVIEW

- Conclusions
- Review of digital I&C research program
- Drivers and boundary conditions
- Digital system reliability modeling
- Current methods
- Research projects
- Summary



United States Nuclear Regulatory Commission

CONCLUSIONS

- NRC research program will answer important questions associated with digital system risk analysis
- Research includes model development, data collection and analyses, and guidance development
- Several of the tool development programs are at the demonstration phase
- NRC is working with other researchers to keep abreast of the current state-of-the-art



United States Nuclear Regulatory Commission

CONCLUSIONS (CONT)

- Current analysis methods are sufficiently mature such that guidance documents can be developed
- Current state of the practice analysis methods have significant weaknesses
- Future work is needed to develop and test an integrated PRA model to support audit calculations
- Research is needed to develop additional data and better use the data that is available
- Additional coordination within the international community is needed and planned



United States Nuclear Regulatory Commission

DIGITAL I&C RESEARCH PROGRAM PLAN

- SECY-01-0155, NRC digital instrumentation and control research plan, published August 2001
- Addressed the need highlighted in the NAS review for a more systematic approach to developing new information and regulatory guidance
- Endorsed by the ACRS and commission
- Includes research in five major areas
- New research plan under development



United States Nuclear Regulatory Commission

I&C RESEARCH PROGRAM GOALS

- I&C research program goal
 - “Continually improving the staff’s analytical capabilities, and fundamental knowledge of digital I&C technology as demonstrated by the development of analytical tools, technical reports, regulatory guidance, papers and articles, and interaction with licensees, vendors, industry research organizations, and the public.”



United States Nuclear Regulatory Commission

I&C RESEARCH PROGRAM GOALS (CONT.)

- Examples of I&C research program products
 - New analytical methods, such as the UVa method
 - Updated regulatory guidance, such as RG 1.168 on “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
 - Technical support of other NRC programs
 - MOX and centrifuge for NMSS
 - Flowmeter work for NRR
 - Software quality work for RES and OIG



United States Nuclear Regulatory Commission

DIGITAL I&C RESEARCH PROGRAM

- System aspects of digital technology
 - Environmental stressors
 - Digital requirement specifications
 - Diagnostics and fault-tolerance
 - Operating systems



United States Nuclear Regulatory Commission

DIGITAL I&C RESEARCH PROGRAM (CONT)

- Software quality assurance
 - Objective software engineering criteria
 - Criteria for software testing



United States Nuclear Regulatory Commission

DIGITAL I&C RESEARCH PROGRAM (CONT)

- Emerging I&C technologies and applications
 - Predictive maintenance and on-line monitoring
 - Advanced instrumentation
 - Smart transmitters
 - Wireless communication
 - Computer security
 - Reviewing technologies and infrastructure including developing and maintaining interactions and interfaces, and standards work



United States Nuclear Regulatory Commission

DIGITAL I&C RESEARCH PROGRAM (CONT)

- Advanced reactor I&C infrastructure
 - Lessons learned from evolutionary plants
 - Technical and regulatory issues encountered in new reactor construction around the world
 - Development of risk models for advanced plants
 - Other projects in research program but not yet funded include:
 - Review of issues associated with multi-module plants
 - Autonomous control
 - New instruments, and advanced diagnostics



United States Nuclear Regulatory Commission

DIGITAL I&C RESEARCH PROGRAM (CONT)

- Risk assessment of digital I&C systems
 - Digital I&C failure data research
 - Digital failure assessment methods and system models
 - Digital reliability assessment methods and integration in PRA's
 - Digital system risk guidance



United States Nuclear Regulatory Commission

RESOURCES

- FY 2004 I&C section budget is 9 FTE and \$3.8M
 - ~1 FTE and \$1.0 M devoted to digital system reliability and risk modeling
 - The remaining resources are devoted to the other parts of the digital I&C research program, system aspects, software quality assurance, emerging I&C technologies and advanced reactor research



United States Nuclear Regulatory Commission

PRA PROGRAM EXTERNAL DRIVERS

- NAS recommendations
- DOE I&C and HMI Working Group recommendations, May 2002
- Halden Workshop on Digital System Reliability, December 2002
- DRAFT EPRI D-i-D&D Topical Report, January 2004



United States Nuclear Regulatory Commission

DIGITAL SYSTEM PRA RESEARCH

- NAS “Digital Instrumentation and Control Systems in Nuclear Power Plant” Report Recommendations
- NRC PRA Policy



United States Nuclear Regulatory Commission

NAS REPORT RECOMMENDATIONS

- Include the relative influence of software failures on system reliability in PRAs
- Develop methods for estimating digital system failure probabilities, including COTS. Include acceptance criteria, guidelines, limitations, rationale and justifications
- Develop advanced techniques for analyzing digital systems to increase confidence and reduce uncertainty in quantitative assessments
- NRC and industry should evaluate their capabilities and develop a sufficient level of expertise to understand the requirements of digital implementations of system functions and the limitations of quantitative assessments



United States Nuclear Regulatory Commission

NRC PRA Policy

- Increase the use of PRA in all regulatory matters to the extent supported by state-of-the-art methods and data in a manner that complements a deterministic approach and supports the traditional defense-in-depth philosophy



United States Nuclear Regulatory Commission

WHAT IS NEEDED IN DIGITAL SYSTEM PRAs

- Develop methods for reviewing digital system reliability models
 - Understanding the state of the data
 - Digital system failure mechanisms
 - Strengths and limitations of digital system models
 - Incorporating digital system models into PRAs
 - Acceptability criteria



United States Nuclear Regulatory Commission

RESEARCH PRODUCTS

- Improve the review process by providing additional information, guidance and tools
- To accomplish this RES needs to:
 - Develop a detailed understanding of the technology
 - Provide guidance that will improve the review process by making it more
 - Quantitative
 - Realistic
 - Repeatable
 - Develop tools that can be used to assist the reviews, inform reviews or be used to perform check calculations



United States Nuclear Regulatory Commission

RESEARCH PRODUCTS

- For the risk assessment projects this tool box will include:
 - NUREGs that will provide information on how digital systems fail and the strengths and limitations of digital system models
 - Guidance that will permit more quantitative reviews
 - Guidance on acceptability of risk informed digital submittals
 - Guidance on quantitative measures of software quality and reliability
 - Guidance on alternate methods for demonstrating system safety
 - Data and analysis to inform reviews and validate assumptions
 - Check tools to independently assess digital system submittals



United States Nuclear Regulatory Commission

RESEARCH PROJECTS

- UVa Integrated digital system modeling project
- UMd software metrics project
- BNL project on digital system risk
- Other database development
 - COMPSIS
 - NRC In-house effort
- Other efforts
 - Halden
 - CSNI initiative



United States Nuclear Regulatory Commission

STRUCTURE OF CURRENT NRC RESEARCH

- UVa integrated digital system modeling project will provide:
 - An integrated digital system assessment method that can be used by the NRC staff to independently assess digital system safety
 - Information on digital system failure modes and reliability that will inform the review guidance



United States Nuclear Regulatory Commission

STRUCTURE OF CURRENT NRC RESEARCH (CONT)

- UMd software metrics project will provide:
 - An assessment method that can be used by the NRC staff to independently assess software quality and reliability
 - Quantitative information on the relative importance of software metrics will be used to inform the current review guidance
 - Input to guidance on quantitative software quality and reliability



United States Nuclear Regulatory Commission

STRUCTURE OF CURRENT NRC RESEARCH (CONT)

- BNL project on digital system risk will provide:
 - Draft interim review guidance for risk informed digital submittals
 - Review current methods and tools for modeling digital systems that will be used in guidance for risk informed digital submittals
 - Review of digital failure databases
 - Digital system PRA model



United States Nuclear Regulatory Commission

STRUCTURE OF CURRENT NRC RESEARCH (CONT)

- Other database development
 - Data and analysis to inform reviews and validate assumptions
- Halden
 - Analysis of operational data to support risk analysis of COTS systems
 - Risk assessment of human system interfaces
 - A tool to assist in combining qualitative and quantitative information in reviews



United States Nuclear Regulatory Commission

DIGITAL SYSTEM RELIABILITY MODELING

- Modeling issues
 - Models should include important failure modes
 - Level of detail of the models
 - Independence of hardware and software
 - Software diversity
 - Number of possible states and the ability to test
- Modeling requirements
 - Ability to predict
 - Supported by or at least consistent with data



United States Nuclear Regulatory Commission

DIGITAL SYSTEM RELIABILITY MODELING (CONT)

- Various analysis methods have been proposed
 - Fault trees
 - Markov analysis
 - Dynamic flow graph methodology
 - Petri nets
- Setting acceptance criteria for both the modeling fidelity and the system reliability will be difficult



United States Nuclear Regulatory Commission

CURRENT METHODS

- In the nuclear industry, use of these methods is limited
- Most methods in trial use today focus on independent software modeling using software fault trees or other similar methods
- Some methods use “bounding” methods to assume digital system reliability
- Most methods in current use assume that the software can be analyzed separate from its hardware context
- The NRC will need to be able to review what is submitted



United States Nuclear Regulatory Commission

OBJECTIVES OF THE BNL PROJECT ON DIGITAL SYSTEM RISKS

- Development of guidance for reviewing PRA-based submittals for digital systems
- Investigate strengths and weaknesses of current digital systems analysis methods
- Generate suggestions for improving the integration of the methods with PRA
- Review of digital failure databases



United States Nuclear Regulatory Commission

BNL PRODUCTS

- Review current methods and tools for modeling digital systems
- List of issues associated with probabilistic failure modeling of digital systems
- Draft interim review guidance on PRA of digital systems
- FMEA of one of the generically approved digital platforms
- Review of digital failure databases



United States Nuclear Regulatory Commission

DRAFT INTERIM REVIEW GUIDANCE ON PRA OF DIGITAL SYSTEMS

- Prepared in anticipation of up-coming industry submittals (not yet received)
 - Identifies information needed for review of PRA models of digital systems
 - Makes use of the information generated by the deterministic evaluation



United States Nuclear Regulatory Commission

DRAFT INTERIM REVIEW GUIDANCE ON PRA OF DIGITAL SYSTEMS (CONT)

- Guidance
 - Refers to qualitative assessment of digital upgrade impacts derived from deterministic analyses
 - FMEA
 - Hazard analysis
 - Abnormal conditions and events (ACEs)
 - New initiating events
 - Notes need for modeling of dependencies - communication links, voting, synchronization
 - Refers to quantitative criterion based on RG 1.174



United States Nuclear Regulatory Commission

MODELING DIGITAL SYSTEMS ISSUES

- Software failures
 - Probabilistic modeling
 - Methods exist for quantifying digital safety system reliability, however, there is no common agreement among experts as to which methods are best or appropriate
 - Common cause failures



United States Nuclear Regulatory Commission

MODELING DIGITAL SYSTEMS ISSUES (CONT)

- Hardware failures
 - What is the level at which component failures should be modeled? What are the failure modes?
 - Does existing failure data adequately capture the unique features of digital systems? What about CCF?
- Software-hardware interactions
- Integration of digital systems models within existing PRAs



United States Nuclear Regulatory Commission

REVIEW OF METHODS AND TOOLS FOR MODELING DIGITAL SYSTEMS

- AP600 PRA - Fault Tree Analysis
- Dynamic Flow Methodology
- GO Methodology
- INEL RPS studies - Fault Tree Analysis of Analog Designs
- Petri Net Method - behavior mode, conversion to Markov
- Fault Injection Method - Markov Model



United States Nuclear Regulatory Commission

REVIEW OF METHODS AND TOOLS FOR MODELING DIGITAL SYSTEMS (CONT)

- Study of generically approved digital platform reliability/availability - markov Model and FMEA
- International Electrotechnical Commission (IEC) standard 61508
- Bayesian belief network
- EPRI report on applying risk-informed method to defense-in-depth and diversity evaluation



United States Nuclear Regulatory Commission

FMEA

- Conducted analysis of a hypothetical RPS based on a generically approved digital platform
- A top down, step-by-step approach focusing on increasing levels of detail
- Identified potential dependencies
- Generated list of questions and issues about design



United States Nuclear Regulatory Commission

INSIGHTS FROM FMEA

- In order to capture the benefits of redundancy and address potential adverse dependencies, a detailed probabilistic model must be developed and supported by deterministic evaluations
 - NRC has not endorsed any generic methods for addressing communication between redundant channels
- FMEA of detailed levels requires detailed design information and a simulation model of the design (which were not available)



United States Nuclear Regulatory Commission

DATABASE REVIEW

- Review of NRC publications
 - LER searches by NRC staff, NUREG/CR-6734 Vol 2
- Review of publicly available databases
 - 217F
 - PRISM
 - TELCORDIA
- PRISM and TELCORDIA databases
- Other sources of data that can be pursued
 - GIDEP – Reports of government agencies
 - Other industries and government agencies
 - Manufacturers may have additional data



United States Nuclear Regulatory Commission

DATABASE REVIEW (CONT)

- Software failures have caused serious accidents in other industries, Therac 25, 1985-1987, Airbus crash, 1994, etc.
- NRC LER searches 1994-1998 and NUREG/CR-6734 Vol 2
 - 8% of all LERs contain digital I&C failures
 - 9% of reactor trips can be attributed to digital I&C failures
 - Digital failures are approximately evenly divided among hardware, software, and human system interface related failures



United States Nuclear Regulatory Commission

DATA BASE REVIEW (CONT)

- Military Handbook 217F, Telcordia, PRISM
 - Military hand book uses parts count and part stress methods to estimate failure rate of series systems
 - Telcordia and databases of other countries are similar
 - PRISM (Reliability Analysis Center) included more recent failure data, provided guidance on use of process grading factors to account for design and manufacturing variability at system level, and provided guidance on use of CMM, Radio Technical Commission for Aeronautics (RTCA) safety level, and ISO 9000 certification to estimate software MTTF using a reliability growth model.



United States Nuclear Regulatory Commission

DATABASE REVIEW (CONT)

- Military Handbook 217F, Telcordia, PRISM
 - Failure rates were estimated by dividing the number of reported failures by the total operating time
 - Redundancy of safety channels must be modeled outside the databases
 - Fault tolerance features are implicit in the failure rate estimates, i.e., if a fault is detected and corrected automatically, no failure is reported
 - Original failure reports are not publicly available



United States Nuclear Regulatory Commission

FINDINGS OF BNL REVIEW

- Acceptable quantitative methods for assessing software failure probability are needed
- Markov-type modeling at the processor level appears to be capable of capturing digital design features
- Probabilistic modeling must be supported by detailed deterministic evaluations
- Data is needed to support detailed probabilistic modeling, failure rates, and diagnostic coverage



United States Nuclear Regulatory Commission

OTHER DATABASE DEVELOPMENT

- **COMPSIS**
 - International effort to develop a database of software failures in computer systems important to safety in nuclear plants, and the lessons learned from these failures
- **NRC In-House Effort**
 - Project to develop an NRC database of digital system failure information for use in validating reliability modeling assumptions



United States Nuclear Regulatory Commission

OTHER EFFORTS

- Halden Reactor Project program
 - As part of the CY 2003-2005 program plan, Halden determined that they would greatly expand their work in digital system safety
 - Part of their new work will be in digital system risk assessment
 - This new work includes analysis of operational data to support risk analysis of COTS systems, risk assessment of human system interfaces, and the use of BBNs to combine qualitative and quantitative information



United States Nuclear Regulatory Commission

OTHER EFFORTS (CONT)

- The CSNI has expressed interest in expanding its role in digital system safety research
- NRC staff will lead a briefing in June by various member countries
- This may result in an expert group assessing this technology and/or a new working group
- The NRC is also holding discussions about starting an international program in this area



United States Nuclear Regulatory Commission

SUMMARY

- Digital system reliability projects include model development, data collection and analysis, and guidance development
- Several tool development projects are in the demonstration phase
- US nuclear industry is moving forward in this area and the NRC research program is working to provide tools, methods, and guidance to support reviews in this area
- Current analysis methods are sufficiently mature such that guidance documents can be developed



United States Nuclear Regulatory Commission

SUMMARY (CONT)

- Current methods have significant strengths and weaknesses
- Future work is needed to develop and test an integrated PRA model to support audit calculations
- Research is needed to develop additional data and better use the data that is available
- Additional coordination within the international community is needed and planned

Digital Systems Modeling Using Fault Injection Methods

Presentation to ACRS at NRC

Barry W. Johnson, Ph.D.

(bwj@virginia.edu)

Director, UVA Center for Safety-Critical Systems

March 26, 2004



Presentation Outline

- **Conclusions**
- **Research Objectives**
- **Background**
- **Challenges**
- **System Modeling Methodology**
- **Safety Assessment Process**
- **Applications**
- **Summary**



Conclusions

- **A safety assessment process has been developed based on fault injection techniques and the consideration of the integrated hardware/software system**
- **The process has been applied to multiple practical commercial applications and approved by an independent safety assessors (e.g. TUV Rheinland)**
- **We are currently developing new fault models and new statistical models to support the approach**
- **We are currently developing new modeling and fault injection techniques based on COTS software tools (Simics)**
- **Digital feedwater control systems application successfully completed**



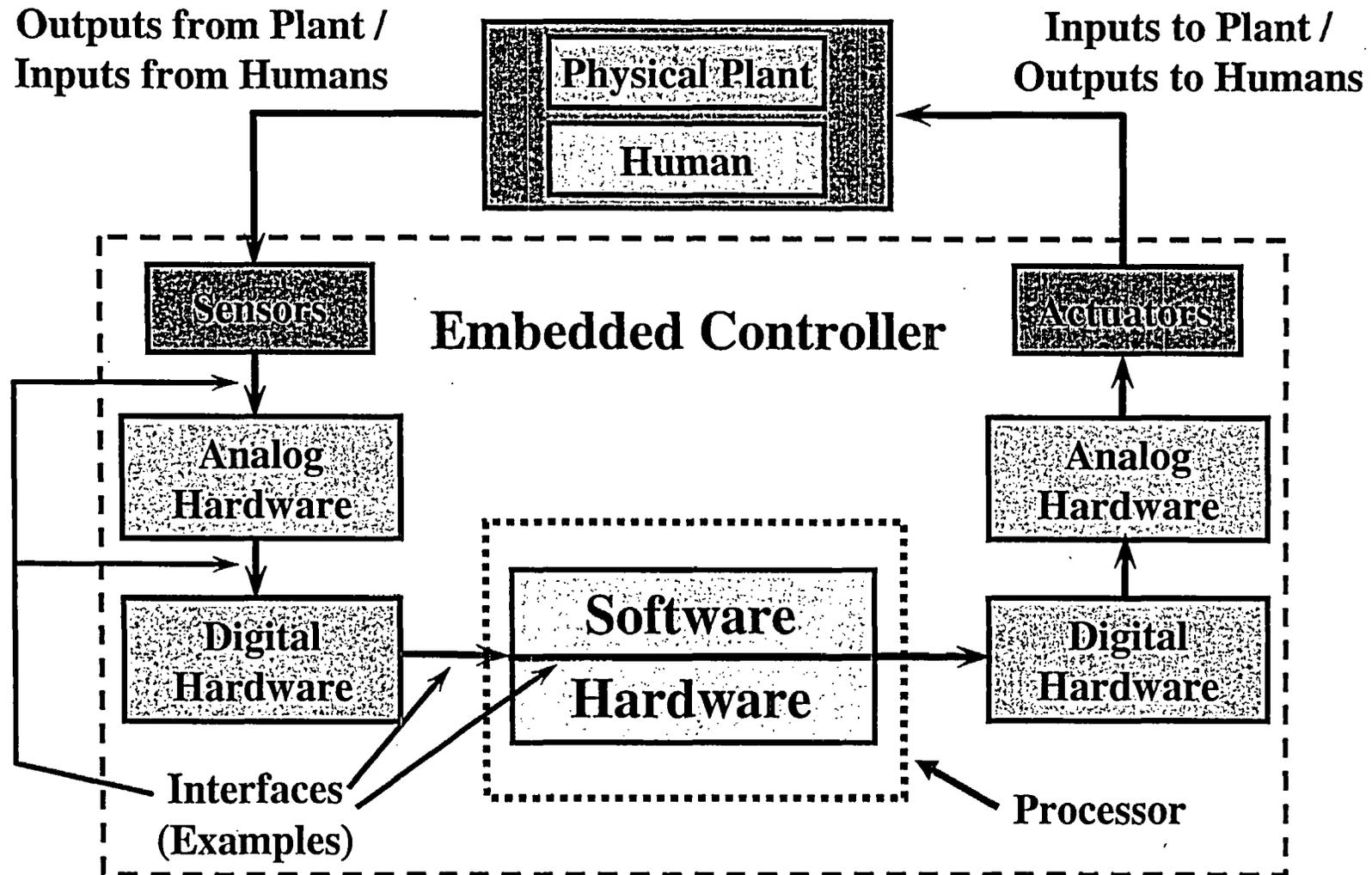
Research Objectives

- **Develop a safety assessment methodology for digital systems**
 - ◆ Consider the integrated hardware/software system
 - ◆ Include commercial-off-the-shelf (COTS) hardware and software
- **Develop modeling, simulation, and experimental techniques that support the assessment methodology**
 - ◆ Support the estimation of quantitative metrics
 - ◆ Support the evaluation of qualitative attributes
- **Develop tools that support the safety assessment methodology**
 - ◆ Use COTS software tools where feasible
 - ◆ Create new tools where needed
- **Demonstrate the resulting approach and tools on real examples**
 - ◆ Nuclear reactor systems
 - ◆ Railway systems
 - ◆ Aircraft flight control systems
 - ◆ Other examples



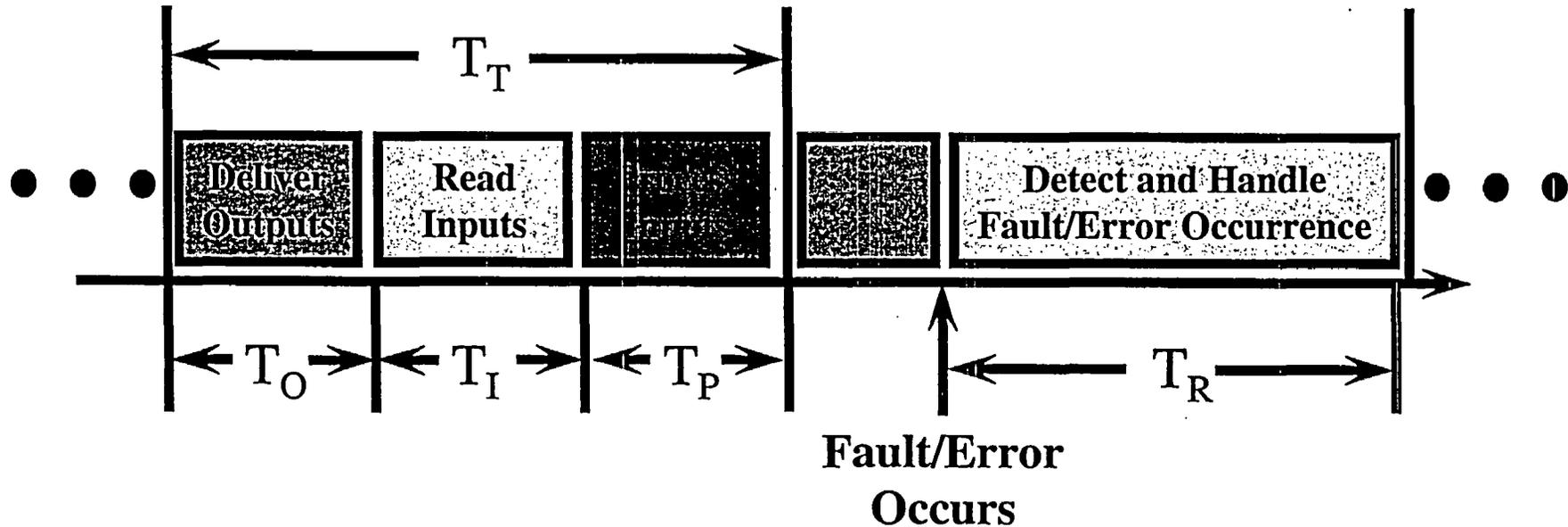
Background

Structure of Digital Systems



Background

Real-Time Requirements

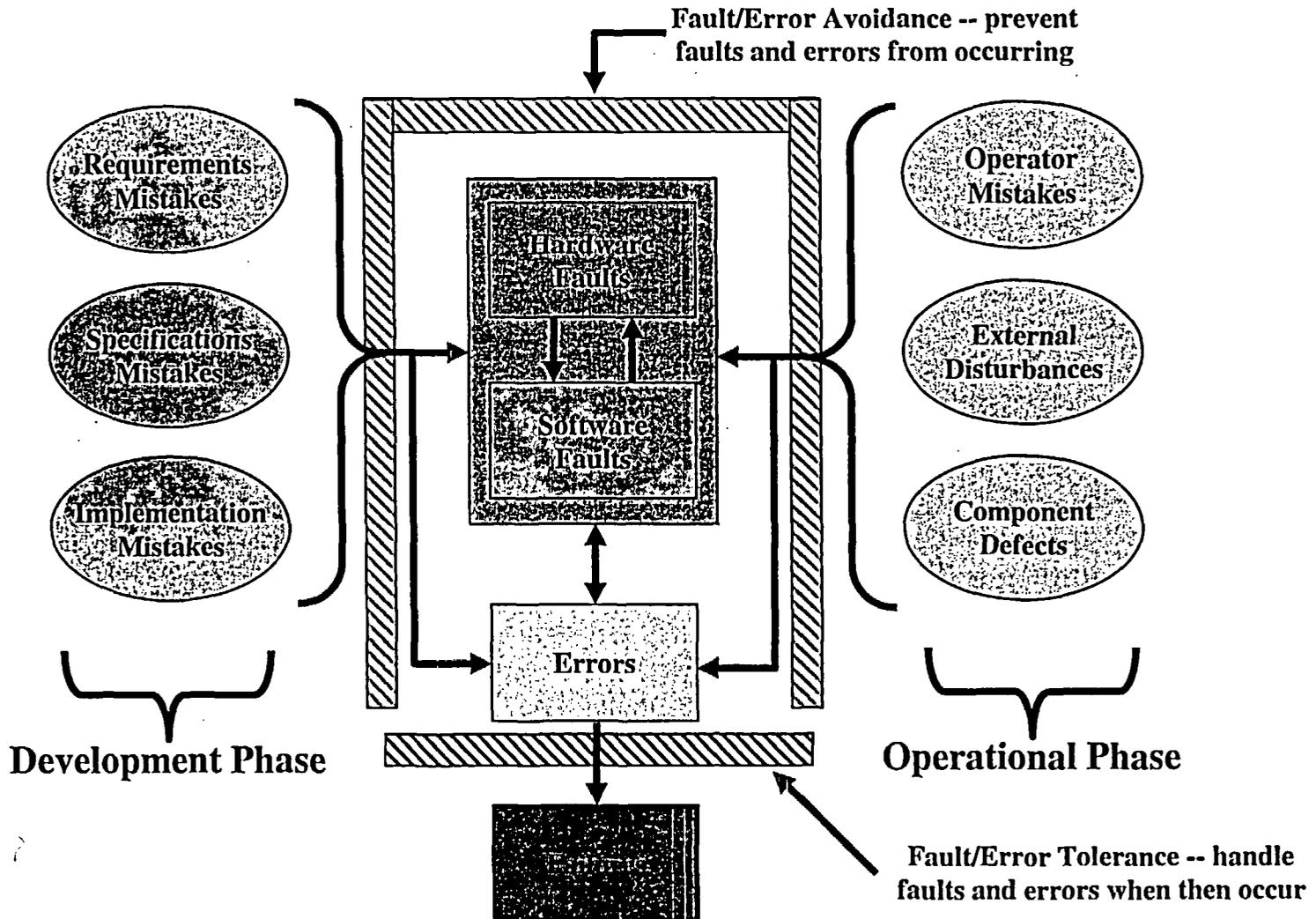


- T_O -- maximum output delivery time
- T_I -- maximum input collection time
- T_P -- maximum processing time
- T_T -- maximum sampling period
- T_R -- maximum time to handle faults



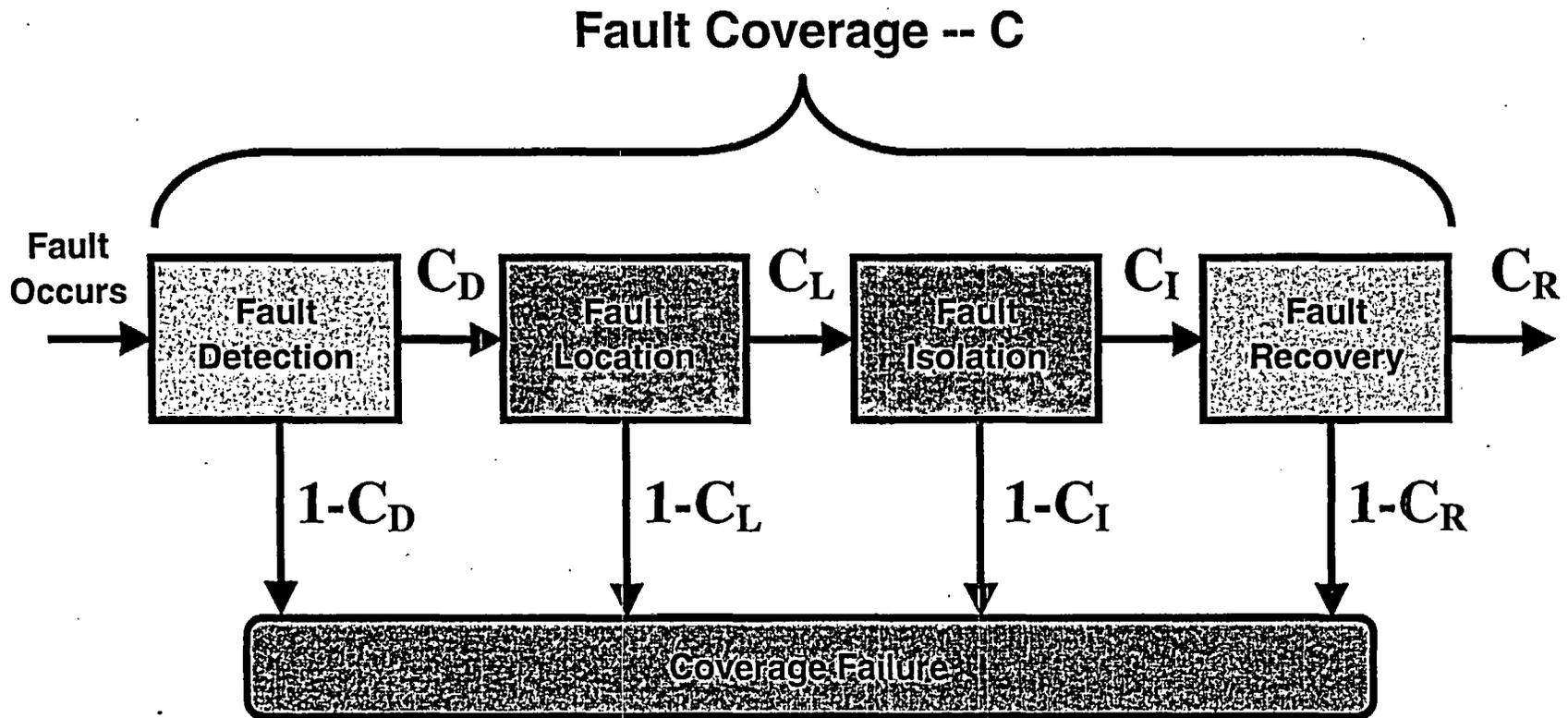
Background

Causes and Effects of Faults



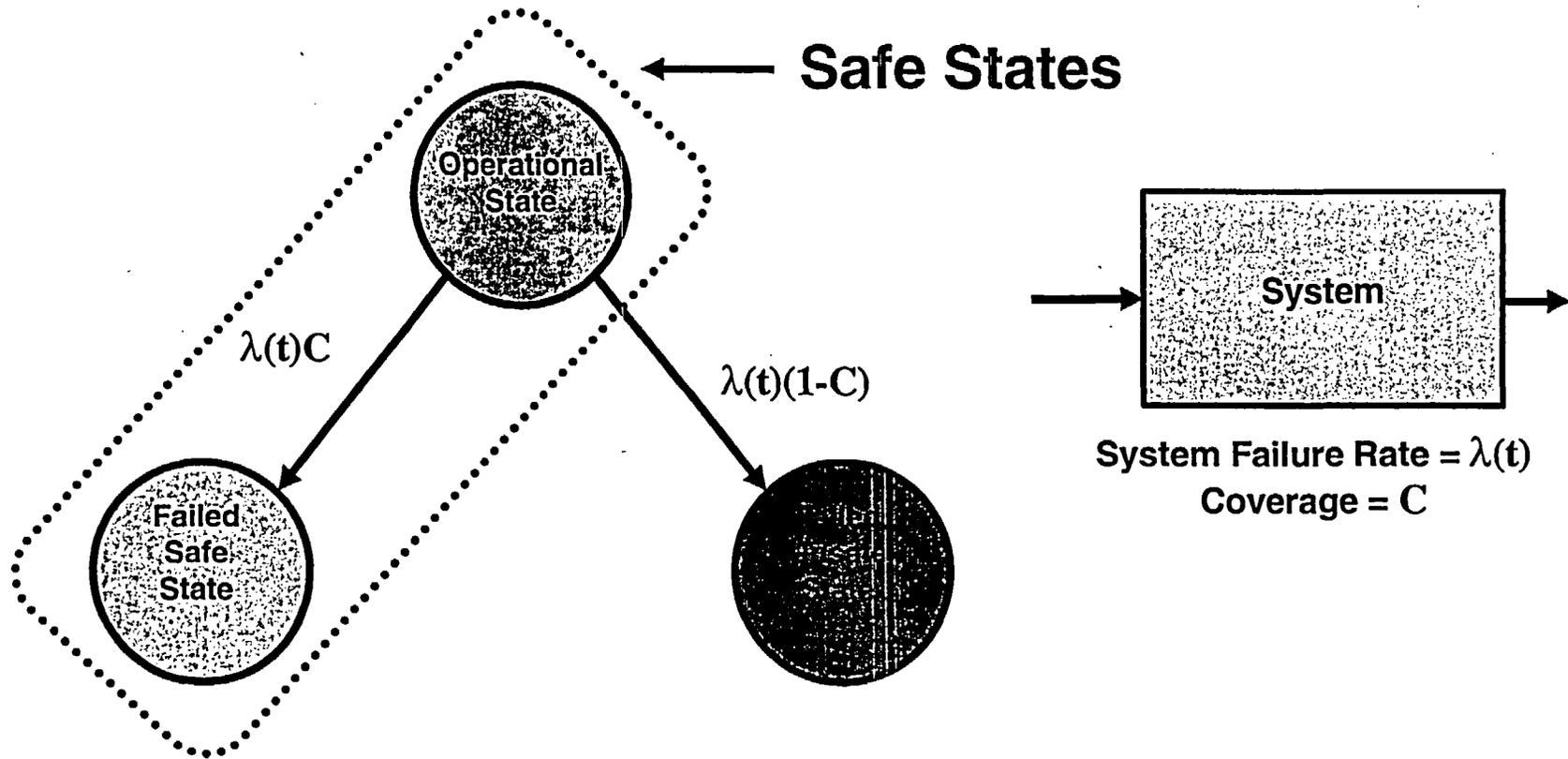
Background

Concept of Fault Coverage



Background

Simple Three-State System Safety Model



- **Fault Coverage (C)** – the conditional probability that a system correctly handles a fault, given that a fault has occurred



Background

Safety, $S(t)$

- **Safety, $S(t)$** – the probability that a system will either perform its functions correctly or will discontinue its functions in a defined safe manner.
- For the simple three-state safety model $S(t)$ can be expressed as the probability of being in either the “operational” or “failed-safe” states.
- **Steady-State Safety (S_{ss})** can be expressed as

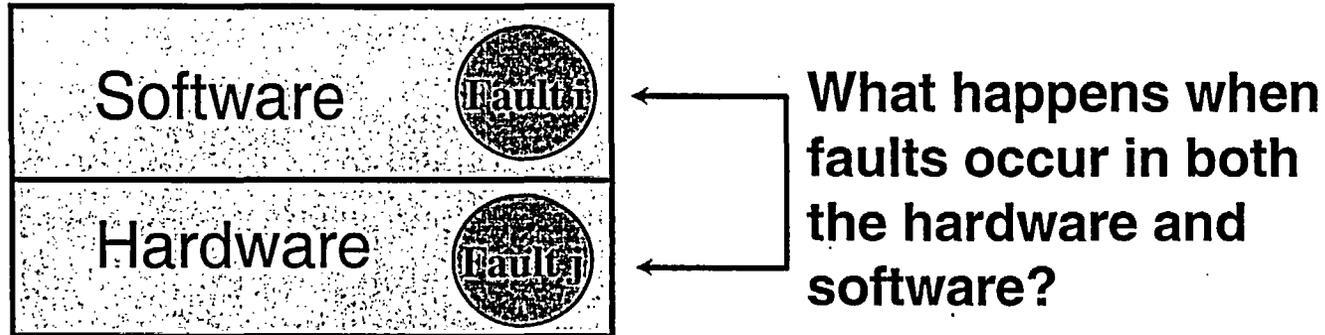
$$S_{ss} = \lim_{t \rightarrow \infty} S(t)$$

- The fault coverage represents a conservative estimate of the lower bound on Steady-State Safety
- For the simple three-state safety model, $S_{ss} = C$



Challenges

Hardware and Software are not Independent

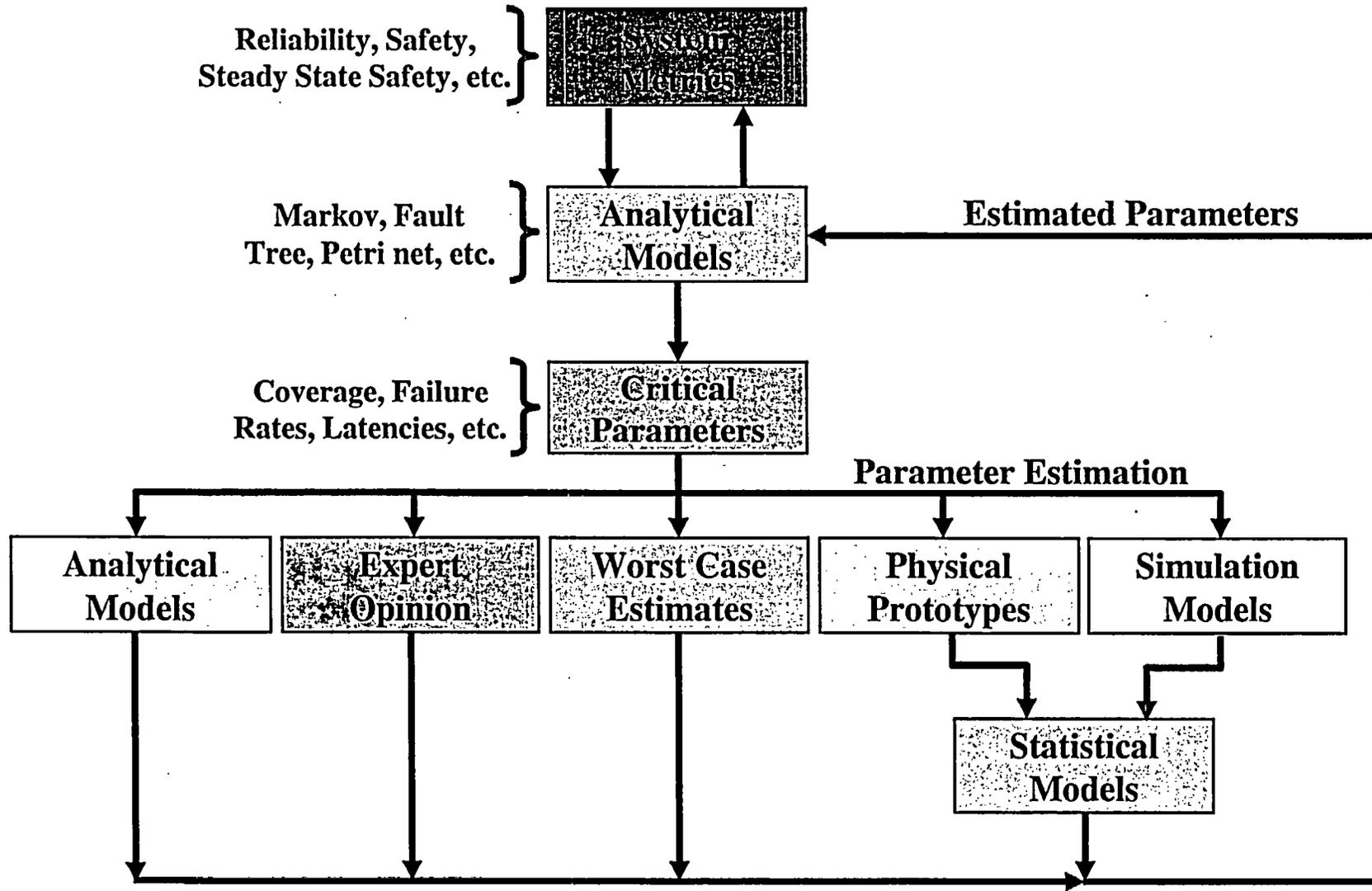


- **Software must execute on a hardware platform. The operation of the integrated hardware/software system is critical.**
- **A fault in software (Fault i) in combination with a fault in hardware (Fault j) can result in unsafe conditions and/or unreliable operation.**
- **Much of the software in safety-critical systems is designed to handle fault detection, fault location, fault isolation, and fault recovery. Such software is often unexercised.**



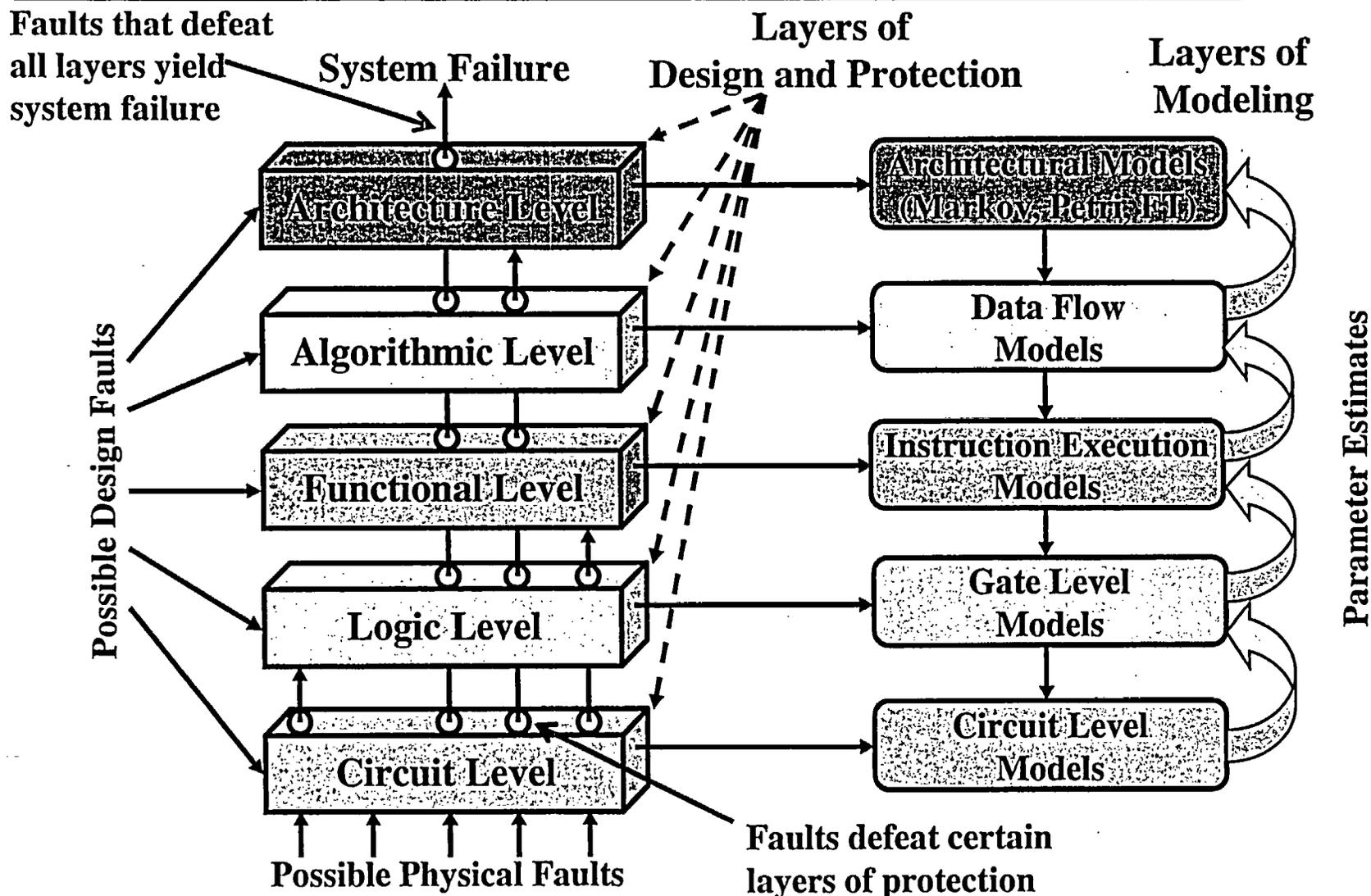
System Modeling Methodology

Overview of the Process



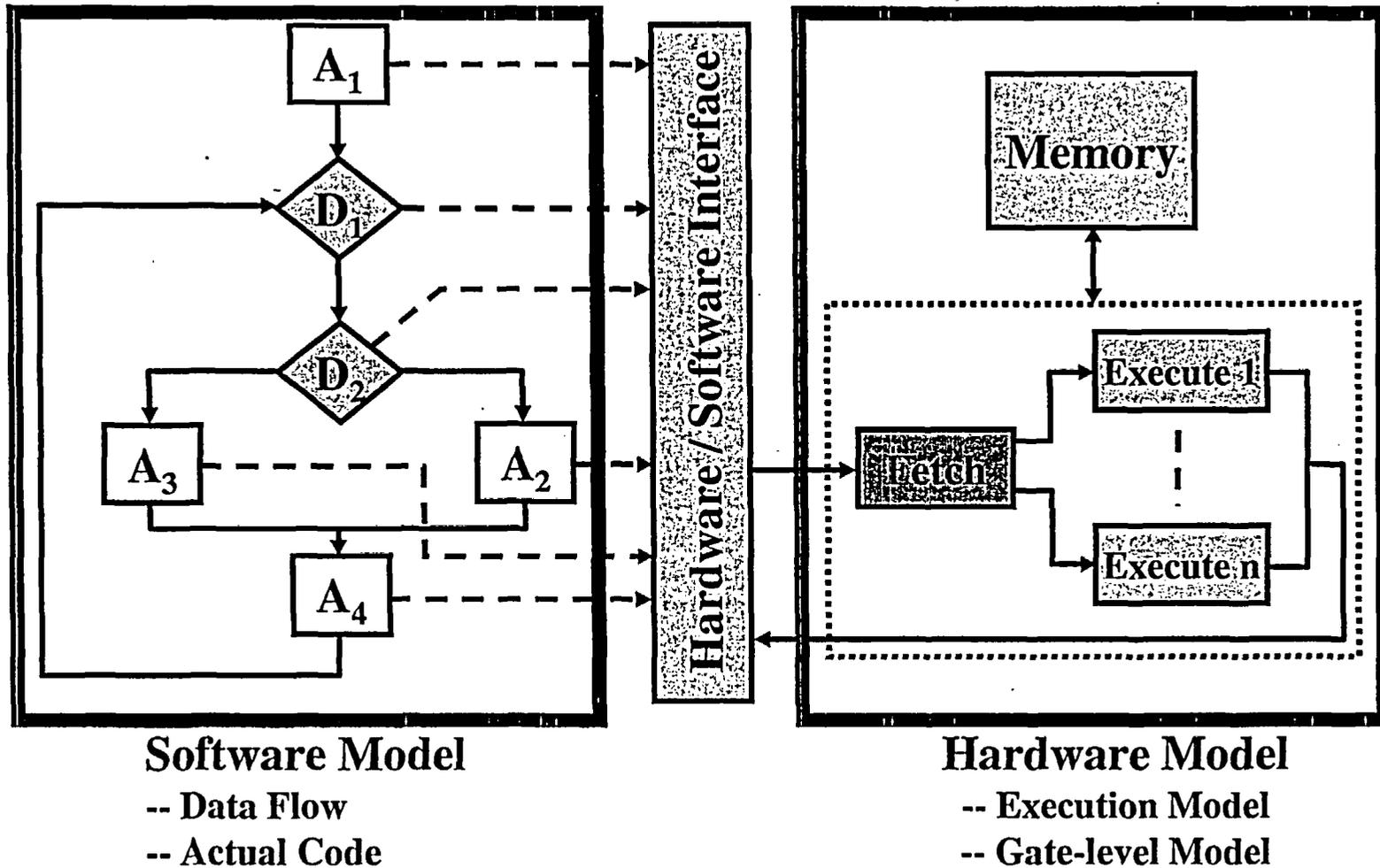
System Modeling Methodology

Hierarchical Approach



System Modeling Methodology

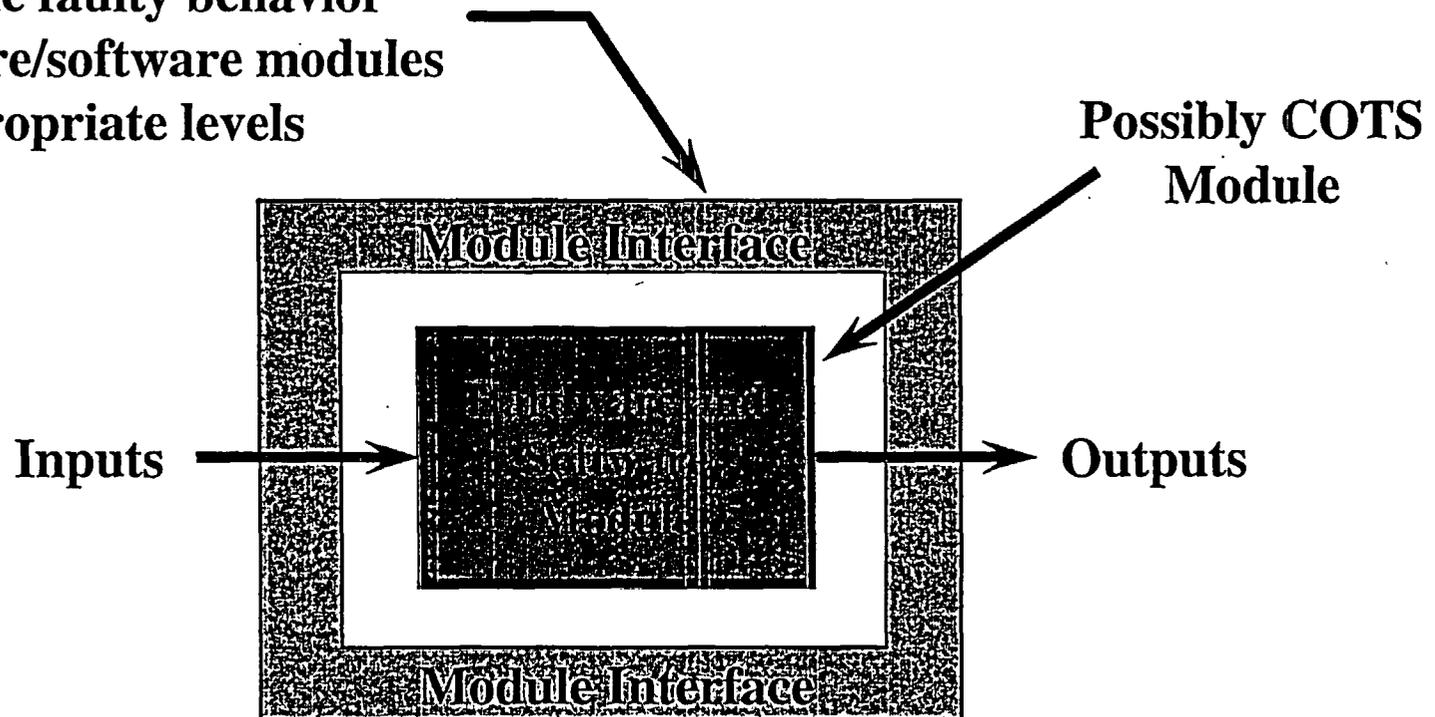
Hardware/Software Integrated Modeling



System Modeling Methodology

Characterization of Faulty Behavior

Models are developed which describe the faulty behavior of hardware/software modules at the appropriate levels



Examples of UVA Research

Johnson, B. and Aylor, J., "Reliability and Safety Analysis of a Fault-Tolerant Controller", *IEEE Transactions on Reliability*, Vol. 35, No. 4, Oct. 1986, pp. 355-362.

Welke, S., Johnson, B., and Aylor, J. "Reliability Modeling of Hardware/Software Systems", *IEEE Transactions on Reliability*, Vol. 44, No. 3, Sept. 1995, pp. 413-418.

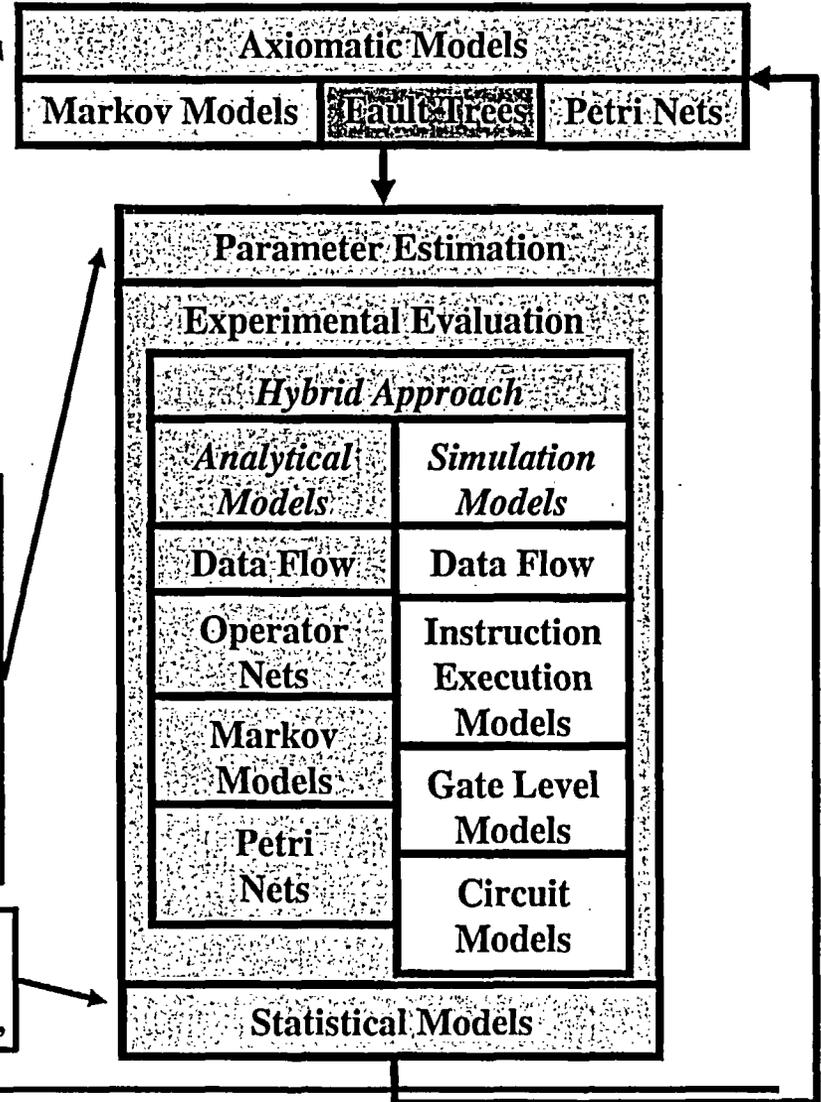
Choi, C., Johnson, B., and Profeta, III, J., "Safety Issues in the Comparative Analysis of Dependable Architectures", *IEEE Transactions on Reliability*, Vol. 46, No. 3, Sept. 1997, pp. 316-322.

Smith, D., Johnson, B., and Profeta, III, J., "System Dependability Evaluation Using a Fault List Generation Algorithm", *IEEE Transactions on Computers*, Vol. 45, No. 8, Aug. 1996, pp. 974-979.

Kaufman, L. M., Johnson, B. W., and Bechta Dugan, J., "Coverage Estimation Using Statistics of Extremes for When Testing Reveals No Failures", *IEEE Transactions on Computers*, Vol. 51, No. 1, January 2002, pp. 3-12.

DeLong, T, Johnson, B., and Profeta, III, J., "A Fault Injection Technique for VHDL Behavioral-Level Models", *IEEE Design and Test of Computers*, Vol. 13, No. 4, Mar. 1996, pp. 24-33.

Smith, D., Johnson, B., Andrianos, N, and Profeta, III, J., "A Variance Reduction Technique Using Fault Expansion for Fault Coverage Estimation", *IEEE Transactions on Reliability*, Vol. 46, No. 3, Sept. 1997, pp. 366-374.



Examples of UVA Research (Continued)

- **Theoretical foundation of safety assessment process**
 - ◆ Ideas were created while in industry (Harris Corporation)
 - ◆ Ideas applied to Harris helicopter flight control system
- **Modeling and Simulation Tools**
 - ◆ ADEPT was the first implementation of system modeling techniques (funded by DARPA, NSF, and NASA)
 - ◆ ROBUST was first hierarchical fault simulation tool (funded by U.S. Air Force)
- **Peer Review of Research**
 - ◆ Research began in 1984 and has been continuously funded by NASA, NSF, DARPA, IBM, Hughes, SRC, Boeing, Ansaldo, FRA, Lockheed Martin, and others
 - ◆ 10 PhDs and 32 MS students have received degrees working on the research topics (4 PhDs in progress)
 - ◆ More than 125 peer-reviewed publications and 1 patent
 - ◆ Named IEEE Fellow for contributions



Applications

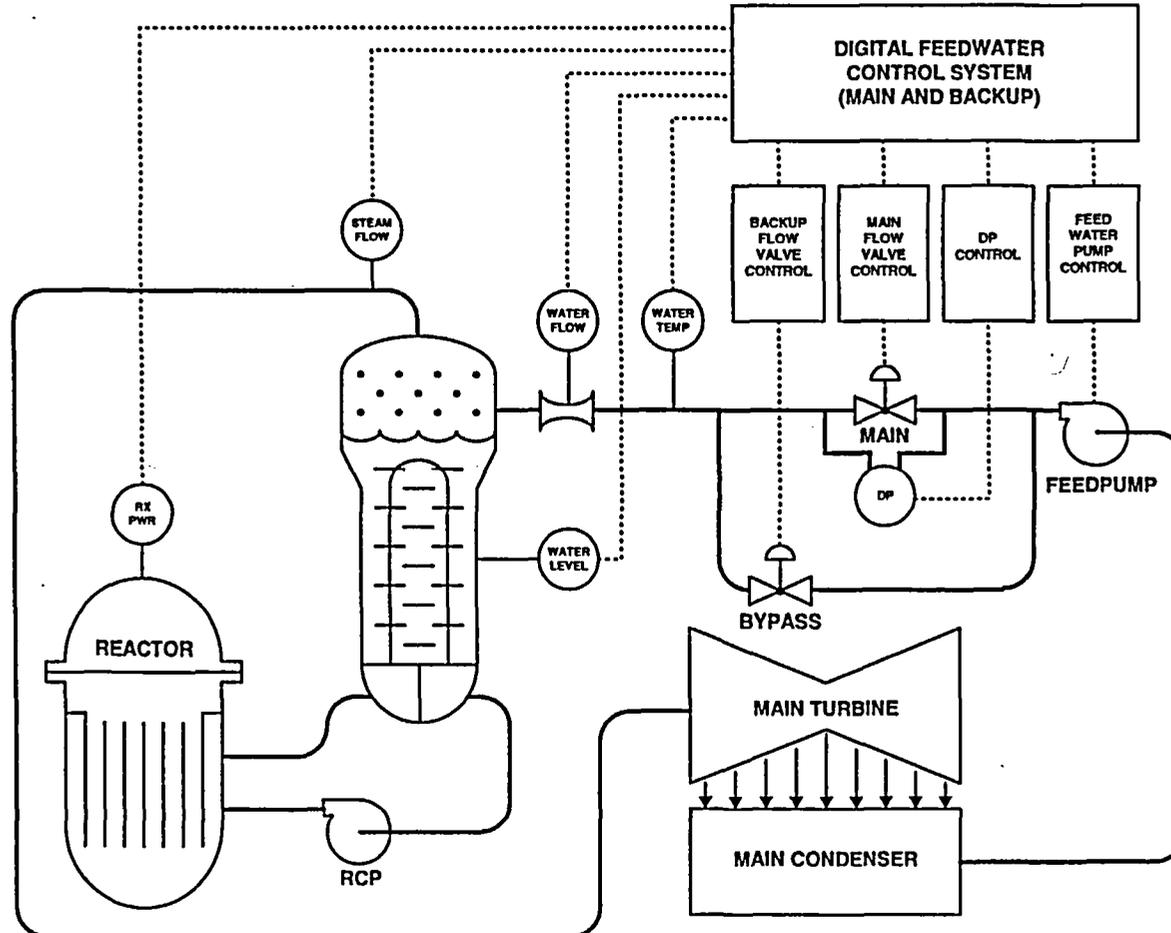
- **Los Angeles Metro Green Line Transit System**
 - ◆ Actual software executing on a hardware model
 - ◆ Results obtained for more than 10 billion experiments
 - ◆ Uncovered three software design faults
 - ◆ Results approved by California Public Utility Commission
- **Copenhagen Metro System**
 - ◆ Physical prototype running complete software system
 - ◆ Gate-level simulations of a complete 32-bit processor
 - ◆ Uncovered one software design fault
 - ◆ Approved by TUV Rheinland (Cologne, Germany)
- **Other systems currently being analyzed**
 - ◆ Calvert Cliffs Digital Feedwater Control System
 - ◆ New York City Transit Authority train control system
 - ◆ CSX communication-based train control system (Georgia)
 - ◆ Magnetically levitated train system (Pittsburgh)
 - ◆ Illinois Department of Transportation train control system



Applications

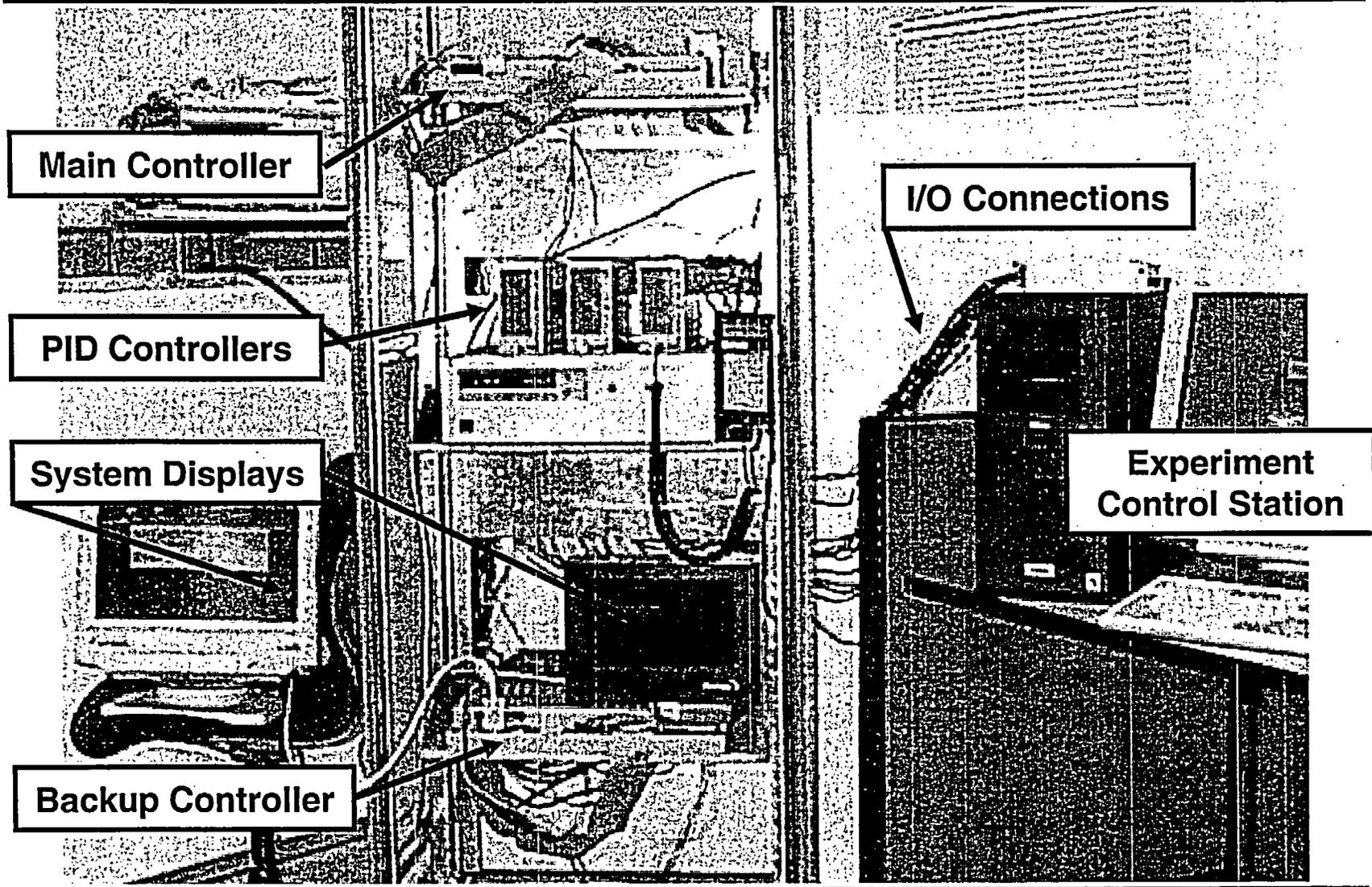
Overview of Calvert Cliffs DFWCS

- Purpose: control the water level in its associated steam generator from ~1% to 100% power



Applications

Experimental DFWCS Prototype



Applications

Dynamic Fault Tree Model for DFWCS

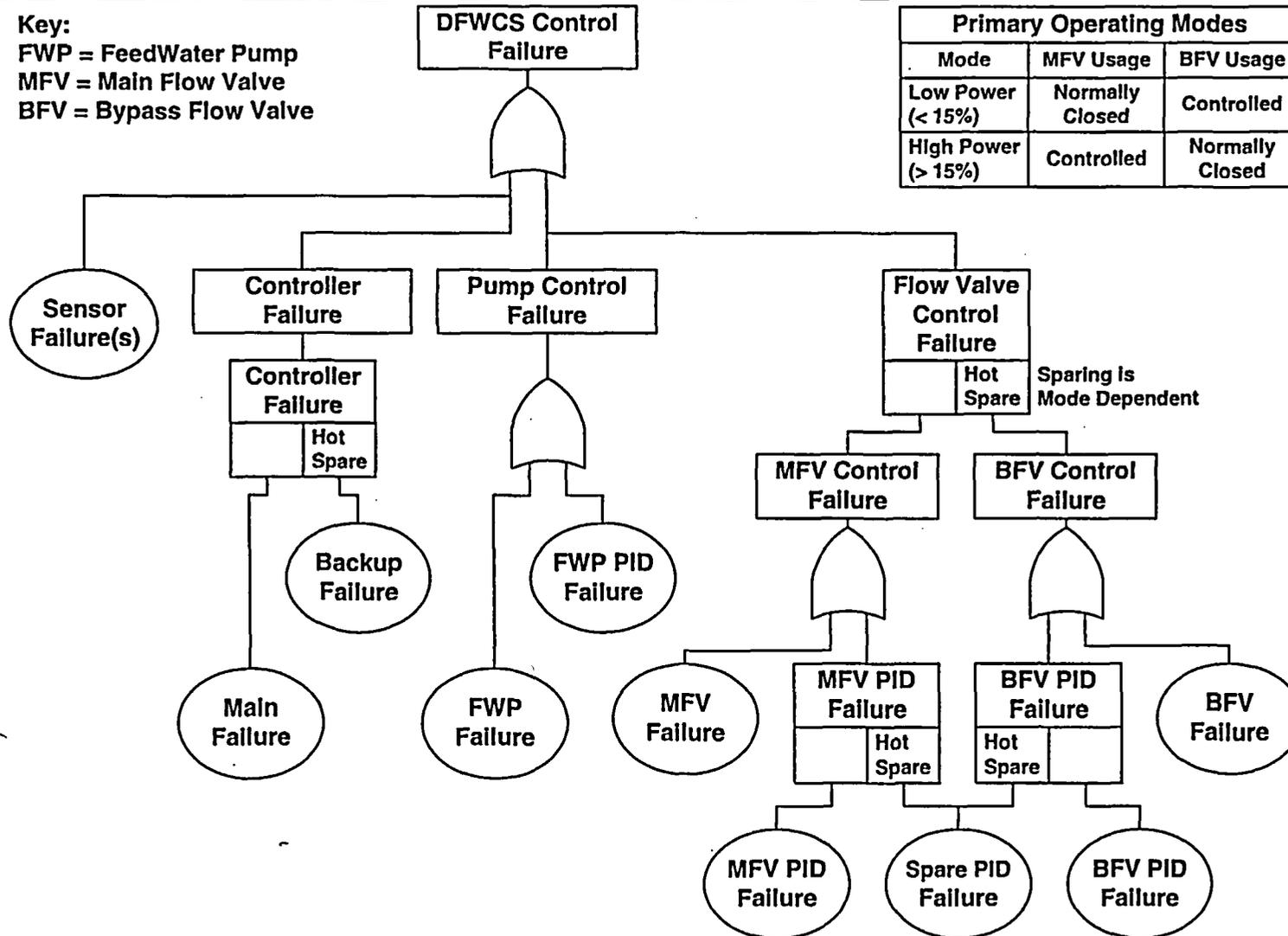
Key:

FWP = FeedWater Pump

MFV = Main Flow Valve

BFV = Bypass Flow Valve

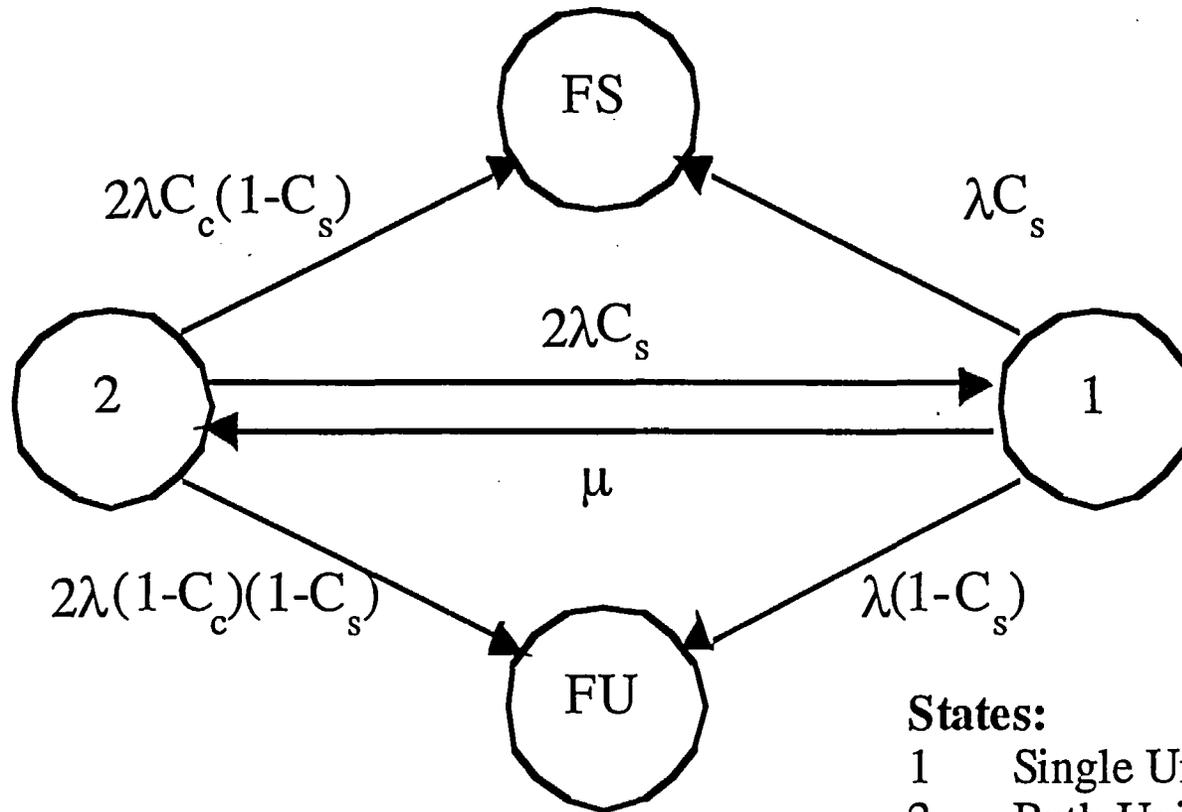
| Primary Operating Modes | | |
|-------------------------|-----------------|-----------------|
| Mode | MFV Usage | BFV Usage |
| Low Power (< 15%) | Normally Closed | Controlled |
| High Power (> 15%) | Controlled | Normally Closed |



Applications

Conversion to a Markov Model

- The resulting Markov model



States:

- 1 Single Unit Operational
- 2 Both Units Operational
- FS Failed-Safe
- FU Failed-Unsafe



Applications

MTTUF and S_{SS} Expressions

- Resulting MTTUF Expression:

$$\text{MTTUF} = \frac{1 + 2C_s}{2\lambda(1 - C_s)[1 - C_c + C_s]}$$

- Resulting S_{SS} Expression:

$$S_{SS} = C_c(1 - C_s) + C_s^2$$

Reference

Choi, C., Johnson, B., and Profeta, III, J., "Safety Issues in the Comparative Analysis of Dependable Architectures", *IEEE Transactions on Reliability*, Vol. 46, No. 3, Sept. 1997, pp. 316-322.



Applications

Fault Injection Techniques for DFWCS

- **Two approaches were investigated: Software-based and Simulation-based fault injection**
 - ◆ **Both fault injection approaches center around assessment of the Main Controller**

- **Software-based fault injection approach**
 - ◆ **Uses software interrupts in operating system to modify register and memory contents during execution of the DFWCS software**

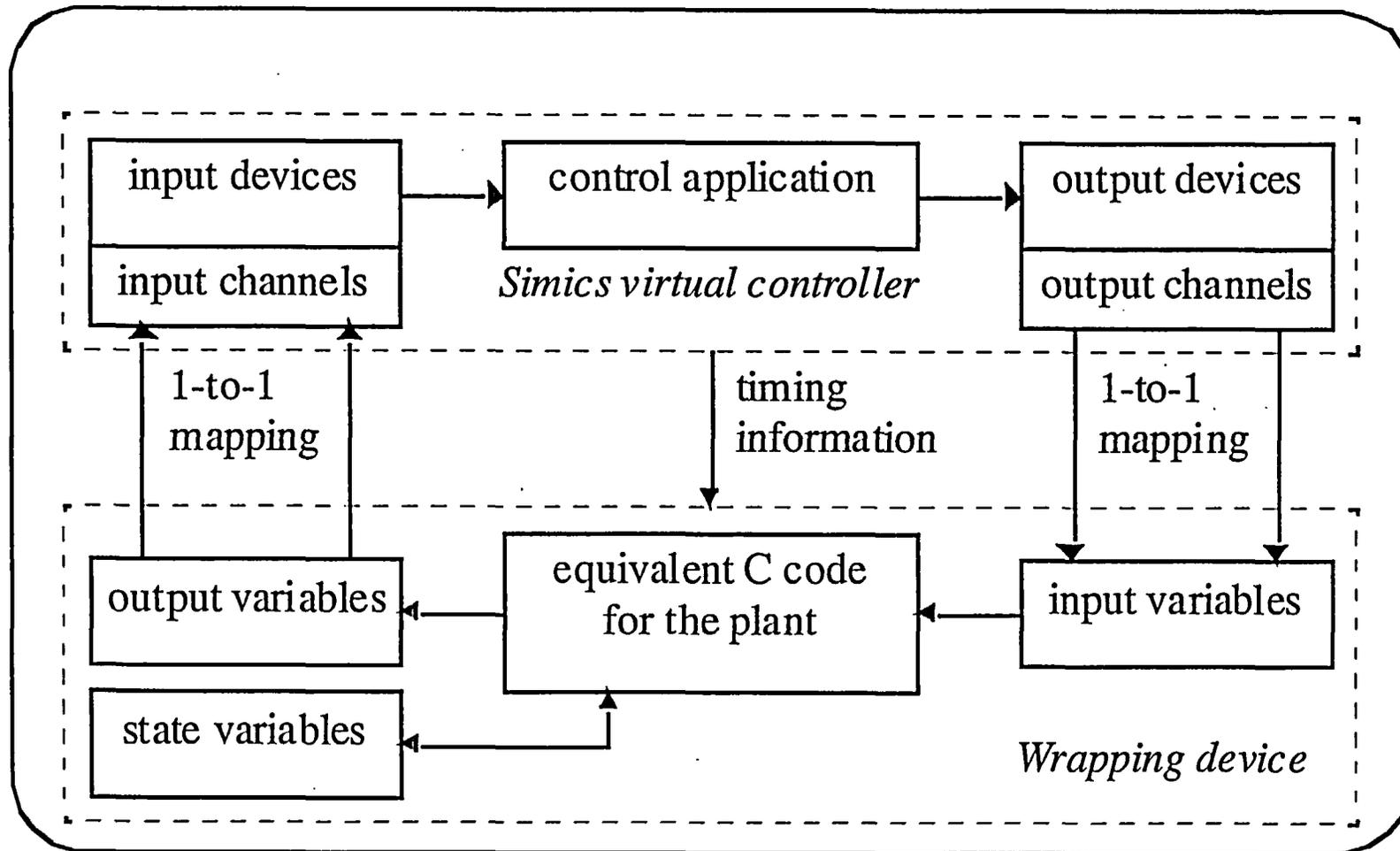
- **Simulation-based fault injection approach**
 - ◆ **Uses COTS simulation tool (Simics) to seamlessly replace the Main Controller hardware with a simulation model**
 - ◆ **Tool allows access to complete programmer's model of the system to perform fault injection**



Applications

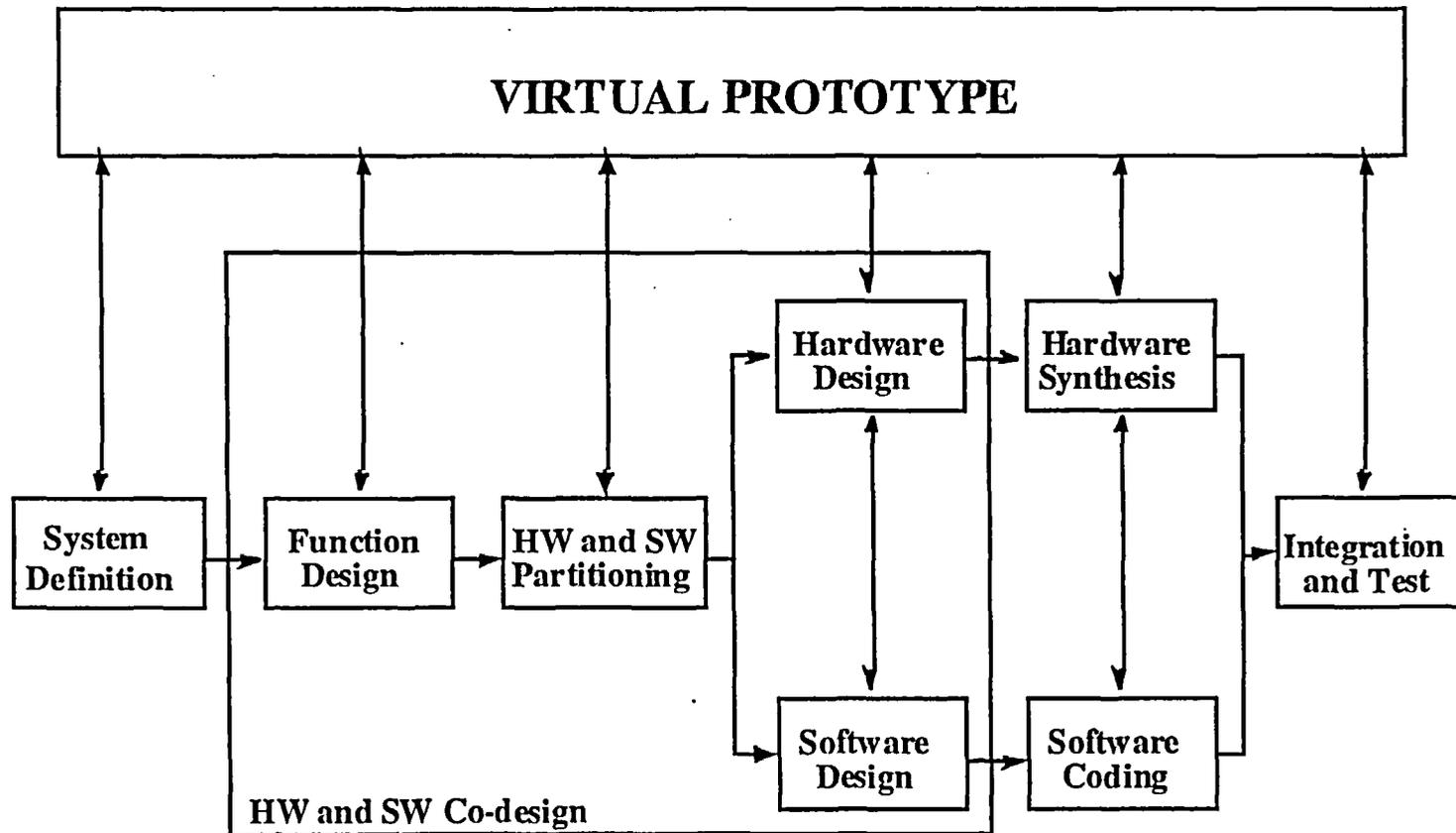
Simulation Environment and Capabilities

Simics simulation framework



Future Research Goal

Design and Assessment Process



Summary

- **A safety assessment process has been developed based on fault injection techniques and the consideration of the integrated hardware/software system**
- **The process has been applied to multiple practical commercial applications and approved by an independent safety assessors (e.g., TUV Rheinland)**
- **Toolsets and computing resources are being developed to allow safety/reliability assessment over the web**
 - ◆ **Equipment under evaluation stays at supplier's facility**
- **We are currently developing new fault models and new statistical models to support the approach**
- **We are currently developing new modeling and fault injection techniques based on COTS software tools (Simics)**



Software Reliability Modeling

The Use of Software Measures to Predict
Software Quality and Reliability

PRESENTED BY

Prof. Carol Smidts

csmidts@eng.umd.edu

COAUTHORED BY

Dr. Ming Li

mli@wam.umd.edu

March 26, 2004



Conclusions

- A method to use software measures as a quantitative technique for predicting software quality and reliability has been developed and piloted
- The results of this method to date have been very promising.
- The method parallels the current review method, so it should be straight forward to implement
- Work is currently ongoing to validate the method on a large, high reliability nuclear application.

The primary objective of this research is to provide a systematic framework to enhance current review practice for software in the NRC.



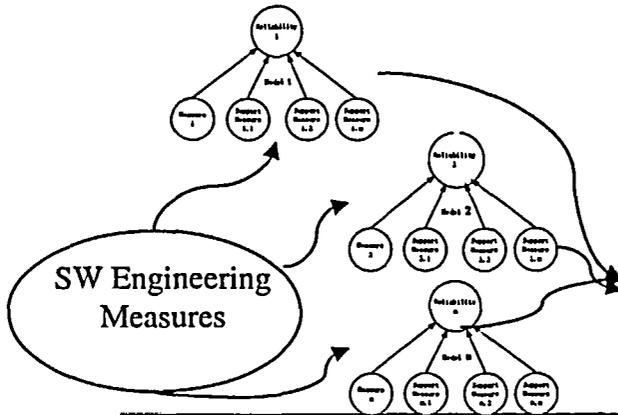
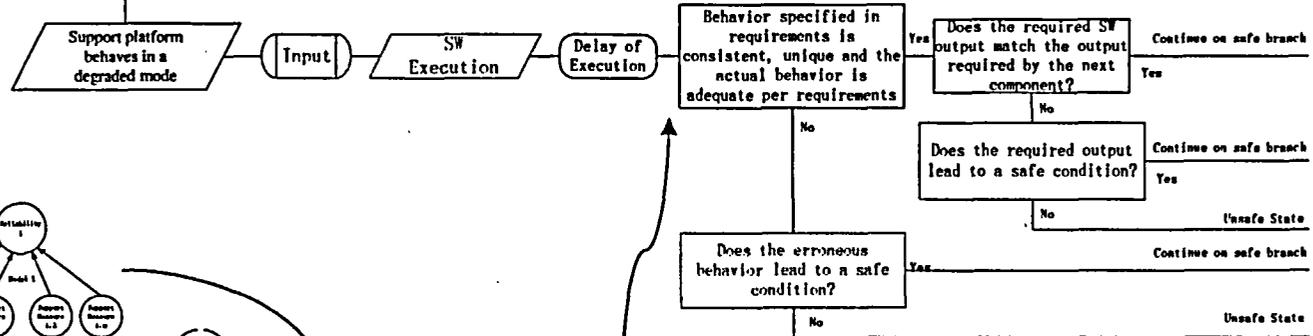
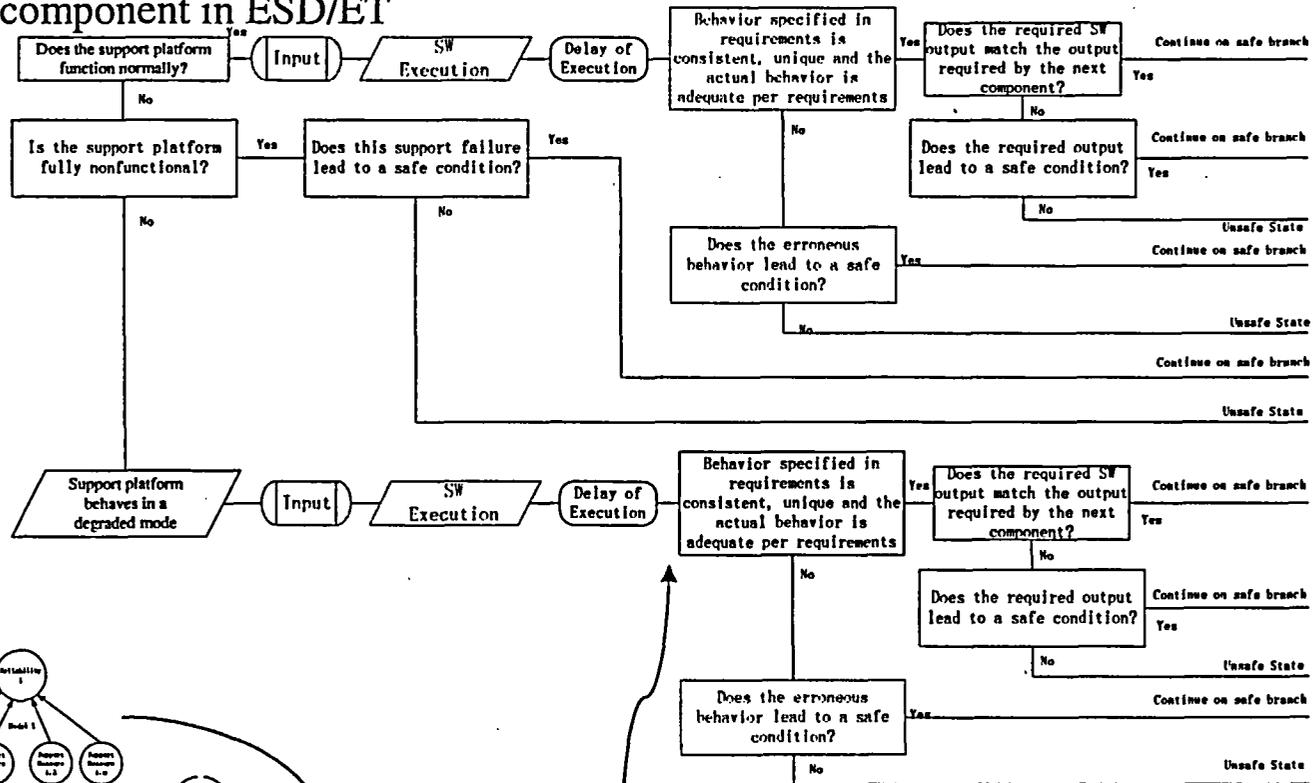
Project History

- Lawrence Livermore National Laboratory (LLNL) Study (1996 –1998)
- University of Maryland
 - Expert Opinion Study (1998 – 2000)
 - Validation Study (2001 – 2002 (9 months))
 - Large-Scale Validation Study (2004 - present)



PRA Framework for I&C Systems

Software component in ESD/ET



Probability Estimation

Parameter and Model Uncertainty

Subjective Information About Models

| | |
|---------|--|
| Model 1 | |
| Model 2 | |
| Model n | |

Objective Information About Models

| | |
|---------|--|
| Model 1 | |
| Model 2 | |
| Model n | |

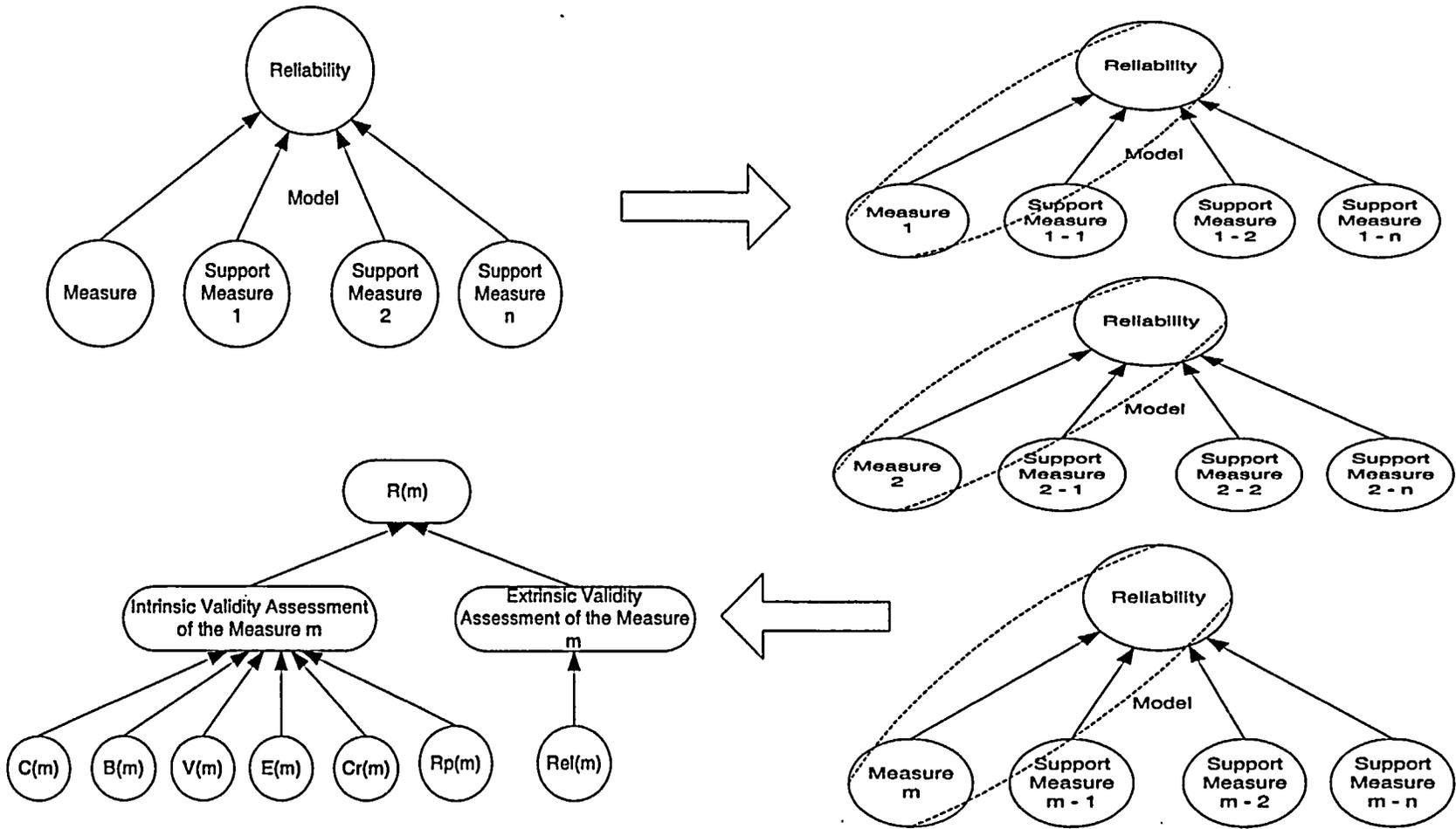


Philosophy Behind This Research

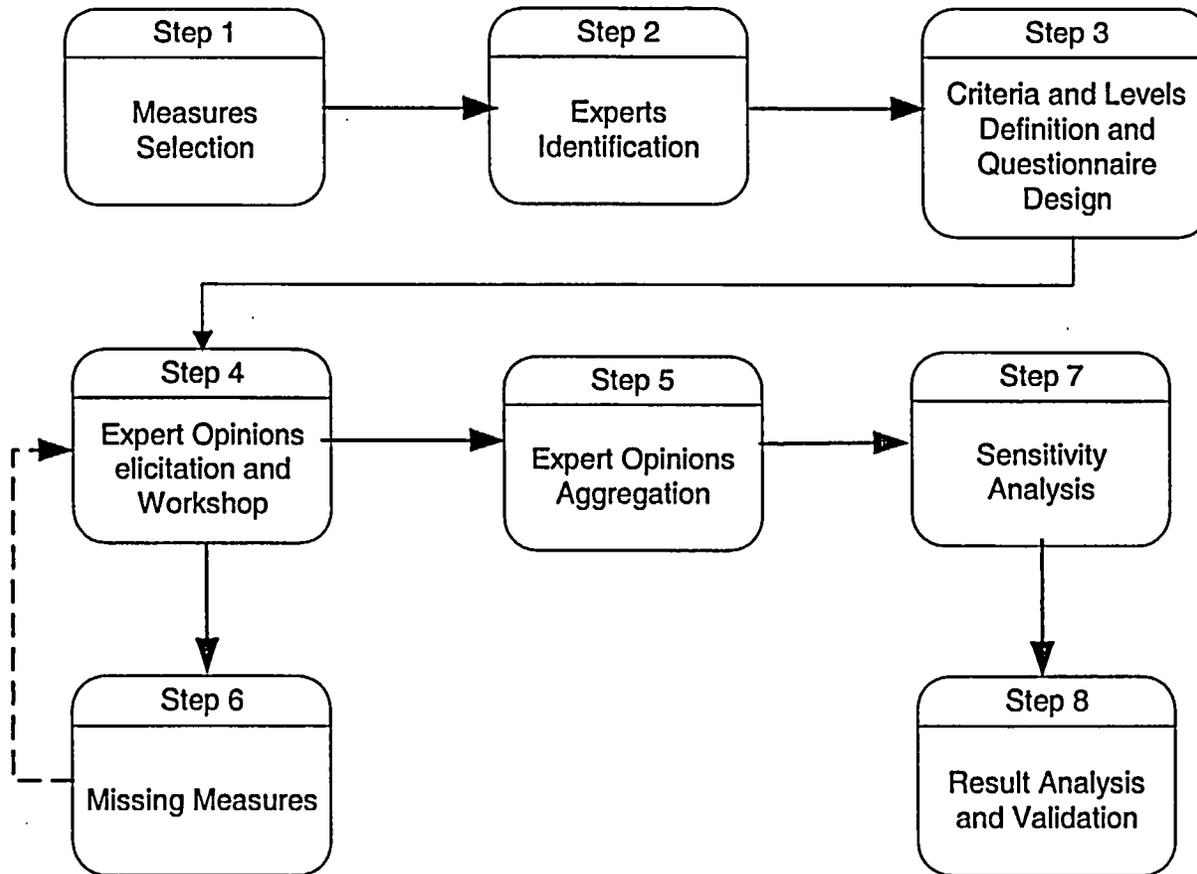
- How is software reliability determined?
 - Product characteristics
 - Project characteristics
 - Development characteristics
 - Operational environment
- Software engineering measures determine software reliability



From Measures to Reliability



Ranking Process



Experts Selection

| Expert | Occupation | Area of Expertise |
|--------------------|-------------------|--|
| Alain Abran | Industry/Academia | Telecommunication, Financial |
| David Card | Industry | Software measurement and process improvement |
| William Everett | Industry | Telecommunication, Aerospace |
| Jon Hagar | Industry | Aerospace |
| Herbert Hecht | Industry | Nuclear, Aerospace |
| Watts Humphrey | Industry/Academia | Aerospace |
| Michael Lyu | Industry/Academia | Telecommunication, Aerospace |
| Jean-Claude Laprie | Academia | Telecommunication, Aerospace |
| William Petrick | Industry | Nuclear |
| Allen Nikora | Academia | Software reliability modeling |



Pre-selected 30 Measures

Intermediate Results from LLNL:

| | |
|--|--|
| Bugs per line of code (Gaffney estimate) | Functional test coverage |
| Cause & effect graphing | Graph-theoretic static architecture complexity |
| Code defect density | Man hours per major defect detected |
| Cohesion | Mean time to failure |
| Completeness | Minimal unit test case determination |
| Cumulative failure profile | Modular test coverage |
| Cyclomatic complexity | Mutation testing (error seeding) |
| Data flow complexity | Number of faults remaining (error seeding) |
| Design defect density | Requirements compliance |
| Error distribution | Requirements specification change requests |
| Failure rate | Requirements traceability |
| Fault density | Reviews, inspections and walkthroughs |
| Fault number days | Software capability maturity model |
| Feature point analysis | System design complexity |
| Function point analysis | Test coverage |

Ranking Results

| Measure | Development Phase | | | |
|--|-------------------|--------|----------------|---------|
| | Requirements | Design | Implementation | Testing |
| Bugs per line of code (Gaffney estimate) | | | 0.44 | 0.37 |
| Cause & effect graphing | 0.45 | 0.43 | 0.40 | 0.45 |
| Code defect density | | | 0.83 | 0.83 |
| Cohesion | | 0.45 | 0.37 | 0.37 |
| Completeness | 0.41 | 0.33 | 0.33 | 0.33 |
| Cumulative failure profile | | | | 0.80 |
| Cyclomatic complexity | | 0.74 | 0.77 | 0.74 |
| Data flow complexity | | 0.63 | 0.60 | 0.60 |
| Design defect density | | 0.77 | 0.77 | 0.76 |
| Error distribution | 0.70 | 0.70 | 0.69 | 0.69 |
| Failure rate | | | | 0.87 |
| Fault density | 0.73 | 0.76 | 0.77 | 0.77 |
| Fault number days | 0.63 | 0.73 | 0.73 | 0.75 |
| Feature point analysis | 0.44 | 0.47 | 0.47 | 0.43 |
| Function point analysis | 0.51 | 0.54 | 0.55 | 0.50 |
| Functional test coverage | | | | 0.61 |
| Graph-theoretic static architecture complexity | | 0.52 | 0.45 | 0.45 |
| Man hours per major defect detected | | 0.65 | 0.63 | 0.65 |
| Mean time to failure | | | | 0.81 |
| Minimal unit test case determination | | | 0.65 | 0.71 |
| Modular test coverage | | | | 0.70 |
| Mutation testing (error seeding) | | | | 0.47 |
| Number of faults remaining (error seeding) | 0.45 | 0.45 | 0.47 | 0.50 |
| Requirements compliance | 0.52 | 0.50 | 0.51 | 0.50 |
| Requirements specification change requests | 0.71 | 0.71 | 0.71 | 0.70 |
| Requirements traceability | | 0.58 | 0.57 | 0.57 |
| Reviews, inspections and walkthroughs | 0.62 | 0.61 | 0.61 | 0.62 |
| Software capability maturity model | 0.62 | 0.62 | 0.61 | 0.61 |
| System design complexity | | 0.56 | 0.55 | 0.55 |
| Test coverage | | | | 0.70 |

Ranking of Top 5 Non-OO Measures per Phase

| Rank | Requirements | Design | Implementation | Testing |
|------|--|--|-----------------------|----------------------------|
| 1 | Fault density | Design defect density | Code defect density | Failure rate |
| 2 | Requirements specification change requests | Cyclomatic complexity | Design defect density | Code defect density |
| 3 | Error distribution | Fault density | Cyclomatic complexity | Coverage factor |
| 4 | Reviews, inspections and walkthroughs | Fault number days | Fault density | Mean time to failure |
| 5 | Fault number days | Requirements specification change requests | Fault number days | Cumulative failure profile |



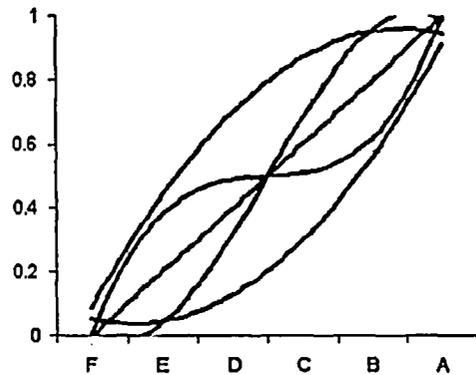
10 Missing Measures

Coverage factor
Full function point (FFP)
Mutation score
Class coupling
Class hierarchy nesting level
Lack of cohesion of methods (LCOM)
Number of children (NOC)
Number of class methods in a class
Number of key classes
Weighted method per class



Sensitivity Analysis - Variations

Letter – Real Conversion



Aggregation Weight

| Co | Be | Cr | Rep | Ex | Va | Rel |
|-------|-------|-------|-------|-------|-------|-------|
| 0.14 | 0.14 | 0.14 | 0.14 | 0.14 | 0.14 | 0.14 |
| 0.13 | 0.13 | 0.13 | 0.13 | 0.13 | 0.13 | 0.25 |
| 0.08 | 0.08 | 0.17 | 0.17 | 0.08 | 0.08 | 0.33 |
| 0.245 | 0.045 | 0.088 | 0.036 | 0.130 | 0.239 | 0.216 |
| 0.20 | 0.03 | 0.10 | 0.17 | 0.16 | 0.14 | 0.20 |
| 0 | 0 | 0.25 | 0.25 | 0.25 | 0 | 0.25 |

Aggregation Function

- Additive
- Multiplicative

Ranges of Correlation Coefficients

| Correlation Coefficient Range | Rate Count | Ranking Count |
|----------------------------------|---------------|------------------|
| 0 - 0.8 | 0 | 1 |
| 0.8 - 0.9 | 4 | 8 |
| 0.9 - 0.99 | 90 | 92 |
| 0.99 - 1.0 | 11 | 4 |



Validation Method

1. Selection of the Application;
2. Measures/Families Selection;
3. Reliability Assessment;
4. Construction of Reliability Prediction Systems;
5. Measurement and Analysis;
6. Peer Review

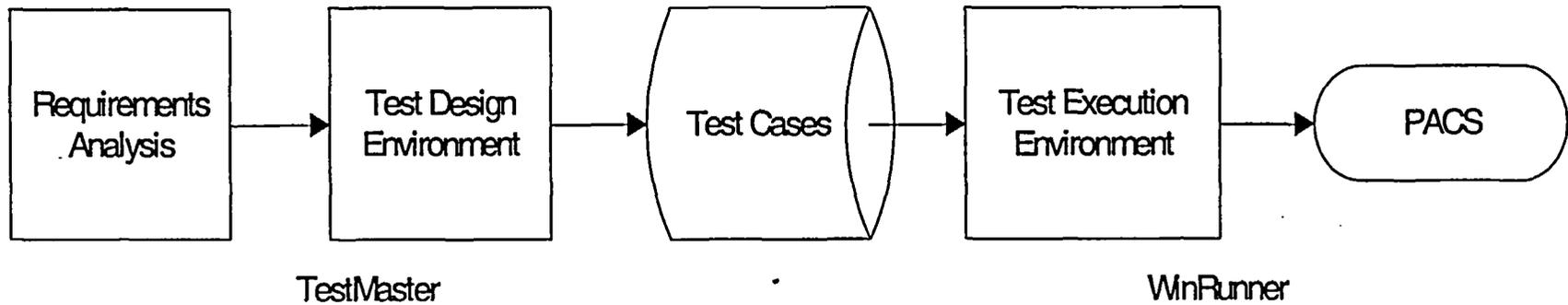


Validation

- Application under validation: PACS
 - PACS 1: CMM Level 4, Industry developed, C++, reliability ~ 0.92 per demand
 - PACS 2: West Virginia University developed, C++, reliability ~ 0.999 per demand (Sponsored by NASA)
- Measures used in validation:
 - Mean time to failure
 - Defect density
 - Test coverage
 - Requirements traceability
 - Function point
 - Bugs per line of code (Gaffney estimate)

Reliability Assessment

- Reliability testing environment



The Operational Profile

| No | Description of the Event | Probability |
|-----|--|-------------|
| 1. | Entering a good card: A good card is card that has the card data in the correct format and has a data that's in the database. In other words this event reflects the number of times a genuine card is being entered in the system. | 0.97 |
| 2. | Entering a good PIN: A good PIN is the event that reflects that the four digits of the PIN are correct and match the entry in the database. | 0.8 |
| 3. | Entry of the 1 st digit within time: The allowed time for entry of the first digit of the PIN is 10 seconds. | 0.98 |
| 4. | Entry of subsequent digits of PIN within time: The allowed time is 5 seconds | 0.97 |
| 5. | Erasure of a PIN digit: The PIN digits are erased whenever the keys # or * are pressed. | 0.001 |
| 6. | User able to pass within the stipulated time after opening of gate | 0.99 |
| 7. | Guard is requested for extra time | 0.01 |
| 8. | Guard allows extra 10 seconds. | 0.01 |
| 9. | Guard Override: This event refers to the event of the guard over riding the verdict of the system. The system passes control to the guard after three failed attempts of entry of PIN/ Card. The message "See Officer" is displayed on the LED and the guard has the ability to allow the user to get in (over ride) or reset the system to its initial state. | 0.5 |
| 10. | Hardware Failure : Although failure of any register from R1 to R11 will induce a system failure, only failure of register R5 and combined failure of registers R1, R2, R3, R4 and R9 results in a failure of level 1. The failure probability is calculated assuming probability of failure of a typical register to be 0.001 per demand. | 0.001 |



Reliability Assessment

- Reliability is determined by:

$$R = \frac{n - r + 1}{n + 1}$$

R Reliability

n Number of runs

r Number of failures

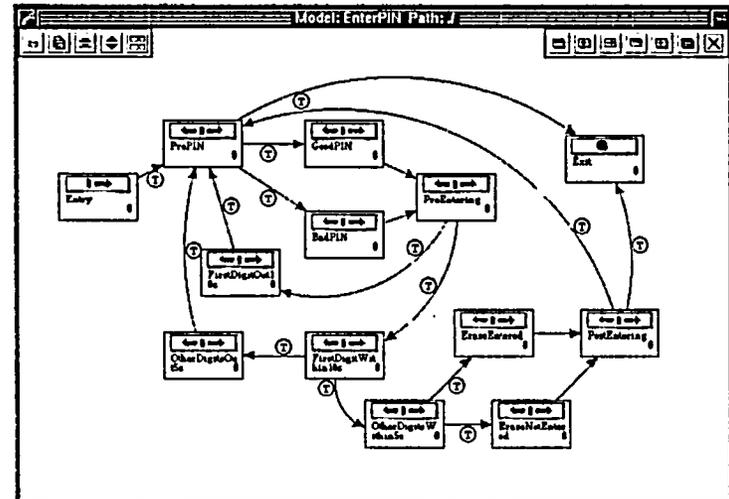
RePSs

- MTTF RePS

$$P_s = e^{-\frac{1}{\rho \cdot MTTF}}$$

- Defect Density RePS

$$p_s = 1 - \prod_i P(i) * I(i) * E(i)$$



RePSs

- Test Coverage RePS

- Derive the number of defects remaining from the number of defects tested.

$$C^0 = a_0 \ln[1 + a_1 (\exp(a_2 C_1) - 1)]$$

$$N = N^0 / C^0$$

$$p_s = e^{-\frac{K}{T_L} N \tau}$$

- C_1 : statement coverage
- K : fault exposure ratio obtained using the finite state machine model.

RePSs

- Requirements Traceability RePS
 - Each untraceable requirement is a defect
 - Apply the Finite State Machine techniques used in Defect Density RePS to obtain the value of P_s
- Function Point Analysis
 - Derived the number of defects remaining from the Function Point counting using Capers Jones data (see next slide)
 - Applying $p_s = e^{-\frac{K}{T_L} N \tau}$
 - K is obtained from the literature

Excerpt From the Literature*

| Function points | Severity 1 (critical) | Severity 2 (significant) | Severity 3 (minor) | Severity 4 (cosmetic) | Total |
|-----------------|--------------------------|-----------------------------|-----------------------|--------------------------|---------|
| 1 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 1 | 0 | 1 |
| 100 | 1 | 4 | 14 | 20 | 39 |
| 1,000 | 6 | 78 | 222 | 250 | 556 |
| 10,000 | 127 | 1,225 | 4,224 | 2,872 | 8,448 |
| 100,000 | 2,658 | 15,946 | 66,440 | 47,837 | 132,880 |
| Average | 465 | 2,875 | 11,817 | 8,497 | 23,654 |
| Percent | 1.97 | 12.16 | 49.96 | 35.92 | 100.00 |

* Table 3.48 from Capers Jones, *Applied Software Measurement: Assuring Productivity and Quality*, 2nd Edition, McGraw-Hill, New York, 1996



RePSs

- Bugs per Line of Code

- Obtain the number of defects remaining from the LOC using an empirical relationship

$$F = \sum_{i=1}^N (4.2 + 0.0015S_i^{4/3})$$

- Applying $p_s = e^{-\frac{K}{T_L}F\tau}$
- K is obtained from the literature

Prediction Quality Indicator: pe

- Definition

$$pe = \frac{|p_s(real) - p_s(est)|}{1 - p_s(real)}$$

pe Prediction error

$p_s(real)$ The probability of success per demand obtained from reliability testing

$p_s(est)$ The probability of success per demand obtained from the RPS

Validation Results for PACS 1

| Measure | Value | p_s^* | pe | Original Rankings Based on Expert Opinion | Rankings Based On Validation |
|--|--------------------|----------|--------|---|------------------------------|
| Mean time to failure | 1267.6 seconds | 0.91849 | 0.0296 | 1 | 1 |
| Defect density | 11.72 defects/KLOC | 0.92243 | 0.0766 | 2 | 2 |
| Test coverage | 94.6% | 0.90800 | 0.0952 | 3 | 4 |
| Requirements traceability | 78.6% | 0.92243 | 0.0766 | 4 | 3 |
| Function point | 75.0 | 0.998546 | 0.9827 | 5 | 6 |
| Bugs per line of code (Gaffney estimate) | 66 (65.6) defects | 0.979902 | 0.7607 | 6 | 5 |
| $p_s(\text{real})$ | 0.916 | | | | |



Peer Review for PACS1

- The validation research was reviewed by four internationally known experts
 - David Card
 - Jon Hagar
 - Herbert Hecht
 - Michael Lyu

Validation Results for PACS 2 *

| Measure | Value | p_s | pe | Original Rankings Based on Expert Opinion | Rankings Based On Validation |
|---------------------------------|-------------------|--------|--------|---|------------------------------|
| Defect Density | 5.60 defects/KLOC | 0.9989 | 0.2667 | 2 | 2 |
| Test Coverage | 97.2% | 0.9988 | 0.2 | 3 | 4 |
| Requirements Traceability | 97.0% | 0.9989 | 0.2667 | 4 | 3 |
| Function Point | 78 | 0.9977 | 0.5333 | 5 | 5 |
| Bugs per Line of Code | 33.4 | 0.9853 | 8.8 | 6 | 6 |
| The real reliability estimation | 0.9985 | | | | |

* Funded by NASA IV&V



Related Publications

- Li, M., Smidts, C., “A Ranking of Software Engineering Measures Based On Expert Opinion”, *IEEE Transactions on Software Engineering*, pp. 811-24, Vol. 29 No. 9, Sept. 2003.
- Smidts C., Li M., “Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems”, prepared for the U.S. Nuclear Regulatory Commission, NUREG/GR-0019, UMD-RE-2000-23, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (2000).
- Li M., Smidts C., “Ranking Software Engineering Measures Related to Reliability Using Expert Opinion”, Proceedings of ISSRE, p. 246 – 258, San Jose, California, 8-11 October, 2000.
- Smidts, C., Cukic, B., et al, “Software Reliability Corroboration”, NASA Software Engineering Workshop, Greenbelt, MD, 4-6 December 2002.

Current Research

- Larger application, more measures and full lifecycle
 - Larger application: STAR system
 - More measures: Coverage Factor, CMM, Fault Days Number, Requirements Specification Change Request, Cause and Effect Graphing, Mutation Testing
 - Full lifecycle: requirements, design, coding, testing
- Improvements for RePSs
 - The estimation of the number of unknown defects
 - The PIE characteristics for unknown defects
 - The estimation of the “true” fault exposure ratio

Summary

- A method to use software measures as a quantitative technique for predicting software quality and reliability has been developed and piloted
- The results of this method to date have been very promising.
- The method parallels the current review method, so it should be straight forward to implement
- Work is currently ongoing to validate the method on a large, high reliability nuclear application.



United States Nuclear Regulatory Commission

Future Plans for Digital System Reliability Modeling

Steven A. Arndt

(saa@nrc.gov, 301-415-6502)

Division of Engineering Technology
Office of Nuclear Regulatory Research

March 26, 2004



United States Nuclear Regulatory Commission

OVERVIEW

- Conclusions
- Ongoing programs
 - UVa
 - UMd
 - BNL
 - Halden
- Future programs
 - Risk modeling
 - EPRI review/regulatory guide
 - Advanced reactor
- Coordination and interactions
- Summary



United States Nuclear Regulatory Commission

CONCLUSIONS

- Both continuing and new research is planned
- Continuing and future research will investigate different aspects of risk analysis of digital systems
- Research will continually review current and evolving methods
- Research will provide tools and guidance for NRR
- Coordination within the program and with other digital system research in the nuclear and non-nuclear fields is critical



United States Nuclear Regulatory Commission

ONGOING PROGRAMS

- UVa
 - New trial application using one of the three approved platforms
 - Development of new modeling methods based on COTS software tools
 - Work to support other parts of the research program
 - An integrated digital system assessment method that can be used by the NRC staff to independently assess digital system safety



United States Nuclear Regulatory Commission

ONGOING PROGRAMS (CONT)

- UMd
 - Larger scale application
 - Use of nuclear digital system (STAR)
 - Full lifecycle with more measures
 - An assessment method that can be used by the NRC staff to independently assess software quality and reliability
 - Quantitative information on the relative importance of software metrics will be used to inform the current review guidance



United States Nuclear Regulatory Commission

ONGOING PROGRAMS (CONT)

- BNL
 - Development of a processor level Markov model for one of the three approved platforms to identify the supporting analysis and data needed to model digital design features
 - Review and development of digital failure databases in conjunction with other database work
 - Development of quantitative methods for assessing software reliability for safety-critical systems in conjunction with other software work



United States Nuclear Regulatory Commission

ONGOING PROGRAMS (CONT)

- Halden
 - Continue to expand research in digital system reliability
 - Continue work in analysis of operational data to support risk analysis of COTS systems, risk assessment of human system interfaces, and the use of BBNs to combine qualitative and quantitative information
 - New work on integrated digital system risk analysis



United States Nuclear Regulatory Commission

FUTURE PROGRAMS

- Risk modeling project
 - Research to develop detailed PRA models of a set of example digital systems, in a example set of current generation PRAs
 - Will review current research to determine what is the most effective method for digital system modeling for inclusion in current generation PRA models
 - Will support, along with BNL development of review guidance



United States Nuclear Regulatory Commission

FUTURE PROGRAMS (CONT)

- EPRI report review/regulatory guide
 - EPRI report proposes a risk-informed approach to the defense in depth and diversity (D-i-D&D) requirements
 - The proposed method uses the RG 1.174 acceptance criteria and a “bounding” reliability analysis method
 - Could be the first of many risk informed digital systems submittals



United States Nuclear Regulatory Commission

FUTURE PROGRAMS (CONT)

- Advanced reactor
 - Objectives of this research are to develop models to support a more risk-informed regulatory approach to licensing of advanced reactors and to develop risk models for new and unique features of advanced reactors
 - Research will build on the advanced reactor lessons learned report and on pre-application review issues (such as the ACR-700 digital systems issues raised by the ACRS)



United States Nuclear Regulatory Commission

SCHEDULE

- UMd's research will be completed in early FY06. Intermediate results will be published in FY04 and can be used as part of guidance development.
- UVa's newest application will be completed in late FY05. Intermediate results are available now and can be used as part of guidance development.
- The first products of the new research (pilot models integrated into current plant PRA's) will be ready in FY05.
- Database work will be on-going.
- Review guidance for risk informed digital reviews will be completed in FY 05.



United States Nuclear Regulatory Commission

COORDINATION AND INTERACTIONS

- The field of digital system reliability is large and work is being done in many fields other than nuclear fields
- RES efforts to stay current
 - NPIC&HMIT '04
 - IWSS
 - DOE advance reactor IC&HMI advisory group
 - CSNI and COMPSIS
 - Work with research organizations that have other industry ties, UVa, UMd, etc.
 - Professional work such as journal reviews, guest editors, etc.
- Coordination within this program and with other research in the nuclear and non-nuclear fields is critical



United States Nuclear Regulatory Commission

SUMMARY

- Both continuing and new research is planned
- Continuing and future research will investigate different aspects of risk analysis of digital systems
- Research will continually review current and evolving methods
- Research will provide tools and guidance for NRR
- Coordination within the program and with other digital system research in the nuclear and non-nuclear fields is critical