

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Wednesday, June 23, 2010

Work Order No.: NRC-311

Pages 1-189

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

1
2 DISCLAIMER

3
4
5 UNITED STATES NUCLEAR REGULATORY COMMISSION'S
6 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

7
8
9 The contents of this transcript of the
10 proceeding of the United States Nuclear Regulatory
11 Commission Advisory Committee on Reactor Safeguards,
12 as reported herein, is a record of the discussions
13 recorded at the meeting.

14
15 This transcript has not been reviewed,
16 corrected, and edited, and it may contain
17 inaccuracies.

18
19
20
21
22
23
NEAL R. GROSS

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

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

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL
SYSTEMS SUBCOMMITTEE

+ + + + +

WEDNESDAY,

JUNE 23, 2010

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear
Regulatory Commission, Two White Flint North,
Room T2B1, 11545 Rockville Pike, at 8:30 a.m., John W.
Stetkar, Chairman, presiding.

SUBCOMMITTEE MEMBERS PRESENT:

- JOHN W. STETKAR, Chairman
- SAID ABDEL-KHALIK, Member
- J. SAM ARMIJO, Member
- DENNIS C. BLEY, Member
- CHARLES H. BROWN, JR., Member

NEAL R. GROSS

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

1 SUBCOMMITTEE MEMBERS PRESENT: (cont'd)

2 MICHAEL CORRADINI, Member

3 HAROLD B. RAY, Member

4 WILLIAM J. SHACK, Member

5 JOHN D. SIEBER, Member

6

7 CONSULTANT TO THE SUBCOMMITTEE PRESENT:

8 MYRON HECHT

9

10 NRC STAFF PRESENT:

11 CHRISTINA ANTONESCU, Cognizant Staff Engineer

12 ALAN KURITZKY

13

14 ALSO PRESENT:

15 DANIEL STILLWELL (via teleconference)

16 ROB AUSTIN

17 TSONG-LUN CHU

18 MENG YUE

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

TABLE OF CONTENTS

	<u>PAGE</u>
I. Opening Remarks and Objectives	4
II. Overview of Program and Current Plans	8
III. Recap of NUREG/CR-6997	38
IV. Workshop on Philosophical Basis for Incorporating Software Failures in a PRA	70
V. Review of Quantitative Software Reliability Methods	106

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

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

(8:30 a.m.)

CHAIRMAN STETKAR: The meeting will now come to order.

This is a meeting of the Digital Instrumentation and Controls Subcommittee.

I am John Stetkar, Chairman of this meeting. ACRS members who are in attendance are: Jack Sieber, Harold Ray, Dennis Bley, Sam Armijo, Charles Brown, Bill Shack, Mike Corradini, and we may be joined by Said Abdel-Khalik and Mike Ryan. I don't know if they will be here or not.

MEMBER ARMIJO: I think Mike has gone home, so --

CHAIRMAN STETKAR: We'll see who shows up.

(Laughter.)

We have a surprising turnout.

MEMBER ARMIJO: It's nothing personal, John.

CHAIRMAN STETKAR: Consultant Mr. Myron Hecht is also attending the meeting. Christina Antonescu of the ACRS staff is the Designated Federal Official for this meeting.

The purpose of today's meeting is to receive a briefing from the staff on the current

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 status of their work on the development of methods and
2 models for the evaluation of digital instrumentation
3 and control systems in a probabilistic risk
4 assessment.

5 The primary focus of today's meeting is to
6 address the philosophical basis for the treatment of
7 software failures in a PRA and a summary of potential
8 methods and models for quantifying software failures.

9 I have also asked the staff to prepare a brief
10 summary of their work on models for digital
11 instrumentation and control hardware and the
12 integration of those models into a traditional PRA
13 framework.

14 The Subcommittee will gather information,
15 analyze relevant issues and facts, and formulate
16 proposed positions and actions, as appropriate, for
17 consideration by the full Committee. At the current
18 time, we do not anticipate a full Committee briefing
19 on these topics, although it seems in effect we nearly
20 have one today.

21 The rules for participation in today's
22 meeting have been announced as part of the notice of
23 this meeting previously published in the Federal
24 Register on May 28, 2010. We have received no written
25 comments or requests for time to make oral statements

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 from members of the public.

2 We have Mr. Daniel Stillwell, Supervisor,
3 PRA, South Texas Projects, Units 3 and 4, on the
4 bridge phone line listening to the discussions.

5 Now, also understand that we have a second
6 line open for another individual. And I don't have
7 the identity of that individual, so whoever else is on
8 the bridge line, could you just please state your name
9 and affiliation, so we know who you are for the
10 record?

11 (No response.)

12 Is there anyone else on the bridge line?

13 (No response.)

14 Bill Stillwell, are you out there?

15 MR. STILLWELL: Yes, I am.

16 CHAIRMAN STETKAR: Okay. So at least we
17 know it's on.

18 Okay. To preclude interruption of the
19 meeting, the phone line will now be placed in the
20 listen-in mode during -- for the subsequent
21 presentations and Subcommittee discussions. We will
22 open the line at the end of the meeting for possible
23 comments from the participants who are listening in.

24 A transcript of the meeting is being kept
25 and will be made available, as stated in the Federal

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Register Notice. Therefore, we request that
2 participants in this meeting use the microphones
3 located throughout the meeting room when addressing
4 the Subcommittee. The participants should first
5 clearly identify themselves, and speak with sufficient
6 clarity and volume, so that they may be readily heard.

7 This meeting was originally planned for a
8 full day, but it has been compressed to accommodate
9 another Subcommittee meeting that we have scheduled
10 for this afternoon.

11 This Subcommittee had a briefing on the
12 hardware modeling part of the project in 2009. I
13 forgot --

14 MR. KURITZKY: Actually, probably April of
15 2008.

16 CHAIRMAN STETKAR: Or April 2008. How
17 time flies.

18 (Laughter.)

19 MR. KURITZKY: Well, we also had another
20 one in August 2009, but that was a small one.

21 CHAIRMAN STETKAR: Well, anyway, since the
22 primary topic of today's meeting is the work on
23 software methods and models, I politely request that
24 the members try to apply a bit of tactful restraint
25 during the first presentation, so we are sure to have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 enough time for full discussions of the second topic.

2 That is sometimes difficult, but be forewarned that I
3 might bang the gavel.

4 We will now proceed with the meeting, and
5 I call upon Mr. Alan Kuritzky, Division of Risk
6 Analysis, Probabilistic Risk Assessment Branch, in RES
7 to provide an overview of the digital I&C PRA program
8 and their current plans.

9 Alan, it's all yours.

10 MR. KURITZKY: Thank you, Dr. Stetkar. As
11 Dr. Stetkar mentioned, my name is Alan Kuritzky with
12 the Office of Research. I am the Project Manager for
13 work being done by Brookhaven National Laboratory in
14 the area of digital I&C PRA.

15 And, as Dr. Stetkar also mentioned, we are
16 here to talk about a number of topics, particularly
17 our work in looking at means for quantifying software
18 reliability. And that is going to be the last
19 presentation of the day, or the morning meeting, so we
20 are going to try and move through the first few
21 presentations relatively quickly, to make sure we have
22 time for that final presentation.

23 Okay. My first presentation here is just
24 to give an overview of some of the activities that we
25 are partaking in this area of digital I&C PRA. There

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 has been some discussion over the past couple of years
2 as to what pieces of work we are pursuing, why we are
3 pursuing some things, not other things, and where we
4 are going with this work.

5 And so my intention with this first
6 presentation is just to kind of show the
7 interrelationship between the various activities that
8 are occurring in the Office of Research and so you can
9 see exactly where we have been, where we are, and
10 where we are going.

11 As everybody is aware, right now digital
12 I&C systems are reviewed and approved based on
13 engineering -- deterministic engineering criteria.
14 Case in point, the Oconee TELEPERM system that was
15 recently approved by the NRC was done purely on
16 deterministic engineering criteria. There was no risk
17 analysis that was part of that submittal.

18 In 1995, the Commission came out with a
19 PRA policy statement that concluded the use of PRA
20 probabilistic risk assessment in all ways possible
21 that is consistent with the state of the art. The
22 concern here in the digital I&C area is that the state
23 of the art for PRA with digital I&C systems is not
24 that well advanced at present.

25 As was discussed in previous presentations

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 where we did look at the hardware models, as well as
2 some other topics related with digital I&C PRA, there
3 are a number of gaps in the state of the art that
4 still need to be worked on, and that is -- the purpose
5 of the work under this program is to try and fill in
6 some of those gaps.

7 The objective of the activities under the
8 digital I&C PRA work are to identify, improve, modify,
9 if necessary develop, methods, tools, and guidance for
10 including digital systems into plant PRAs, as well as
11 to use risk information associated with such systems
12 to help with various risk-informed initiatives, such
13 as risk-informed tech specs or significant
14 determination process analyses or evaluations or using
15 it for Regulatory Guide 1.174-type submittals.

16 This figure -- and for people in the
17 audience who have a black and white handout, there is
18 a color version of this figure at the very back of
19 your package. The members have it right there in the
20 package, but in any case this is the main part of my
21 first presentation here. This is to kind of show the
22 various activities that we have done, what we are
23 working on right now, and where we need to go, and how
24 they relate to each other.

25 If you look at the -- let me see if I --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 in the upper left-hand section here, we have the
2 initial reliability modeling work that is shown in
3 red. Red activities are those that have already been
4 completed. That covers the work that was done over
5 the last few years by two teams looking at modeling a
6 digital feedwater control system, in one case using
7 advanced dynamic methods, and in a second case using
8 what we call traditional methods.

9 For clarity and definition, what we refer
10 to as "dynamic methods" are methods that explicitly
11 attempt to account for the dynamic interactions
12 between the system that is being modeled and the plant
13 physical processes and the timing of those
14 interactions, and so by traditional methods we are
15 essentially saying any method that doesn't actually
16 explicitly account for those dynamic interactions

17 To a large extent, we tried to also, under
18 the banner of traditional methods, use methods that
19 were more familiar with the PRA community and the
20 technical community and had been applied more
21 frequently. But the real strict definition is just
22 that those traditional methods do not explicitly
23 account for the dynamic interactions.

24 The work on the dynamic methods approach
25 was led by Ohio State University with several

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 subcontractors. That work was documented in a number
2 of NUREG reports, and I think -- I'm not sure if one
3 of the later presentations will address that, but it
4 is NUREG/CRs 6901, 6942, and 6985. It has been
5 presented in previous meetings to the Subcommittee and
6 to the full Committee.

7 The work under BNL traditional approach
8 modeling for the digital PRA control system is
9 documented in NUREG/CRs 6962 and 6997. 6997 is going
10 to be the topic of the next presentation that Dr. Chu
11 is going to present.

12 Actually, let me just take a quick moment.

13 Here with me today and giving presentations are Dr.
14 Louis Chu and Dr. Meng Yue, both from Brookhaven
15 National Laboratory. They are two of our principal
16 technical people on this project. Dr. Chu is the
17 principal investigator, and Yue is supporting him.

18 Mr. Gerardo Martinez-Guridi, who has
19 presented before this Subcommittee before, is also a
20 key member of the team but was unable to come today.
21 You will hear from Dr. Chu when he discusses the
22 NUREG/CR-6997 work as well as a workshop that was held
23 at Brookhaven last spring on the basis for modeling
24 software failures in PRA. And both Dr. Chu and Dr.
25 Yue will participate in the presentation on our work

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 on quantitative software reliability methods, which is
2 the final presentation.

3 Okay. So initial reliability modeling
4 efforts were completed. NUREGs have been produced,
5 but they only represent one step in the overall
6 process. As you can see from this figure, the
7 ultimate goal of regulatory guidance, there are still
8 a number of things that we have to go through to get
9 there.

10 The final reliability modeling will
11 certainly be influenced by what we have learned from
12 doing this initial modeling task in the proof of
13 concept studies that we performed with the digital
14 feedwater control system, but there's a lot of other
15 areas that still need to be addressed as were
16 identified in those studies. And in the middle block
17 there you see additional research that we still need
18 to get into.

19 At the top of that list is software
20 modeling, and that is the subject for today. There
21 are also a number of other areas that still have to be
22 addressed, and those have not yet -- we have not begun
23 work on those yet, but there are a number of
24 supporting areas down at the bottom of the figure --
25 failure mode identification analysis, operating

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 experience analysis, and digital system inventory and
2 classification -- which are activities under the five-
3 year digital I&C research plan.

4 And we have started -- there is some work
5 that was completed under those areas previously.
6 There is activities that are undergoing right now in
7 some of those areas, and there is work to be completed
8 that has yet to be started in those areas.

9 We also have been leveraging, to the
10 extent possible, with outside organizations. If you
11 see on the left of the figure we have memoranda of
12 understanding with EPRI and with the National
13 Aeronautics and Space Administration. Both those MOU
14 -- we have active work involved with those, with EPRI.
15 They are currently working on developing a failure
16 analysis guideline, and we have been working with them
17 as part of that effort.

18 Also, with NASA, we have been interacting
19 with them in several meetings and exchanging reports
20 and work to see -- because NASA has some of the same
21 issues that we have as far as trying to incorporate
22 software reliability in their PRA models for their
23 manned missions.

24 Later this summer there is going to be a
25 meeting where we're -- we are going to have a technical

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 interchange meeting with NASA, because the jet
2 propulsion laboratory in California has access to a
3 bit of software reliability data, or software
4 operational experience, from some of their missions,
5 and we want to try to mine that data to see what we
6 can learn about failure modes, identifying and
7 analyzing failure modes. So that is going to occur
8 later in the summer.

9 MEMBER BLEY: Alan, can you say just a
10 word about the failure analysis guidelines, just what
11 they're aimed at?

12 MR. KURITZKY: Well, that is in the very
13 initial stages right now. And Mr. Austin from EPRI is
14 here, so if you want to hear a minute or two about
15 that I am going to yield to him.

16 MR. AUSTIN: You are using your lifeline?

17 MR. KURITZKY: Yes, exactly.

18 (Laughter.)

19 MR. AUSTIN: Rob Austin, I&C Program
20 Manager, Electric Power Research Institute. This is a
21 project which we just now started. We had an initial
22 meeting, both with our project team and then a
23 separate meeting with NRC Research. The goal of the
24 project is guidelines for performing failure analysis
25 for digital-based systems. It is at this point just

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 guidelines for what would be a deterministic analysis.

2 We are not getting into risk models as
3 part of this guideline. But one of our intents is to
4 define the failure mode's effects such that it can
5 feed into a risk-based model perhaps in the future.

6 One of our initial steps we want to do,
7 actually, is to develop a taxonomy, because when we
8 talk about failure modes, mechanisms, and effects,
9 there seems to be some debate on that. One person's
10 mechanism is another's mode is another's effect. So
11 we are trying to get some definition upon that.

12 Right now it looks like our technique --
13 we want to use a combination of both top-down
14 techniques like fault tree, use those to inform and
15 design, to hopefully eliminate classes of failure from
16 more detailed consideration in there, and where we
17 have to use a more detailed method like failure modes
18 and effects on a bottom-up analysis.

19 CHAIRMAN STETKAR: Rob, does the scope of
20 that also include software, or are you focusing only
21 on the hardware part of it?

22 MR. AUSTIN: No, we are trying to include
23 software as well. Thank you.

24 MEMBER BLEY: Thank you.

25 MR. AUSTIN: Thank you.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. KURITZKY: Thank you, Rob. Okay.
2 That was a useful use of my lifeline there.

3 (Laughter.)

4 Okay. So one other thing -- I get two
5 more?

6 PARTICIPANT: You get two more.

7 MR. KURITZKY: Excellent.

8 (Laughter.)

9 One of the things that we have tried to do
10 all along the work in this project is to get extensive
11 peer review. Because it is a somewhat controversial
12 area, and there is a lot of differences of opinion on
13 a lot of the aspects in this modeling work, we have
14 tried to have everything we have done put out for an
15 extensive peer review.

16 And that means going to the national
17 laboratories, going to academia, using a lot of
18 international organizations, regulatory and support
19 organizations, to look at our work, as well as
20 industry, other government agencies like NASA. So we
21 have gone through a fairly rigorous attempt to peer
22 review everything that we have produced under this
23 project. And we will continue to do so in the
24 deliverables that we are going to discuss later in the
25 morning meeting.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Again, just to touch on some of the items
2 on the bottom of that list, the failure mode
3 identification analysis, as we just discussed, there
4 is some work being done by EPRI on that area. BNL has
5 previously done some work. They did a failure mode
6 and effects analysis for the digital feedwater control
7 system before we actually started the modeling task,
8 and that just fed into that.

9 There is work that is being done by the
10 Division of Engineering in this area and in the
11 digital I&C research plan. Task Number 3.1.5, calls
12 for some analysis of the approved platforms that exist
13 out there right now, for instance, the Common Q, the
14 TELEPERM system, the Triconex. And that work hasn't
15 actually begun yet, but that is in the plan to be
16 started hopefully sometime in the not-too-distant
17 future.

18 Under operating experience analysis,
19 again, there was a bit of work that was done
20 previously by Brookhaven. They looked at hardware and
21 software experience, both in the nuclear area and in
22 non-nuclear industries, such as aerospace and defense,
23 you know, petrochemical, telecommunications. And they
24 attempted to come up with some reliability parameters
25 for hardware.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 It is based on some -- as expected some
2 fairly varied data, and so there is limited value in
3 the use of those numbers, but it was a worthwhile
4 exercise to see what was out there.

5 Oak Ridge also has investigated the
6 various databases that exist for digital systems.
7 Their experience under that project was -- well, their
8 attempt was to come up with a unified framework for
9 failure modes and mechanisms, and they were unable to
10 accomplish that objective because of the lack of
11 sufficient data and the quality of the data that was
12 out there.

13 The data source that was probably the most
14 beneficial for them was EPIX data, but even that I
15 think over a third of the events did not have
16 information on failure modes, and it just didn't have
17 sufficient detail for them to do what they had set out
18 to do.

19 And the inventory and classification
20 arena, that is an ongoing project with Oak Ridge.
21 They are looking at the different types of systems
22 that are out there and trying to come up with a
23 structured classification and categorization scheme
24 for systems that exist --

25 MEMBER BLEY: I'm sorry. Is there an

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 effort to obtain -- or the people who design and sell
2 these systems providing data on failure modes for
3 their equipment, are they in any way involved?

4 MR. KURITZKY: That -- you know, under the
5 Digital I&C Steering Committee that was established a
6 few years back, there was a task force in Group 3,
7 which was on digital I&C PRA risk, and in some of
8 those meetings we had discussed with industry the
9 possibility of getting hold of data like that.

10 Unfortunately, most of that data is
11 proprietary, and I think the people that were
12 participating at the meetings had limited ability to,
13 you know, affect that outcome. So nothing I think
14 really transpired from that.

15 You know, one thing to keep in mind is we
16 are trying to look at a way of modeling the systems,
17 and the methods of how we can go ahead and include
18 these systems in a PRA. The responsibility for
19 actually doing the analysis will fall on the licensee,
20 whoever owns the system. Theoretically, they may have
21 access to their vendors to provide the quantification
22 values for those models.

23 So even though we don't -- they are not
24 publicly available, and we can't use them for our
25 proof of concept studies, it doesn't mean that it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 doesn't exist for use in a regulatory application.

2 However, that said, for us to approve
3 those numbers we would want to know what went into the
4 sausage. So there would have to be some way for us to
5 access that. But right now for our proof of concept
6 studies, which we want to be out publicly, so they can
7 get lots of peer review in the technical community, we
8 have to stay away from proprietary information. So
9 that has -- we haven't pursued that.

10 MEMBER BLEY: I know this doesn't help,
11 but I just put it on the table. The people who build
12 them must be collecting really useful, deep-level data
13 on what are the failure modes and working on how to
14 correct them. There ought to be some way to clean the
15 data so it can feed the industry database. I don't
16 know what that is, but go ahead.

17 MR. KURITZKY: Right. And I agree with
18 you in theory. It's just -- it's a question of
19 whether or not various companies want -- I mean, it's
20 one thing to take an industry database, nuclear
21 industry database, and scrub the name of the plant
22 off, and, therefore, have data that doesn't associate
23 with a plant. It's another thing to take the
24 telephone system and have them list all the failures
25 that they have encountered. So --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: In some sense, though,
2 the availability -- not so much the numbers per se,
3 but the level of detail at which people compile the
4 data is often useful information to help modelers
5 understand the level of detail at which you should
6 develop your models.

7 In other words, we all know from
8 experience that people in the early days developed
9 hardware models down to the level of detail of, you
10 know, open wire connectors and short-circuited
11 resistors, and, you know, things like that. And the
12 fact of the matter is people -- the data were just
13 simply not available to support that level of detail.

14 So even if you are not able to find the
15 detailed data, it would at least be useful to
16 understand the level of detail at which the vendors
17 and the industry -- I think part of the work with Oak
18 Ridge is finding some of that information from their
19 sources. But it might be useful to ask the vendors,
20 without disclosing necessarily their deep-rooted
21 secrets, at least what level of information they have.

22 MR. KURITZKY: Yes, I agree. I think
23 that --

24 CHAIRMAN STETKAR: Help the scoping of the
25 modeling, and, you know, boundary conditions if you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 will, and conceptual models.

2 MR. KURITZKY: Yes, that's a good point,
3 because the level of detail is a big issue as far as
4 how far down we need to go in these models. And the
5 data is --

6 CHAIRMAN STETKAR: There is a terrible
7 tendency of modelers to want to go down to
8 excruciatingly fine detail, and then -- you know, and
9 then discover that the information isn't available at
10 that detail to support that model. So --

11 MR. KURITZKY: And, in fact, the work that
12 Brookhaven did on the digital fuel rod control system
13 went to a relatively detailed level, because that is
14 where they actually had some --

15 CHAIRMAN STETKAR: And that's fine. I
16 mean, that's great.

17 MR. KURITZKY: Again, going back to the
18 vendors, yes, I think it's worthwhile to see what we
19 can find out from them. I think one of the problems
20 is that a lot of the different databases or, you know,
21 different companies keep their data or analysis their
22 data to different levels.

23 And even within a certain source not every
24 event is going to get analyzed to the same level. And
25 some organizations may say, "Hey, this card has

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 failed. Let's toss it and get a new one." Other ones
2 are going to do a root cause analysis. And whether or
3 not there is some organization that is tracking all of
4 that information and categorizing it, you know,
5 remains to be seen. But it's a point well taken.

6 Thank you.

7 CONSULTANT HECHT: Alan?

8 CHAIRMAN STETKAR: Make sure your
9 microphone picks you up.

10 CONSULTANT HECHT: I'm sorry. With your
11 permission, John, I would suggest that one way of
12 actually learning about the data that is being
13 collected, without necessarily having to see the data,
14 is to request copies of their database schemas and
15 their procedures for collecting data. And that might
16 be easier to get than the actual data themselves, and
17 might give you what you want.

18 Also, you mentioned about the level of
19 detail, and so do you dispose of a part or -- in its
20 disposition, or do you try to repair it? Of course,
21 what we're talking about here is software, in which
22 case we generally do try to fix it if you can.

23 So the -- they will generally have a
24 resolution of a software problem, if it's
25 reproducible. If it's not reproducible, that's also

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 important information, because that tells you that it
2 is a random failure and may need to be handled
3 differently than a fixable, deterministic type
4 failure.

5 CHAIRMAN STETKAR: Thank you. Yes, I
6 think --

7 MEMBER BLEY: I'm sorry. Before you leave
8 that area, did you try to have any of the
9 designer/vendor people involved in your expert panel?

10 I know there weren't any there.

11 MR. KURITZKY: For which -- the expert
12 panel on software reliability or --

13 MEMBER BLEY: Yes, the one that was held
14 at Brookhaven where you --

15 MR. KURITZKY: Yes, we did. We had --
16 actually, Bob Enzinna from AREVA was.

17 MEMBER BLEY: Oh, that's right. We did
18 have AREVA. That's the only one, okay, that you had
19 down. Good, thanks.

20 MR. KURITZKY: Okay. All right. So
21 anyway, that is the basic gist of the program
22 activities and how they fit together. So the going
23 away point here is that initial modeling activity --
24 oh, sorry, go ahead, Mr. Brown.

25 MEMBER BROWN: To springboard from a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 couple of the other questions on the detail to which
2 you go, it has always struck me -- okay, stand to --
3 put aside my normal perceptions of this stuff, okay?
4 Is that the ability to do the analysis or the modeling
5 that you want is subject to more than just a general
6 generic model.

7 In other words, the types of programming
8 languages -- or the programming languages used are so
9 variable, there are so many of them out there, and
10 everybody picks what they decide they want to use,
11 whether it's, you know, a C++ or a B--, or whatever
12 the program of the day, flavor of the day, is right
13 now.

14 And they embody different characteristics,
15 from friends, inheritants, global variables, different
16 types of connectors which are used within the
17 programming to do different things, because the
18 programmers like to do that. It's kind of slick.

19 And trying to assess those with a -- just
20 a generic risk model that you can then plug in seems
21 to me to be extremely complicated based on -- and it
22 is almost a catch -- every different one has to have a
23 different model that you apply.

24 Is that within the bounds of the thinking,
25 where you are all going? I mean, it's very

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 complicated if you are going to do that, because the
2 rules vary within those various programming languages.

3 Do you understand my question?

4 MR. KURITZKY: Right. Well, as of right
5 now, most of our discussion to now has been mostly on
6 the hardware modeling. What you are getting at is the
7 software modeling, which is going to be the topic of
8 the later discussion.

9 MEMBER BROWN: Okay. I thought that was
10 addressing -- some of their comments were relative to
11 software modeling.

12 MR. KURITZKY: Right. And some of that
13 was bleeding over to -- I was going to reply to Mr.
14 Hecht that the discussion on the data was more towards
15 hardware, not software right now. But when we get to
16 the software, it's going to be a totally different
17 type of paradigm than what we are discussing here for
18 the hardware modeling.

19 So, and I don't want to jump the gun, but
20 in the discussions of the various methods for trying
21 to quantify a failure probability or failure rate for
22 software -- and we will define later what we kind of
23 mean by "failure rate."

24 MEMBER BROWN: Okay. So what you're --
25 let me -- when you talk about hardware, are you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 talking about microprocessor failures or D-RAM
2 failures or EPROM failure?

3 MR. KURITZKY: Yes.

4 MEMBER BROWN: I mean, you are talking
5 about within the hardware components that make up and
6 move the software or the data around.

7 MR. KURITZKY: Yes, exactly.

8 MEMBER BROWN: Okay. I got it. Thank
9 you.

10 MR. KURITZKY: Okay. So then the final
11 thing, just to wrap up with this, is the initial
12 modeling efforts that were done, the studies that were
13 done by OSU and Brookhaven, those are just a first
14 step. We are not yet anywhere close to the final
15 guidance. There is a lot more work that has to be
16 done.

17 I think we are pretty much out of time on
18 this presentation. These other slides that come up,
19 just put down the words -- most of it we were
20 discussing on that one slide. The only thing I would
21 mention -- and you are going to hear more about some
22 of those things in the later presentations -- the only
23 thing I would leave you with is the final bottom line
24 on this slide here, number 8, which is that we fully
25 expect that we can include a digital system model in a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 PRA, and we can quantify that model.

2 The question is: how well can we do it?
3 And what that ends up -- and how much effort does it
4 take to do it? So the bottom line is, we can do it,
5 but is it worthwhile in terms of the level of
6 resources and effort that it is going to take to do
7 it, whether or not -- whether we will have enough
8 confidence in the number that our model spits out,
9 that we can use that to support a regulatory decision.

10 And that level of effort and the usability
11 of the number are the two things that we don't know,
12 we can't answer right now. That's why we're doing the
13 work. But that's really going to be the ultimate test
14 of whether or not this is something that has
15 commercial applicability.

16 MEMBER BROWN: Okay. Relative to your
17 confidence, you know, how you derive that confidence
18 in terms of a regulatory position or decision process,
19 is the aim -- and I didn't get this out of reading the
20 various papers on the philosophical basis -- is the
21 aim of this to be able to assess the risk involved
22 with digital systems, whether it's hardware, software,
23 or a combination, whatever, that allows the
24 elimination of, say, diverse backup systems?

25 In other words, if you are going to do --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you ought to be doing it for a reason, to get rid of
2 stuff that may cost money or, you know, impede the
3 plant's operating or increase maintenance or what have
4 you. Is that the goal, to be able to say, "Hey, we
5 trust these systems so well, because we have done
6 these risk analyses, that we can now eliminate the
7 need for backup analog systems"?

8 MR. KURITZKY: That's an excellent
9 question, because that gets to one of the key points
10 that we -- I would actually like to express, is that
11 ultimately going forward we are going to look at the
12 various ways of modeling and quantifying the models
13 for digital systems. The ultimate use of this is, as
14 I mentioned in the beginning, is to support -- is to
15 include these systems in a PRA and to support, where
16 we can, regulatory decisions using risk information.

17 Now, in reality, because -- or there is
18 going to be some -- there is going to be a finite
19 limit on our confidence in these numbers. And
20 different levels of sophistication of modeling may
21 give you more or less confidence in the number you
22 generate.

23 It may be that for different uses we have
24 to -- we accept different types of modeling, different
25 levels of modeling. It might be that for a simple

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 thing, like an extension of an allowed outage time for
2 a relatively benign piece of equipment at the plant, a
3 relatively simple model that we don't have -- may not
4 have the greatest confidence in the value, but it's
5 not that big a concern.

6 We say, "Okay. At least it shows us that
7 it's not a big risk outlier, and we can approve this,
8 you know, eight-hour extension." So that may be
9 something that's sufficient. For something that has
10 more safety significance, we might want a higher level
11 of sophistication and a greater confidence in the
12 value.

13 Something, as you mentioned, trying to
14 eliminate an entire layer of defense essentially from
15 the plant, quite honestly, I don't think we will ever
16 have confidence enough in these models that we can do
17 something like that. I think that -- you know, as you
18 go through the spectrum of the levels of
19 sophistication of the modeling, and how much you are
20 willing to use it for, that is not an end of the
21 spectrum that I don't -- I just don't see us getting
22 there.

23 MEMBER BROWN: Okay. So the way I read
24 your -- what you're saying, to allow us to get within
25 your timeframe here, is that fundamentally you are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 looking at, how do I use these models to improve the
2 fundamental reliability of these systems and identify
3 vulnerabilities as opposed to eliminate necessarily,
4 okay, other backup systems because of -- from the
5 diversity standpoint.

6 MR. KURITZKY: Right. Definitely, we are
7 not intending to use them to eliminate diversity. But
8 as far as improving the systems --

9 MEMBER BROWN: Well, the backup -- don't
10 talk -- forget the --

11 MR. KURITZKY: Okay. The backup system.
12 It is really -- the intent isn't really to use these
13 to improve the systems, and that may be an artifact
14 that comes out of doing the work. In any PRA, a lot
15 of times you identify things that can go back, feed
16 back, and improve things. But the real purpose is to
17 just be able to categorize or assess the risk of these
18 systems to use in various risk-informed applications.

19 So that's the main point. But it's
20 definitely not necessary to get out of the inclusion
21 of backup systems. I mean, theoretically, I mean,
22 even in areas of PRA that we are much more confident
23 in, and we don't actually use it today to get out
24 of --

25 MEMBER BROWN: Okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. KURITZKY: -- you know, requirements
2 in backup systems, really, so, I mean, that wouldn't
3 -- that's not really an end goal here.

4 MEMBER BROWN: Okay.

5 MEMBER BLEY: Alan, one -- just a comment.
6 In addition the two things you cited, I would add,
7 instead of just the numbers, a qualitative
8 understanding of the importance of -- the relative
9 importance of failure modes and different kinds of
10 systems.

11 MR. KURITZKY: Yes. Thank you, yes.

12 MEMBER BLEY: MEMBER BLEY: Because that
13 could be the -- a real --

14 MR. KURITZKY: Very valuable, right.

15 CHAIRMAN STETKAR: And I will throw my --
16 my 37 seconds here. Also, it's important to
17 understand the integrated nature of this through the
18 whole -- you know, through the whole plant model. I
19 think one of the important things we have learned of
20 doing PRA is not necessarily so much the numbers.
21 It's the understanding of the possible risk
22 contributors when you finally put the whole plant
23 model together, when you integrate the instrumentation
24 and controls, with its dependencies, with its signals,
25 with the entire rest of the plant.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So that -- again, that's a qualitative
2 understanding. It's a better confidence that indeed
3 we have an integrated complete model of the risk of
4 the facility, not just piece-parts that are somehow
5 hung together somewhere.

6 MR. KURITZKY: Right. Good point.

7 Okay. So let me just wrap up my
8 presentation, just to mention that the letter report
9 that we are currently finalizing on the quantitative
10 software reliability methods is going to be released
11 publicly some time later in the summer, and then we
12 are also going to start -- we are actually working on
13 the next phase of the work, which is selecting a
14 couple of the methods to apply in a proof of concept
15 study. And we will have a NUREG for public review on
16 that later in the year.

17 One thing where we are kind of running
18 into a little bit of trouble -- the two methods we are
19 kind of leaning towards -- and you will hear more
20 about this when Louis talks -- are the Bayesian Belief
21 Network modeling and software reliability growth
22 model.

23 Those are two methods that we are kind of
24 leaning towards in a proof of concept study, but
25 that's one thing that -- Louis will talk more about

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 those various methods, and that's one area that we are
2 very anxious to hear feedback from the Committee if
3 they have opinions as to what are the more appropriate
4 methods to pursue.

5 The actual proof of concept, the pilot
6 system that we would like to use for the proof of
7 concept study, that is actually turning out to be a
8 little bit of a stumbling block. In order to do the
9 proof of concept study robustly, we need a lot of
10 information on a system.

11 We need a lot of information about the
12 system design and operation, of course, as well as the
13 source code for the software, a lot of information on
14 the software life cycle activities. We would want
15 access to people involved in the various phases of the
16 software life cycle.

17 So there is a lot of information --
18 results, testing results, operational experience.
19 There is a lot of information that would go into that
20 proof of concept study, which a) is difficult to get,
21 period, b) because one of the goals of our study is to
22 get it reviewed in the technical community, we want
23 something that is publicly available. And,
24 unfortunately, a lot of that information, even for
25 systems that we are able to identify, is proprietary.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So we are kind of going to be left I think
2 with two choices. One is, do the study of proprietary
3 information. We'll learn from it, but we will have
4 limited information we can share publicly and with the
5 technical community.

6 A second alternative is to take -- to kind
7 of synthesize a prototype system by taking pieces and
8 parts of publicly-available information from various
9 systems and kind of kluging that together and filling
10 in the gaps with our own constructed information for a
11 proof of concept study.

12 Now, that of course has some negative
13 aspects associated with it, but for a proof of concept
14 that might be sufficient. And it may be preferable to
15 -- because that allows us to put everything out in the
16 public domain. So, anyway, that issue is one that we
17 are still wrestling with.

18 CHAIRMAN STETKAR: I really hope that
19 industry would come forth and have some creative
20 suggestions on how a real analysis of a real system
21 might be done, because every time we have tried in the
22 past to do the -- as you put it, kluge together
23 generic models, people have been, often justifiably,
24 criticized for the fact that they are not models of
25 the real world, they don't show you the real problems

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 of real models of the real world.

2 And there is obviously a lot of industry
3 interest in our ability to finally develop some type
4 of coherent methods for modeling and assessing the
5 risk from these systems. So I would just really hope
6 that industry would show some creativity and cooperate
7 and get past this issue somehow. I mean, there has to
8 be a way to solve that problem.

9 MR. KURITZKY: We'll take that --

10 CHAIRMAN STETKAR: It's as much for the
11 people in the back of the room, obviously --

12 (Laughter.)

13 -- as with the people in the front.

14 MR. KURITZKY: We appreciate the plug.

15 Okay. So basically that's -- so that
16 NUREG would hopefully come out for public review late
17 in the year, and then we would plan to come back to
18 the Subcommittee some time after that was available,
19 so we could give you an update on where we stand.

20 Okay? Now, with that, we will move on to
21 -- Dr. Chu is going to talk a little bit about the
22 previous report, the study done on the digital
23 feedwater control system with traditional methods.
24 That is documented in NUREG/CR-6997.

25 CHAIRMAN STETKAR: Now, to remind the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 other members -- and, again, so we can hopefully keep
2 on schedule -- we did have a briefing on this project
3 whenever it was. My memory is terrible these days.
4 Last August? A year ago.

5 The reason that I asked the staff to make
6 this presentation is, as with this meeting, the last
7 meeting was kind of abbreviated, and we didn't really
8 have time to hear from Brookhaven and the staff
9 regarding some of the kind of what I consider as more
10 interesting parts of this study. So this is sort of
11 closing the gap on that last meeting.

12 MR. KURITZKY: Okay.

13 MR. CHU: Thank you, Alan.

14 I am presenting, as it was pointed out,
15 that we have given a presentation on detail of our
16 study before. So this is just to -- this presentation
17 is a pretty abbreviated one, but I guess any
18 questions, you know, we will try to discuss and
19 address.

20 Alan pretty covered what is on this slide
21 in Alan's presentation, so I am not going to say too
22 much.

23 In the past, our study is considered the
24 traditional -- using traditional method, while the
25 study led by Ohio State is considered the dynamic

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 methods. They were all applied to a digital feedwater
2 control system.

3 I guess one thing a little bit new, in
4 addition that we did, was the first sub-bullet. We
5 identified desirable characteristics for reliability
6 models of digital systems. This characteristic can be
7 used to evaluate methods or models of digital systems,
8 for input to the staff for the staff's consideration
9 in developing the staff guidance.

10 The key finding of our study -- our study
11 is called traditional. In fact, it is not that
12 traditional. As it has been pointed out in the past
13 ACRS meeting, the basic thing is use of a simulation
14 tool to propagate failures.

15 Our model is detailed enough to capture
16 many of the digital design features. While it is not
17 too complicated to solve, we managed to get it done,
18 and the method is a general one. In that sense, it
19 can be applied to any digital system.

20 The use of simulation tool is an important
21 part of our model development. Later I have two
22 slides that elaborate on this more.

23 Our use of -- our simulation tool is not
24 different from the -- what the simulation, the dynamic
25 people do. Our simulation tool is mainly simulation,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the execution of the software itself. Use of the
2 simulation tool makes Markov method or fault tree
3 method just tools for quantification. The basic model
4 is kind of more in the simulation tool than in the
5 quantification tool, like the Markov model.

6 In performing our analysis, we have
7 identified two scenarios that were not recognized in
8 the plant hazard analysis. One has to do with
9 detailed timing of the events. The other one related
10 to both the redundant CPUs entered -- both entered
11 tracking mode, meaning not including control.
12 Therefore, you lose control of the feedwater system.

13 We stumbled upon these potential design
14 questions when we were doing this FMEA. In addition,
15 in our analysis, since our model is pretty detailed we
16 were able to evaluate the benefit or importance or
17 certain design features like use of the -- having the
18 redundancy, like the ability to detect all the range
19 or deviations, and the benefit of the watchdog timers.

20 So we were able to use our model to evaluate the
21 benefit of these digital design features.

22 CHAIRMAN STETKAR: Louis, I don't remember
23 those two features that you discovered. Did they come
24 out of the qualitative failure modes and effects
25 analysis? Or were they only revealed through the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 simulation?

2 MR. CHU: They were -- the first one, the
3 timing issue, were discovered when we were doing the
4 manual FMEA that is looking at individual failure and
5 see how it affects the system. It is just based on
6 our understanding, looking at the documentation, and
7 we feel the behavior is not what the plant's hazard
8 analysis says.

9 The second case happens during what is
10 discovered during the simulation, because it involves
11 more than one failures. We were doing them -- FMEA
12 manually for individual failures.

13 CHAIRMAN STETKAR: Standard single --

14 MR. CHU: Yes. When it comes to
15 combination higher order of sequences, then you cannot
16 do every one manually.

17 CHAIRMAN STETKAR: Okay. Thanks.

18 MR. CHU: In doing our analysis, we
19 recognized that the order in which failure occurs can
20 affect the impact that is -- you have failure A and B.

21 If A occurs after B, you may have system failure.
22 When you reverse the order in which they occur, it may
23 not cause a system failure.

24 In the Markov model, you model things in
25 terms of transitions. Therefore, the order in which

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 -- and timing in which a sequence of events occurs can
2 easily be accounted for, so it's a natural tool for
3 the quantification.

4 There are certain modeling limitations
5 that Alan already pointed out. One is weakness in --
6 weaknesses in the data, and also lack of software
7 quantification -- backup quantification or software
8 failure. That is, our model essentially is a model of
9 hardware failure, but we did put in some software,
10 generic software failure mode, in our model. But we
11 don't have a good quantification, so we call them
12 placeholders.

13 So, in general, we can also put some
14 generic hardware -- software failure into our remodel,
15 but you can consider that certainly is a weakness of
16 our model. We don't have software failure rate in the
17 model, don't have it quantified. And as I mentioned
18 earlier before, the method is a general method, so we
19 believe it can be applied to protection systems, such
20 as the reactor protection system.

21 Next two slides talk a little bit more
22 about the automated tool. It is a tool based on the
23 software of the modules. That is, this system
24 consists of six modules with six microprocessors, and
25 we essentially take the source code from the modules

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and link them together, because the simulation is done
2 on a desktop computer, but the real thing has three
3 microprocessors running at the same time.

4 So we took the source code from them, we
5 put in interface software, connecting input to output.

6 You have output from one processor that becomes input
7 to the other processor, and then we put in means of
8 injecting component failures.

9 The effect of the component failure is in
10 terms of the signals that the system posits, so we can
11 automate the process of injecting component failures
12 in different orders, and also put in certain rules in
13 the software to determine if a system has failed.

14 For example, we define "system failure" as
15 loss of automatic control of the system. If the
16 device controller somehow switched to the manual mode,
17 that means the output signal from this controller will
18 stay constant, and the operator will have to take
19 manual control. We consider this as a system failure,
20 so there are other rules on how -- detecting system
21 failure using this new tool.

22 And by developing the tool, it will allow
23 us to have a pretty realistic representation of the
24 software. In the past, we have been encouraged to,
25 you know, try to model software.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Well, I was using the simulation tool. It
2 is a very realistic way of modeling the normal
3 behavior of the software. But when it comes to
4 failure of the software, the way we have it is we put
5 in some placeholders in the model.

6 One thing that Alan pointed out before
7 that we don't have is we don't -- and like the dynamic
8 modeling people, we don't have -- we don't model the
9 physical process associated with the feedwater control
10 system. And we have some discussion in our report
11 looking at this weakness. We feel that a drifting
12 signal may be a situation that a model of a physical
13 process can possibly help.

14 That is, in our model we assume the
15 drifting signal will either fail high or fail low,
16 such that it will be detected. Once it is detected,
17 it will be processed by the software. In reality, the
18 drifting signal may not reach the subpoint of being
19 high, too high or too low. And if you feed that
20 signal to the feedwater system, and you have a
21 physical model, you can determine the effect of the
22 drifting signal.

23 In that sense, a physical model may help,
24 but if you do have a physical model you can determine
25 certain drifting signal will cause system failure.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 That common failure mode can be put in our model,
2 then. You can look at the thermal hydraulic analysis
3 as a supporting analysis of our work, and you can put
4 in that common failure mode and then we don't miss
5 anything.

6 I already mentioned the -- we create rules
7 to detect failures in the simulation, to detect system
8 failure in the simulation tool, so that the process of
9 identifying failure sequences can be automated.

10 The bottom part of this slide shows the
11 number of individual failures. There is a total of
12 421 individual failure modes. It is at this level
13 that we also did FMEA manually.

14 CHAIRMAN STETKAR: I'm sorry. Taxonomy is
15 important. When you say 400 individual failure modes,
16 you mean 400 individual failures that caused the loss
17 of feedwater, which is actually the failure mode.

18 MR. CHU: No. It's --

19 CHAIRMAN STETKAR: Failure mode?

20 MR. CHU: -- 421 component failures. Out
21 of them only 100-and-some caused system failures.

22 MR. KURITZKY: Just to clarify, Dr.
23 Stetkar, failure mode there, because the components
24 can have more than one failure mode, so we have to --
25 instead of saying 421 individual component failures,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 it should have been component failure modes.

2 MR. CHU: Okay.

3 MR. KURITZKY: Because it's a different
4 bearing mode -- failure mode of the component. Like,
5 for instance, a component like an analog-digital
6 converter. It could fail high, it could fail low. We
7 have all bits fail to zero, one bit fails to zero.
8 There is various different what we call failure modes
9 at the component level.

10 MEMBER BROWN: They don't all result in
11 loss of automatic control necessarily, though.

12 MR. KURITZKY: Right. Just -- in the
13 whole model we had --

14 MEMBER BROWN: They may drift of where you
15 want, but it doesn't crash.

16 MR. KURITZKY: Again, as Dr. Chu
17 mentioned, we defined rules for what would qualify as
18 failure of the system, so there was 421 individual
19 component failure modes that by our, you know, defined
20 rules would result in loss of automatic control.

21 MEMBER BROWN: Oh, okay.

22 MR. CHU: Only 100 -- out of 421, only
23 100-and-some actually caused loss of automatic
24 control. So --

25 MEMBER BROWN: That is not what he just

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 said. I thought you said 421 actually resulted in a
2 loss of control.

3 MR. CHU: Okay. This is --

4 MR. KURITZKY: Oh, I'm sorry. I'm
5 thinking of a different side. That 111 -- yes, that's
6 what -- I was wondering why your numbers are higher.

7 (Laughter.)

8 There is another slide we have that lists
9 only the ones that caused system failure. This I
10 guess is just all the total number.

11 MEMBER BROWN: That's why I asked the
12 question.

13 MR. KURITZKY: Yes. I'm sorry, yes. It
14 was 111 or so that was actual caused failure, and
15 40,000 or so doubles that caused failure, and about 11
16 million or 12 million triples that caused actual
17 system failure. I'm sorry.

18 MR. CHU: Right. These -- what's on this
19 slide are the number of sequences of failures that we
20 simulated. Some of them cause system failure; some
21 don't. And after we evaluated the triple failure
22 sequences, we found that the system failure
23 probability has pretty much converged. Therefore,
24 that's where we stop. And it took quite some time to
25 simulate the sequences, though.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CONSULTANT HECHT: And this was only for
2 the hardware failures and you say those components,
3 correct, or --

4 MR. CHU: Correct. Yes. We put in some
5 generic software failure mode as a placeholder, and we
6 can, you know, generally sequence this in software
7 failure, too. But we don't have a good quantification
8 of the software failure.

9 MEMBER BLEY: Just to clarify and see if
10 this helps, these are failure modes of cards or
11 whatever in the system.

12 MR. KURITZKY: Components.

13 MEMBER BLEY: But they could have failed
14 because of -- software could cause these failure
15 modes, yes? Some of them.

16 MR. KURITZKY: I mean, again, that goes to
17 how you are going to define the software, whether it's
18 essentially embedded in the hardware or the component
19 failure or whether it's something that's treated
20 separately. In our model, we have separate
21 placeholder events for software failure. So these
22 actually represent essentially hardware failures.

23 MEMBER BLEY: But when you said their --

24 MR. KURITZKY: This is --

25 MEMBER BLEY: -- is high, there could be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 then a separate software failure mode that gives you
2 the same functional effect.

3 MR. KURITZKY: Exactly. Exactly.

4 MEMBER BLEY: Okay.

5 MR. KURITZKY: But --

6 CHAIRMAN STETKAR: These are simply output
7 states from pieces of hardware, correct?

8 MR. KURITZKY: Right.

9 MEMBER BLEY: Defined as hardware
10 failures.

11 CHAIRMAN STETKAR: Defined as a --

12 MEMBER BLEY: But the same output failure
13 could be caused by software.

14 MR. KURITZKY: Yes.

15 CHAIRMAN STETKAR: Okay.

16 CONSULTANT HECHT: I'm not quite sure I
17 understand. Are the software failure modes done at
18 the task level?

19 MR. CHU: We have put in some software
20 failure modes. Say they are -- there is a main CPU,
21 there is a backup CPU. They both run the same control
22 software, and we put in software -- one failure mode,
23 it could be Software House.

24 CONSULTANT HECHT: Yes, that's a classic
25 one.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. CHU: In that case, since they run
2 identical software, we assume that same failure mode
3 will affect both of them. Effectively, the failure
4 mode will cause a system failure.

5 CONSULTANT HECHT: So of the software
6 running on the controller, what is considered as a
7 monolith, you didn't separate it, for example, into an
8 operating system kernel and a data acquisition task
9 and a data processing task and --

10 CHAIRMAN STETKAR: Myron, this is not
11 addressing software, so don't --

12 CONSULTANT HECHT: Okay.

13 CHAIRMAN STETKAR: -- let's -- I'm going
14 to cut that off. We'll talk about software later.
15 This is simply the hardware part of the problem for
16 all practical purposes.

17 CONSULTANT HECHT: Right. Got it.

18 MR. CHU: In terms of simulating the
19 timing of the occurrence of the events, we did it in a
20 -- it is an approximation of the real thing. The real
21 thing is you have six microprocessors running in
22 parallel. They exchange data at different times.

23 We put all the software and link them and
24 put them on a single desktop computer. So there is
25 some approximation involved in the timing. It is our

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 understanding that the CPU modules has a maximum
2 running time of maybe 100 milliseconds per cycle, and
3 the controller software has a maximum of I think 50
4 milliseconds.

5 Therefore, the way we simulate the
6 execution is that we -- every time we run the main --
7 the CPU software we run the controller software twice.

8 We run the CPU software once and the controller
9 software twice, and they exchange information.

10 In that sense, we approximately simulate
11 the execution of the real system, and I think we
12 account for the order -- we can account for the order
13 in which failure occurs correctly. But when they
14 argue that if the two failures occur before the
15 signals stabilize, that is within the execution cycle
16 of a processor, then our model may not correctly
17 represent the real system. But we can argue, you
18 know, the likelihood of that happening is very, very
19 small.

20 Here I -- the second part of the slide
21 gives an example of the importance of the order in
22 which the failure occurs. Think of the main CPU. It
23 has a failure mode that can be -- that cannot be
24 detected. Then, the main CPU, this failure mode, will
25 directly cause system failure.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Well, another failure mode of the main CPU
2 can be detected. In that case, when the failure is
3 detected, it switches to the backup CPU, and the
4 backup CPU takes control and everything is fine.

5 MEMBER BROWN: So that's what you mean by
6 -- excuse me, by automatic reconfiguration is the
7 shifting from a primary --

8 MR. CHU: Right.

9 MEMBER BROWN: -- to a backup controller,
10 running the same program, getting the same data, and
11 each capable of providing that automatic control.

12 MR. CHU: Right.

13 MEMBER BROWN: Okay. It's not a software
14 -- they are not redoing software when you are looking
15 at this. We are still in the hardware realm.

16 MR. CHU: So in this example, if the
17 detectable failure occurred first, and it switches to
18 the backup CPU, then any additional main CPU failure
19 will not have any effect on the system, because it is
20 no longer in control. So, in that sense, the order in
21 which the failure occurs makes a difference.

22 As part of our work, we identified some
23 areas of additional research. It includes improved
24 approach for defining and identifying failure mode of
25 digital system. Essentially, it is a question of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 completeness of the failure mode.

2 MR. KURITZKY: And just to point -- that
3 is under -- the figure I showed before under
4 Task 3.1.5 of the five-year research plan, there is
5 work that is scheduled that is supposed to delve into
6 that area.

7 MR. CHU: The second bullet is on method
8 for quantifying software failure rate and failure
9 probability. That is an ongoing project that we are
10 working on. Alan already talked about it -- plan to
11 apply some methods to a case study.

12 Third bullet, better data for hardware
13 failures. In our study, we have been criticized that
14 the data that we obtained has very large uncertainty,
15 and it is not good enough to be used in supporting
16 decisionmaking. So data is always an issue.

17 Earlier there was some discussions on
18 finding other sources of data. The critical thing is
19 how to get the owner of data to supply it -- the fact
20 that failure data usually is sensitive.

21 MR. KURITZKY: But, again, I would point
22 out that for our proof of concept study we don't
23 actually need very accurate data to demonstrate the
24 methods. For regulatory application, we would need to
25 have that data. So, again, if a vendor or somebody

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 has that data and is willing to share it with the
2 reviewer, then that problem might go away. But I have
3 a feeling that data is always going to be an issue.

4 MR. CHU: Modeling of digital design
5 features, we feel we have a pretty detailed model, and
6 we are capturing the detail of the digital feedwater
7 control system design features pretty well. Of
8 course, the feedwater control system doesn't have all
9 the features -- all the features of digital systems.
10 Therefore, there are other features that, you know,
11 modeling of other features need to be looked into.

12 Others that are related -- human
13 reliability analysis associated with digital systems,
14 the fact that new reactors will have a totally
15 integrated digital control room.

16 Last bullet was on determining if dynamic
17 methods is necessary in developing a reliability model
18 of a digital system. In case of control system, it
19 has a control loop. Therefore, it interacts with the
20 plant process all the time. In that sense, the
21 physical model of the plant -- modeling physical
22 process may be useful, but when it comes to protection
23 system it has no control loop. Therefore, probably
24 it's not that necessary to do -- to develop an
25 integrated physical process model with reliability

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 model.

2 Integration of a model -- or the feedwater
3 control system model with a PRA -- since we used
4 Markov model, we defined failures in terms of
5 sequences of failure. That is, the order in which
6 failure occurs makes a difference.

7 Therefore, the quantification of the
8 sequences is not the same as that of a typical fault
9 tree cutset quantification. Therefore, integrating
10 our sequence -- our sequences with PRA model poses
11 some difficulty. But I would say in -- we can
12 represent the sequences that we have in terms of
13 cutsets.

14 The purpose you want to -- the reason you
15 want to integrate is that you want to account for
16 sharing of components. In this case, the components
17 in there are shared. Could be sensors, could be
18 support systems.

19 These are, you know, failure events in our
20 sequences. You represent the sequences in terms of
21 cutsets, and then these cutsets can be linked with the
22 cutsets, with the rest of the PRA model. Then, you
23 can account for the quantification, account for the
24 sharing.

25 After that, you can look at the resulting

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 cutset and see how you can quantify it. Knowing, you
2 know, how the failure occurs, quantification can be
3 done.

4 In our work, we didn't quite discuss
5 integration or try to integrate. But in the dynamic
6 methods study, they do have a specific chapter talking
7 about integration. I don't know the detail of what
8 they discussed, but I think the approach has got to be
9 similar to what I just described. You represent your
10 sequences in terms of cutsets, and you link cutsets to
11 account for sharing.

12 This is the end of the presentation on
13 this subject.

14 CHAIRMAN STETKAR: Okay. And the good
15 thing is we are a bit ahead of time, but I am going to
16 try to torpedo that.

17 I think this is a good presentation. The
18 NUREG has a lot of really interesting work in it. I
19 am left kind of hanging in some sense saying, "Where
20 do we go from here?" And I'm a bit concerned, because
21 everything that I hear is we need to do more and more
22 and more and more detailed simulation and simulation.

23 Is there any effort to step back from this
24 whole effort and say, "What did we learn from this
25 effort? And did we learn that maybe we don't need to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 do this?" For example, what -- from a modeler's
2 perspective, in practical terms, what is the practical
3 value added by doing the simulation? For example, I
4 know you did a qualitative failure modes and effects
5 analysis. I don't know the resources required for
6 that, nor do I know the resources required for the
7 simulation model.

8 If by performing this exercise we have
9 learned that by doing the simulation we have added two
10 percent value for three times the cost, it is probably
11 not necessarily worthwhile to do that. I mean, in
12 principle, it would be wonderful for a plain old
13 normal Rube Goldberg hydraulic turbine control system
14 to go in and try to simulate the heck out of
15 everything that could possibly go wrong with that. We
16 don't do that, because we have learned that we have
17 sufficient data to -- at a certain level to understand
18 how frequently turbines trip, how frequently they
19 might overspeed, and things like that.

20 So my real question is, going forward now,
21 having done this exercise, I think I'd caution a
22 little bit about too much emphasis on more and more
23 detail and more and more simulation without stepping
24 back and saying, "What's the real purpose of this?"
25 The real purpose is to try to develop something that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 is addressed on the two last bullets as not having
2 been done, which is how you integrate a practical
3 model of a digital I&C system into a real-world PRA.

4 So that is just kind of a caution. And I
5 would -- Alan, is --

6 MR. KURITZKY: Yes, I want to --

7 CHAIRMAN STETKAR: You mentioned peer
8 reviews, and I was wondering whether part of the peer
9 review process is getting --

10 MR. KURITZKY: We haven't seen --

11 CHAIRMAN STETKAR: -- input from people --

12 MR. KURITZKY: Well, I don't think -- in
13 our peer review comments, I can't remember all of them
14 in detail from that study, but I -- but just to
15 directly address what you're talking about, yes, we
16 agree. And we have taken time to look back and say,
17 "Here, we've done this study. We have spent a lot of
18 money and a lot of effort." And even there we still
19 have many gaps that aren't filled.

20 So that's why I said this before, by the
21 time we're all said and done, we will have spent many
22 years and many millions of dollars, which may be fine
23 as a research, as a government funded research study,
24 but whether that is something -- and I use the word
25 "commercially applicable." I mean, is it something

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that can then be -- you know, are the masses going to
2 use it and implement it? Are the utilities all going
3 to do this for every digital system in their plant?

4 Okay. If it something that costs multi-
5 years and multi-million dollars, at PRA -- current PRA
6 isn't necessarily taking all of that level of effort.

7 So to do that for one system --

8 CHAIRMAN STETKAR: Any reasonably simple
9 system, by the way.

10 MR. KURITZKY: Right, right. Isn't going
11 to make any sense. So you go to -- so your first
12 question was, do we need to go to this level of
13 simulation? And, if so, what are we getting from it?

14 Well, I would say that at the level of
15 detail that we did the model, we felt that we had to
16 go to a certain level of detail, both to represent the
17 various features of the system, but also primarily
18 because that's where we had data. And so that is kind
19 of like -- the data available drove us to that level
20 of detail, and at that level of detail you needed to
21 have a simulation tool in order to just be able to
22 handle all of the various combinations.

23 Okay. If we could do it at a higher level
24 -- and, believe me, I would love to do that -- being a
25 PRA guy, boy, would I love to do that at a higher

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 level. And that may be somewhere in the future we may
2 have to go there. It goes back to the statement when
3 I was talking to Mr. Brown about, what are we going to
4 use this for?

5 And if it's some smaller -- I call it
6 "smaller," but some less risk-significant use maybe,
7 we can get by with a cruder model or less -- you know,
8 a coarser model, and in which case we may not need
9 that level of detail and that simulation.

10 The problem is, how do we ultimately
11 quantify whenever it is we're going to stick in the
12 PRA model. And that's where we have -- that's where
13 we run into the problem, because at that higher level
14 there is no data at that level, at least not that
15 we're aware of, and so we're forced to do some kind of
16 expert elicitation. Well, even at the lower level we
17 are going to find out that we are going to need -- for
18 software we are probably going to have to do -- expert
19 elicitation is going to have to pop up at some place
20 anyway, just because of lack of data.

21 So if we are going to do expert
22 elicitation at that level, can we do it at just a
23 higher level for the system or a function of the
24 system and be done with all of that other detail?

25 MEMBER BLEY: Alan, can I turn John's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 question around just a little?

2 MR. KURITZKY: Sure.

3 MEMBER BLEY: Have you learned anything
4 from the detailed simulation that will let you use
5 those results to build a simpler model and do
6 something from those results or using maybe a larger
7 simulation one time to generate data that you could
8 use in a simpler model? Have you chased that, or have
9 any of your reviewers helped you chase that?

10 MR. KURITZKY: We haven't -- none of the
11 reviewers have brought that up. And, actually, the
12 report itself I think in one of the list of findings
13 or conclusions or something, I think we identify that
14 as one of the things.

15 Now, we go through this thing, one thing
16 to consider would be: are there ways that we can
17 simplify this going forward? You know, doing things
18 -- going through the details one time to understand
19 what are the drivers -- and this is a hypothetical.
20 Maybe we identify, these are the main concerns. Can
21 we just have a model limited to those concerns and
22 ignore the rest of the detail because it doesn't
23 really make much difference and make the whole problem
24 much simpler?

25 That is one thing that it would be nice to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 be able to do. We just identified that that's
2 something that probably should be done. We have not
3 pursued that yet. It was nothing that was obvious to
4 us and something that said, "Oh, wow, that -- we can
5 just get rid of that and just focus right here, and
6 this will be a much easier problem to tackle."

7 We didn't have any "ah ha" moment like
8 that, but that is something that, you know, once we go
9 through the first exercise --

10 MEMBER BLEY: Yes. But were you asking
11 the question? I mean, is that --

12 MR. KURITZKY: Yes. Sometimes it pops
13 out, but sometimes, if you're looking for it --

14 CHAIRMAN STETKAR: We can find it.

15 MR. KURITZKY: Well, that's definitely --
16 look, everybody invests in PRA, it has been about --
17 it has been in their minds, because there is no one
18 that I know of who does a PRA that wants to do this in
19 their PRA. No offense.

20 (Laughter.)

21 MEMBER BROWN: Alan, that was -- to
22 springboard on that, it was reflected several times
23 throughout the reports, it was mentioned that a
24 conservative approach to this would be to assume a
25 failure of 1.0, a probability of --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: Probability for a
2 common cause failure.

3 MEMBER BROWN: Whatever. It was mentioned
4 several places.

5 CHAIRMAN STETKAR: That's a different
6 issue, though.

7 MEMBER BROWN: Well, but, I mean, it talks
8 about -- you talk about simplicity. That makes it
9 simple. If something is 1.0, it makes it simple.
10 That's a very high-level simplicity, but you've -- at
11 least it was recognized.

12 MR. KURITZKY: As a design aid, there may
13 be some value to that, and that will leave you to have
14 one of those backup systems. But as far as trying to
15 represent the risk at the plant and identify what are
16 the contributors to the risk profile of the plant,
17 that would mask the --

18 MEMBER BROWN: That would not work.

19 MR. KURITZKY: Right.

20 CHAIRMAN STETKAR: I think, Alan, to just
21 kind of close up here, you might want to think --
22 having been through things like this, not in the
23 digital world, but the non-digital world, you are
24 absolutely right. I mean, this type of exercise seems
25 to be a necessary evil of evolution of understanding

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 how to model things.

2 There is, as you are well aware, the
3 danger that the people who are deeply involved in a
4 particular project know so much about the details.
5 Even though you might be sensitive to the fact that
6 you need to step back and think about simplifying or
7 creatively packaging some of that information, it is
8 really difficult to do that when you have lived with a
9 project very, very closely for, you know, many -- how
10 many -- a couple of years, for example, or more.

11 So it might be useful -- and the problem
12 is if you have reviewers or a peer review team that
13 you ask, and you gather those reviewers based on their
14 expertise and modeling and digital systems, and you
15 ask them to review your study, they tend to also focus
16 on the detailed elements of your study without
17 stepping back.

18 So it might be useful to bring together a
19 group of marginally knowledgeable, disinterested
20 folks, who have some PRA expertise, and kind of ask
21 them their opinions. And when I say "marginally
22 knowledgeable," that's -- you know, I'm trying to get
23 across a message here that haven't been so deeply
24 involved in this -- these particular types of
25 activities that they are married to a particular

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 approach, and see what their insights -- I mean, they
2 might not have an "ah ha" moment, but they might have
3 some different ways of looking at the problem that
4 folks so deeply involved haven't seen before.

5 MR. KURITZKY: Yes, I totally agree with
6 you. In fact, I actually talked with -- I informally
7 gathered a few of the senior-level PRA advisors and
8 digital advisors at the NRC to try and talk over
9 whether there are some alternative simpler approaches
10 that we could go about pursuing in parallel to doing
11 this work, because we need to go through the evil
12 exercise, but we -- but in parallel, try to see
13 whether there is something that would be more useful
14 in a production mode.

15 CHAIRMAN STETKAR: I think that's
16 important, because, you know, as you said, it is --
17 ultimately, this project needs to have some practical
18 benefit to folks who are out there looking for, you
19 know, real guidance, and, you know, agreement between
20 the NRC and the industry in terms of things like level
21 of detail, general modeling methodology, and things
22 like that. So --

23 MR. KURITZKY: Yes, I agree. And
24 that's --

25 CHAIRMAN STETKAR: And we need to get that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 -- I mean, also the message is we kind of need to get
2 there, you know, before you retire.

3 (Laughter.)

4 MEMBER RAY: Isn't that the role of the
5 industry, though, to simplify and -- it would seem
6 like the regulatory function needs to be able to say,
7 "Yes, that's the right answer based on a more
8 detailed" --

9 CHAIRMAN STETKAR: You know, the industry
10 apparently has some efforts, and I'm not going to
11 speak -- we have a representative from EPRI here who
12 might want to say -- this is one of those areas
13 similar to things like the fire risk assessment that
14 the NRC has stepped up to take the lead, and there
15 hasn't been as detailed --

16 MEMBER BLEY: Just to your point,
17 Harold --

18 CHAIRMAN STETKAR: -- industry
19 involvement, a --

20 MEMBER BLEY: Evolving out of this into a
21 simpler method based on this is this method is
22 research, though.

23 CHAIRMAN STETKAR: Yes.

24 MEMBER BLEY: It is not -- it is not a
25 regulatory function or some other. It is, can we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 devise a method for analysis that is both practical
2 and meaningful? And so I see that as a very
3 reasonable thing for Research to --

4 CHAIRMAN STETKAR: You know, and I think
5 our Committee has recommended that industry, you know,
6 through collaborative agreements get involved with
7 this process. And I think that is really, really
8 important as the methods development phase evolves
9 into things like a -- you know, a pilot application,
10 something that Alan was talking about.

11 MEMBER RAY: Well, you're -- I'm not
12 trying to intrude in that --

13 CHAIRMAN STETKAR: Because that's what --

14 MEMBER RAY: It is research, but it's the
15 research on the part -- on behalf of the regulatory
16 agency, not the government doing it for industry. And
17 the result ought to be to validate what the industry
18 does, and it would just seem to me like instinctively
19 that would offer more detail than would be used by the
20 industry in doing what they do. It's a simple
21 paradigm.

22 MR. KURITZKY: And I think just to -- you
23 know, we have actually a memorandum of understanding
24 with EPRI, both in the PRA area, which calls digital
25 I&C as its subtask, and in digital I&C, which has PRA

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 called as a subtask. So the infrastructure is there
2 to try and collaborate more broadly with industry in
3 that area. Up to now, we haven't done a lot --
4 haven't really pursued that a lot.

5 It has been focused on something -- you
6 know, Rob Austin talked to you about the failure
7 analysis guidelines and some of the other work that
8 they are doing, but -- so we haven't really pursued
9 the PRA one as aggressively as maybe we need to going
10 forward.

11 CHAIRMAN STETKAR: Because there is -- I
12 mean, as Harold -- there is expertise out there. The
13 people have -- industry have been modeling, to a
14 greater or lesser extent, digital systems.

15 MR. KURITZKY: Right.

16 CHAIRMAN STETKAR: And there are -- there
17 is an evolving, you know, level of knowledge out there
18 and level of expertise that it may be time to --

19 MR. KURITZKY: To tap into.

20 CHAIRMAN STETKAR: -- to tap into.

21 MR. KURITZKY: The only difference is that
22 there is going to be a different -- there is a
23 different opinion between those camps as to what is an
24 appropriate or acceptable level or --

25 CHAIRMAN STETKAR: You know, and that's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 why -- that's why it would be good to get together,
2 isn't it?

3 MR. KURITZKY: Right.

4 CHAIRMAN STETKAR: Rob Austin?

5 MR. AUSTIN: Rob Austin, Electric Power
6 Research Institute. To also clarify, on our failure
7 analysis, what we have done for risk and probabilistic
8 methods for digital I&C is we're kind of hanging back
9 on those until we can move further ahead with the
10 deterministic failure analysis.

11 One of the things we have seen as we do
12 these, like I mentioned before, is that you -- I think
13 we need to have agreement. We want to work with staff
14 on this -- to have agreement on our taxonomy, our
15 definitions, and then the basic failures of what we
16 are trying to quantify before we can actually quantify
17 it.

18 And that has been a fairly consistent
19 comment from ACRS and staff on when we have done --
20 presented some of our risk work before is that, if we
21 don't have agreement on some of these foundational
22 areas, that is where we are focused right now, but
23 definitely welcome -- this is very interesting work
24 actually on the NUREG. I would just also -- not only
25 the contents of it, but a lot of the background

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 material in it that you guys had was really nice and
2 appreciated. So, and we are -- welcome the peer
3 reviews and work with you on this moving forward. So
4 --

5 MR. KURITZKY: And, in fact, to clarify,
6 we -- I mean, EPRI has been involved in peer reviewing
7 those documents. Ken Canavan in particular has been
8 involved, and other people have met with him.

9 CHAIRMAN STETKAR: Good. Anything else on
10 the hardware part of it?

11 (No response.)

12 If not, I think it's time to take a break.

13 And I'm generous, we'll go until 10:10.

14 (Laughter.)

15 Be back at 10:10, please. By the way, for
16 all of those attending, if you have looked at your
17 schedule, we are going until 12:30 today, so you are
18 going to have a short lunch.

19 And with that, we will recess for a break
20 until 10:10.

21 (Whereupon, the proceedings in the foregoing matter
22 went off the record at 9:52 a.m. and went
23 back on the record at 10:09 a.m.)

24 CHAIRMAN STETKAR: We are back in session,
25 and we will come back to the staff and hear

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 presentations on the software side of the story.

2 MR. CHU: Okay. This part of the
3 presentation deals with establishing philosophical
4 basis for modeling software failures.

5 Essentially, I will start by organizing a
6 workshop of experts. Some background information, the
7 National Research Council Committee made the
8 recommendation to expressly include software failure
9 in the PRA of nuclear powerplants. And the second
10 conclusion they say, "As in other PRA computations,
11 bounded estimates for software failure probabilities
12 can be obtained by a process that includes valid
13 random testing and expert judgment."

14 The important thing is the footnote, which
15 indicates that Committee member Nancy Leveson did not
16 concur with this conclusion. You can look at it this
17 kind of as the issue. She probably can be considered
18 a representative of the people who are against
19 probability modeling of software.

20 MEMBER BROWN: Would you repeat that
21 again? I mean, I read that. That's on page 1 of the
22 -- or, actually, 2-1 of the report. And so you say
23 the general conclusion was that -- I'm covering this
24 as a summary. That it's not possible to identify all
25 -- and eliminate all faults, and you say, "Therefore,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 residual faults always exist," which seems like kind
2 of a no-brainer.

3 MR. CHU: Yes.

4 MEMBER BROWN: And then -- and Ms. Leveson
5 didn't agree with that.

6 MR. KURITZKY: No, she --

7 MEMBER BROWN: That's why I got out --

8 MR. KURITZKY: She didn't agree that you
9 can -- what we're mentioning there, since there are
10 residual faults, there is a need to consider the
11 likelihood that the software will not do -- in the
12 system it will not do what you want it to do because
13 of some software-related issue. And so we are trying
14 -- so we believe that we can model that in a
15 probabilistic manner to come up with a probability
16 that it will not work properly.

17 What Nancy Leveson has said is that she
18 does not believe that it is -- that you can model that
19 probabilistically, that the likelihood is that the
20 software will contribute to the system, not
21 accomplishing this function.

22 MEMBER BROWN: Oh, okay. I didn't read it
23 that way. Thank you.

24 MR. KURITZKY: And she represents -- and
25 what Louis is mentioning is that she is a single

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 member on that Committee, but she represents a camp, a
2 group of people who believe that you can't model it
3 probabilistically -- you know, the software
4 contribution probabilistically. So that's --

5 MEMBER BROWN: How do you become a member
6 of that camp?

7 (Laughter.)

8 CHAIRMAN STETKAR: You are in it already.

9 (Laughter.)

10 MR. CHU: There was a conference I went
11 to. It's a systems safety conference. There I asked
12 a stupid question. Someone did an analysis of a rail
13 car model. It's modeling of hardware. And at the end
14 of his presentation I asked questions, I said, "How
15 did you model a software failure?" And then,
16 everybody in the room got surprised by the question,
17 and then the session chairman looked at me and told
18 me, "Software do not fail." So that was --

19 (Laughter.)

20 So some people think it is, you know, it's
21 -- software behavior is deterministic, and then some
22 argue that it is not worthwhile trying to quantify
23 software failure rate or failure probability. You are
24 better off spending the resource trying to find the
25 bugs and fix them. So they were -- that kind of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 makes --

2 MEMBER BROWN: I understand the statement
3 about software not failing. Software tends to do what
4 you tell it to do. And if you tell it the wrong
5 thing, because you didn't understand it, then that can
6 be interpreted as either a requirements failure, which
7 did not get executed, is that a software failure, did
8 the ones and zeroes -- I mean, the only real -- I'm
9 saying this not only -- I don't want to start a fight.

10 The ones and zeroes are ones and zeroes.

11 They process through in the program step
12 mode of doing whatever is done. And whatever is in
13 that byte or multiple-byte step gets executed. That's
14 what's there.

15 So if the wrong thing is in there, is that
16 a software failure, or is that because the information
17 that told it what to be there is wrong? You can argue
18 back and forth, but I -- you know, it's --

19 MEMBER BLEY: If you read the consensus
20 statement of their panel up at Brookhaven, it
21 addresses that.

22 MEMBER BROWN: Well, no, they --

23 MEMBER BLEY: It's pretty useful.

24 MEMBER BROWN: They could identify that
25 that's true, but that it's a situational --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: Yes, I was trying to figure
2 out, when I went through this, because they discussed
3 that, is where -- where do we work the software
4 failure issue as opposed to the things that generate
5 the coding of that software?

6 MR. KURITZKY: And I think what's going to
7 happen is, as we go and discuss the various
8 approaches, that is going to get -- that is not going
9 to be distinguished per se. I mean, some of the
10 approaches do better at one type of software -- coding
11 error versus a requirements error.

12 But in general we are interested in
13 anything that results in the software, not -- in the
14 system that the software resides, not accomplishing
15 the function that we want it to, because of something
16 related to the software. And whether that is a coding
17 error, or whether that is a design or a specification
18 error, or anything else is not -- is immaterial. We
19 just want to make sure the system does what it needs
20 to do.

21 MEMBER BROWN: I don't -- I'm not
22 arguing --

23 MR. KURITZKY: So we used the phrase
24 "software failure" -- just to be clear, we used the
25 words "software failure" as kind of a --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: But it encompasses those
2 other --

3 MR. KURITZKY: Right.

4 MEMBER BROWN: You're just saying it
5 encompasses the requirements or coding errors --

6 MR. KURITZKY: Right.

7 MEMBER BROWN: -- or blah, blah, and
8 that's an approach. I don't have --

9 MR. KURITZKY: Okay.

10 MR. CHU: Thank you. The most immediate
11 reason we had this task is that the ACRS Subcommittee
12 actually made the recommendation to address the issue.
13 The way we approach it is that we organized a
14 workshop that took place in May of 2009 of experts in
15 software reliability.

16 The objective of the workshop is to obtain
17 a consensus or at least agreement among the workshop
18 participants on the philosophical basis for
19 incorporating software failure into digital systems
20 reliability models. And as part of that workshop, the
21 expert also talked about some technical issues
22 associated with modeling of software failures.

23 Before the workshop took place, we put
24 together some questionnaires. It included some
25 background discussion of the issues associated with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the software, the philosophical basis, the modeling of
2 software failure, and sent them to the participants.
3 And the participants provided a written response to
4 the questionnaire. And after the workshop, we put
5 together a summary report on this task.

6 This slide shows the experts of the
7 workshop. We have a representative from the NRC, we
8 have a representative from the industry, we have some
9 international participation also, and we have
10 participant -- participation of Allen Nikora, who
11 represents the outside contractor at JPL.

12 And then, we have a few professors who are
13 pretty well known in the area of software and
14 reliability. In addition, we also have Myron Hecht,
15 who was there as an observer. He didn't participate
16 in the discussion, but he was there observing I guess
17 for the ACRS.

18 Professor Littlewood was not able to
19 attend the meeting, but he did provide a written
20 response to the questionnaire.

21 So this is the bottom-line answer -- a
22 philosophical basis for modeling software failure
23 probabilistically. Software failure is basically a
24 deterministic process. The first sentence is kind of
25 to satisfy the people who said software failure is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 deterministic.

2 However, because of our incomplete
3 knowledge, we are not able to fully account for and
4 quantify all of the variables that define the failure
5 process. Therefore, we use probabilistic modeling to
6 describe and characterize software failure process.

7 And this description of software failure
8 or this basis is essentially the same as a basis for
9 many other probabilistic processes, such as tossing a
10 coin. We are not able to reproduce, we are not able
11 to control everything that affects the movement of a
12 coin. Therefore, it is reasonable to model a coin
13 toss using probabilities. In that sense, software
14 failure is no different.

15 At the workshop, besides establishing,
16 discussing about the philosophical basis, the experts
17 also talked about technical issues associated with
18 modeling software failure. I have some slides that
19 goes into a little more detail about the discussion on
20 those.

21 How do software failures occur? The
22 description here basically is part of the discussion
23 that took place about philosophical basis. It gives
24 some more background information about software
25 failure. Software can fail because they provide a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 service, and software -- the service may not be
2 delivered correctly, or the software may perform an
3 undesired action. So RPS can fail to trip, RPS can
4 trip spuriously.

5 This can be considered as failure of
6 software, or you can -- you can consider this as a
7 high-level definition of software failure.

8 Faults are introduced during the software
9 life cycle, and it is not possible to remove all the
10 faults for -- except for maybe some non-trivial
11 software. Therefore, there is also some residual
12 fault in the software.

13 During the operation of the software, if
14 some input occurs, which interacts with the internal
15 state of digital system, can trigger a fault in the
16 software. This is how a software failure occurs. So
17 this is some background information supporting the
18 philosophical basis for modeling software.

19 This slide gives a summary of the
20 discussion on how do we include software in the
21 reliability model of a digital system. Most experts
22 agree that software failures can be modeled
23 separately. Hardware and software failure can be
24 modeled separately in the same reliability model.
25 They assure us that the tendencies among these

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 failures are appropriately accounted for.

2 And the majority of the participants
3 believe that generic failure modes of software can be
4 used in a reliability model to model software failure,
5 and they actually provide -- come up with some generic
6 software failure modes.

7 MEMBER BROWN: Can I ask a question? Can
8 you go back to the previous bullet on dependencies?
9 I'm trying to understand what you meant by that. I
10 can envision a hardware dependency. In other words,
11 you could have a failure of a memory unit where a
12 memory bit fails. And all of a sudden it used to be a
13 one, now it's a zero. Whatever it is, you can see
14 that. Therefore, the software gets affected, because
15 it is now getting incorrect information.

16 So that's a dependency from hardware to
17 software I could see, but I couldn't envision a
18 software to hardware dependency. So that -- and I --
19 is there an example of one?

20 MR. CHU: I think the dependency is in
21 general -- an example could be, say if you have a
22 microprocessor, it runs the software. So in your --
23 in the development of the model, if the hardware has
24 already failed, you cannot expect the software to
25 perform its function.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: That part I got. The
2 hardware dependency can affect the processing of the
3 software. In other words, the bits and bytes, the
4 fundamental program that is embedded, how did that --
5 if the program gets corrupted, that won't necessarily
6 make the hardware fail. You will just get an
7 incorrect result. You may not trip. You may --
8 that's not a hardware failure. That's not a
9 dependency. It's an incorrect result.

10 So I had a hard time going the other
11 direction. That's what --

12 MR. KURITZKY: Yes, I don't -- and, Louis,
13 I don't know whether you have an example for --

14 MR. CHU: Say it generates an incorrect
15 result. If you have a good reliability model, then
16 you can capture the effect of this incorrect result.
17 For example, our model of the digital feedwater
18 control system -- if you introduce an incorrect
19 signal, the simulation tool will automatically
20 propagate its effect and determine how the software
21 failure can affect the outcome on the system.

22 MEMBER BLEY: You are just saying, if the
23 software doesn't generate a signal, then the hardware
24 not performing is because it didn't get a signal, and
25 that's a linkage between the hardware and software, is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that what you are --

2 MR. KURITZKY: Let me try and clarify.
3 Actually, we are going down I think a path that we
4 don't want to go down. I think more important -- more
5 to the point is that in this discussion about
6 dependencies, and whether or not the hardware and
7 software can be modeled distinctly in the model, in
8 the BNL model they have separate placeholder events
9 for software, and I think that our intention -- we
10 don't know for certain, but our intention is to model
11 them as separate, basic events in the model, to use
12 fault tree speak.

13 I think there are other approaches we can
14 use where you assume that the software is embedded on
15 the hardware, and, therefore, there is a single event
16 in the model that is the failure of that component,
17 whatever. And whether it fails because of the
18 hardware failure or some software glitch is not going
19 to be distinguished.

20 I think when you go back to the -- and
21 there are people here who can speak to this better
22 than I can, but if you go back to the dynamic approach
23 that was pursued by Ohio State University, I think
24 when they tried to qualify their models they didn't
25 assume that the software were separate. It was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 embedded in there.

2 So they did a fault coverage type testing
3 thing where they injected faults into a mock-up of the
4 model or a version of the system, and they would track
5 how many of the faults would -- the system could
6 correctly account for and which ones it couldn't, you
7 know, to determine the fault coverage, and use that to
8 quantify the models.

9 So implicit in there is whether the
10 failure was a software failure or a hardware failure
11 wasn't important. It's just that it didn't work, and
12 that is one approach, and there are issues about that
13 approach as well as there are issues about our
14 approach. But that is the case where they are
15 embedded together as opposed to the other instance
16 where you would separately quantify them each
17 individually. And that is really what we are trying
18 to -- the point we are trying to make with that
19 bullet.

20 MEMBER BROWN: Okay. Well, that seemed to
21 me -- I looked at that and said, "Hey, if you want to
22 be able to include it," I understood the thought
23 process. I've got hardware, I've got software, I can
24 do them separately, I can do them together, but I've
25 got to understand the dependencies. So I was trying

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to connect, where is the glue between the
2 dependencies? If you can't -- if I can work and
3 figure out the hardware dependencies, fine, I can do
4 -- I work those. I can include them in the model.

5 But if I can never reach an agreement on
6 what software dependencies are that could cause the
7 hardware -- I mean, what -- the software is really
8 what the programmer writes. It gets converted to ones
9 and zeroes. It gets put into the -- you know, the
10 proms and the memories and all the other type stuff.

11 The hardware has to hold on to it. The
12 software can get corrupted, but that's about it.
13 Software itself doesn't -- I don't want to use the
14 word "fail," but defining -- if you don't understand
15 the dependencies the other direction, that seems to me
16 that that provides a difficulty of completing your
17 statement up there where I can model these things, if
18 you don't understand those dependencies.

19 MR. KURITZKY: Right. And --

20 MEMBER BROWN: And I got one direction. I
21 don't have the other direction.

22 MR. KURITZKY: Right. And again --

23 MR. CHU: One example --

24 MR. KURITZKY: Okay. Let me just -- I
25 think the one thing -- the point I forgot to clarify

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 also that goes to your question is that in the one
2 direction, the hardware to the software direction,
3 that was one aspect that we would have to consider, is
4 the fact that various hardware failures would
5 influence what the conditional probability of the
6 software failure is to use the standard terminology.

7 So, in that direction, we want to make
8 sure that, depending on the level of sophistication of
9 our software quantification -- standard quantification
10 method, whether we can get to that level, but you
11 might want to consider that, if component X fails, the
12 likelihood of the software failing may be a lot higher
13 than if everything was working normally. Okay? So
14 that depends -- we would ideally want to account for.

15 I don't know if there are any examples
16 that go the other way around, like I say, where the
17 software -- where something would affect -- in the
18 software would mean that our failure probability for
19 the hardware would be different than what we would
20 just normally give it as a failure probability.

21 My inclination is that I doubt we would
22 ever use a different hardware failure probability
23 based on what has -- what is going on with the
24 software. It would be the same failure rate or
25 failure probability we would always use. But I can

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 envision why we might want to use a different failure
2 probability for the software, depending on what has
3 transpired in the hardware part of the system.

4 MEMBER BROWN: Okay. Bear in mind, when I
5 talk about the software, I am not talking about data
6 that comes in and gets corrupted. I am talking about
7 the software program itself gets affected --

8 MR. KURITZKY: Right.

9 MEMBER BROWN: -- by, you know, whatever
10 external effect, whether it's noise or whether it's
11 gamma rays or whatever it is. It changes something in
12 the programmable read-only memory.

13 MR. KURITZKY: Right.

14 MEMBER BROWN: Okay.

15 MEMBER SIEBER: I would seem to me if you
16 are trying to develop for -- basic principles for what
17 the instrument system failure rate is, you would have
18 to treat software and hardware differently. And that
19 way you could test the hardware devices for its
20 ability to perform over so many cycles, and put those
21 things down, and then you would analyze the software
22 to determine where the opportunities for a software
23 failure to occur, combine those.

24 On the other hand, if you really don't
25 care about what the failure rates of individual

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 components is, and you don't intend to investigate it
2 that way, you have to test whole systems. And then,
3 when you move it, that system design from plant to
4 plant has got to be identical, or the failure rates
5 aren't correct.

6 And it seems to me the separation of
7 hardware and software failures will give you a better
8 answer for systems where there are design variations
9 from one facility to another, or within one plant.

10 MR. KURITZKY: And I think at the workshop
11 the point they were making is -- in fact, the approach
12 you just mentioned is actually the kind of approach
13 that BNL is pursuing, that there is -- they recognize
14 that there are other approaches out there that others
15 might --

16 MEMBER SIEBER: You can do a lot of --
17 there are several different ways.

18 MR. KURITZKY: Right.

19 MR. CHU: Yes. About this first bullet, I
20 don't think the panel is, you know, elaborating too
21 much on that. My interpretation of that is that, you
22 know, you recognize the interaction between hardware
23 and software. So whatever model you develop, you come
24 up with your results. You have your sequences,
25 failure sequences. So it's the typical PRA purpose.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 To generate your sequence or to generate
2 your dominant cutsets, you want to make sure they make
3 sense, they represent the real --

4 MEMBER SIEBER: Right.

5 MR. CHU: -- real failures. In that
6 sense, you know, you can -- I think you can interpret
7 that first bullet that way, too.

8 Meng, you wanted to mention --

9 MR. YUE: Meng Yue. One example I can
10 think of in the direction you mentioned is your
11 software -- you can send, for example, a very abnormal
12 value to a piece of hardware equipment. And, of
13 course, due to physical limitations, the hardware may
14 not -- like its output will be saturated, but also
15 your software -- abnormal value may cause some damages
16 to your hardware or treat it as a protection of the
17 hardware equipment. That is also a possible case.

18 MEMBER BLEY: Like running a pump against
19 the shutoff head, because the valve didn't come open.

20 MEMBER BROWN: Yes. But, I mean, if you
21 look at ones and zeroes piling into a joint -- I mean,
22 the only one I can envision is when you have a LAN-
23 based type system, where you can overpower the bus, if
24 you want to say it, because you've got high
25 utilization and your bandwidth -- you have collisions,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and, therefore, information does get to where it is
2 supposed to go in a timely manner, which means you may
3 have an overrun, and, therefore, you don't process a
4 certain, you know, subroutine, or whatever it is,
5 where now everything breaks down after that. Is that
6 a -- that's not a dependency. That's more, in my
7 mind, a software failure that affects the performance
8 of the hardware in a manner that is detrimental.

9 So, I mean, that's the only thought. I
10 probably ought to go on here.

11 CHAIRMAN STETKAR: Yes.

12 MEMBER BROWN: Is that acceptable, John?
13 Thank you.

14 MR. CHU: Okay. Regarding modeling
15 software failure, the panelists have very diverse
16 opinions regarding the right level of detail of
17 probability modeling, and often, you know, it depends
18 on the availability of the data, it depends on the
19 objective of the studies.

20 This slide talks about method for
21 quantifying software failure rate and probabilities.
22 The panelists agreed that a constant failure rate is
23 appropriate for modeling software failure.

24 Two panelists point out there may be
25 situations where -- time periods where there are more

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 challenges for software in that situation. You know,
2 I guess the failure rate needs to be adjusted or
3 changed according to the condition.

4 The panelists discussed the feasibility of
5 quantifying probabilistic parameters, and proposed
6 that testing of software as the main method for
7 quantifying software reliability. Of course, in the
8 -- you know, in the later presentation we talked about
9 methods of quantification of software failure rate and
10 failure probabilities, and we will talk about issues
11 associated with these things.

12 The panelists also think the quality of
13 the development activity associated with software is
14 important and should be somehow accounted for in the
15 quantification methods. In particular, they have
16 mentioned that Bayesian Belief Network is a promising
17 method to consider.

18 MEMBER ABDEL-KHALIK: Now, in an earlier
19 slide, you say that it is not possible to identify and
20 eliminate all faults of a non-trivial software. And
21 of course the implication of this is that the failure
22 probability is a function of the level of complexity
23 of the software. And if that is the case, wouldn't
24 that be inconsistent with the first bullet on this
25 slide?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. CHU: No.

2 MR. KURITZKY: Well, why would you -- I
3 mean, the first bullet says that for a given piece of
4 software, regardless of how complex it is, that you
5 would have a constant failure rate at all times for
6 that piece of software. Now, there is actually issues
7 that people bring up about that assumption, but,
8 nonetheless, that is saying for a given piece of
9 software you have a constant failure rate.

10 CHAIRMAN STETKAR: Okay. At a given level
11 of complexity. Okay.

12 MR. KURITZKY: It has its own internal
13 level of complexity.

14 MEMBER ABDEL-KHALIK: Okay.

15 MEMBER BROWN: That is arguable.

16 MEMBER ARMIJO: Why is it arguable?

17 MEMBER BROWN: Well, if you -- just from a
18 basic experience, if you have ever actually executed
19 complex software, which I did, I didn't run into
20 constant failure rates or glitches or things that
21 happened. Stuff was in service for years.

22 CHAIRMAN STETKAR: It could have had a
23 small constant failure rate.

24 MEMBER ARMIJO: Well, very, very small,
25 almost, you know, 10^{-19} or something. I don't know as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I'd want to put it in your metrics here.

2 CHAIRMAN STETKAR: Per year? You are old.

3 (Laughter.)

4 CONSULTANT HECHT: Yes. I just wanted to
5 point out that characterizing software complexity is
6 problematic. I'll give you an example of a real-time
7 system which might have 5,000 lines of code, might
8 have a much higher failure rate than a database
9 management system with millions of lines of code,
10 simply because the inputs aren't as well characterized
11 and controlled.

12 So the actual structural complexity of the
13 software, which is what I think you are trying to get
14 to, is one of many factors that --

15 MEMBER ARMIJO: Yes, I just want to get to
16 Charlie's point. It's --

17 MEMBER BROWN: Myron and I would have a
18 disagreement. Simple software is more easily tested,
19 more easily manually tested, more easily reviewed,
20 more easily set up to look at what are the various
21 inputs. Now, you've got -- that costs money. It
22 takes time and people to do that. But it's more
23 easily reviewed to make a -- to have a good
24 understanding of what you're doing.

25 MEMBER ARMIJO: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: So, I mean, simplicity of
2 code is while you may be able to make another
3 argument, the simpler the code -- it's like everything
4 else, simple is better.

5 CONSULTANT HECHT: I would say that there
6 is kind of a niche. In other words, so long as you
7 can totally characterize the behavior of the software,
8 that would be true. However, at some relatively small
9 size, you end up with so many paths that that becomes
10 impossible. I don't know if it's 3,000 lines or 5,000
11 lines, but it's certainly less than 25,000.

12 MEMBER BROWN: It depends on how you
13 generate the programming.

14 CHAIRMAN STETKAR: Can I cut this off and
15 refer the Subcommittee back to the last bullet on
16 page 7 that says, "The panelists had very diverse
17 opinions regarding" --

18 (Laughter.)

19 It is clear that -- it is clear that
20 diverse opinions are present, and that's the power of
21 getting these panels together.

22 MEMBER BROWN: Yes.

23 MEMBER BLEY: For a problem with the
24 topic. When you bring up the quality of the
25 development of the software, at one level the things

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we're looking at are controlled by NUREG-0711, is it,
2 the John O'Hara study on how you lay out a program for
3 I&C development. On the other hand is the actual
4 development within a vendor shop --

5 CHAIRMAN STETKAR: Sure.

6 MEMBER BLEY: -- which I expect is what
7 this is talking about, which there is -- if you can't
8 even get failure mode information from, you're sure
9 not going to get any information that would make this
10 a feasible thing to incorporate in a program. Or am I
11 missing the boat somewhere?

12 MR. KURITZKY: No. That's a good point.
13 That's not really germane to this particular
14 discussion, but when we go to actual -- the bullet I
15 mentioned previously for the -- when we were talking
16 about a proof of concept, where we need to get all of
17 the information on a system to do a test case for it,
18 that type of information is something that we would
19 want to have, and it is very difficult to get.

20 Now, there is -- there are some sources of
21 that information for some -- there is certain code
22 that is publicly available code, and the processes
23 used by the developers might not be proprietary, or
24 they may not care. For instance, the teleprint system
25 that we looked at, there is certain information in the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 SER for that that is in the public domain.

2 But when it gets to all of the procedures
3 for the software life cycle stuff, you will see a big
4 list of references with "proprietary" next to them
5 all. So, yes, that is going to be -- I agree, that is
6 going to be very difficult to get, from our purpose,
7 our research purpose of doing a test model. In a real
8 application, the person doing the study should be able
9 to have access to that information. But for us to do
10 our test case that is going to be an issue.

11 MEMBER BLEY: Even if you have that,
12 knowing how to incorporate it into your model and data
13 seems to me a pretty big leap.

14 MR. KURITZKY: Right. And that is what we
15 are trying -- that is one of the focuses of the work
16 that we are doing now on quantitative software
17 reliability methods is to take a couple of methods --
18 one, for instance, the BBN, let's say, is going to
19 need to incorporate that type of information.

20 And so, like I said, we may have to make
21 it up, or who knows how we are going to deal with it
22 in our test case, but theoretically in a real
23 application the applicant will have that information.

24 MEMBER BLEY: Okay.

25 MEMBER SIEBER: It would be far more

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 difficult to figure out how to test it than it would
2 be to write it in the first place.

3 CONSULTANT HECHT: Often that's true.

4 MEMBER SIEBER: Yes. That's my
5 experience.

6 MR. CHU: Okay. The whole workshop lasted
7 only a day and a half, so the discussion was at a
8 relatively high level.

9 The last bullet on this slide, you know,
10 for the safety sensitive nuclear powerplant, you tend
11 to have probably redundant channels running identical
12 software. The panelists agree that in PRA modeling it
13 is reasonable to assume that if they fail, they will
14 fail together. That is, using a common cause failure
15 -- a data factor of one, it may be somewhat
16 conservative. It's a reasonable thing to do when you
17 model channels running identical software.

18 Conclusions. The panelists established a
19 philosophical basis for incorporating software failure
20 in a PRA. And probability theory can be used to model
21 software failures, but we need to account for the
22 unique characteristics of software. Quantitative
23 methods can be used to quantify software failure rates
24 and probabilities.

25 MEMBER BROWN: That is what you are going

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to prove to us next, right?

2 MR. KURITZKY: Well, I don't know if we
3 are going to have proof of it today, but we -- these
4 conclusions, by the way, are consistent with what came
5 out of that 1997 National Research Council study, too.

6 They came up with essentially the same conclusion as
7 the panel members that were at the BNL workshop. So I
8 guess that is enough of an endorsement that we are
9 proceeding forward with this work. How well it --

10 MEMBER SHACK: But you didn't invite Nancy
11 Leveson to the workshop.

12 MR. KURITZKY: And that was actually a
13 conscious decision. We didn't -- one thing at that
14 workshop, we decided whether we should invite people
15 from both camps and decided in our day and a half we
16 would have nothing but the "he said, she said," and
17 that "tastes great, less filling," and we would not
18 get anywhere. So --

19 MEMBER SHACK: Your first one is almost a
20 foregone conclusion, then, considering who you
21 invited.

22 MR. KURITZKY: Well, in many regards --

23 (Laughter.)

24 In many ways, it was --

25 MEMBER SHACK: That was one of my

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 objections to the results.

2 MR. KURITZKY: But it is also -- but,
3 remember, to establish the basis, we don't need to
4 have universal agreement.

5 MEMBER SHACK: No.

6 MR. KURITZKY: We just need to -- we
7 wanted to make sure that there was -- beyond our small
8 realm, there were well educated and experienced minds
9 that knew what we were thinking. And that was what
10 the workshop accomplished.

11 CHAIRMAN STETKAR: Alan, one quick
12 question. One thing that, as you are well aware, the
13 ACRS has emphasized repeatedly is the search for, and
14 definition of, failure modes of software. And Louis
15 had it as a bullet on one of his slides, but there is
16 actually a table in the report where apparently the
17 group of panelists --

18 MR. KURITZKY: Well, the generic failure
19 modes --

20 CHAIRMAN STETKAR: -- agreed on a list of
21 generic failure modes. And I was curious -- it is,
22 you know, a relatively small, fairly concise group. I
23 was curious whether that was -- there was strong
24 endorsement of that in terms of comprehensiveness, or
25 was this simply a trial balloon that was floated and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the group said, "Yeah, yeah, sure, sure, that's okay"?

2 MR. KURITZKY: In between. It wasn't
3 quite that simple, but it wasn't a rigorous
4 evaluation. I think at that point of the meeting it
5 was -- we wanted to see whether people had some ideas
6 about generic failure modes. We would put things up
7 on the board; people would discuss them. It got --
8 you know, it would get changed a little bit as people
9 would voice various opinions, but it wasn't -- I
10 wouldn't call it a very rigorous --

11 CHAIRMAN STETKAR: You didn't explore much
12 detail about the extent of that list. Is that what
13 I'm hearing?

14 MR. KURITZKY: Louis, what is your
15 recollection? I don't remember it being exhaustively
16 discussed. It was --

17 MR. CHU: No, it was not. No.

18 CHAIRMAN STETKAR: But, for example, I
19 couldn't pick up this nice, neat table and say, "Yea,
20 verily, we have convened a panel of experts, and they
21 all agree that this is where we need to focus our
22 effort."

23 MR. KURITZKY: No. I think if you were
24 going to go forward and do work in this area, you
25 might take that piece of paper and say, "Here is a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 starting point for an input," but I wouldn't take it
2 as --

3 MEMBER BLEY: I didn't quite get that
4 impression.

5 CHAIRMAN STETKAR: I didn't get that
6 impression either. I was trying to see if --

7 (Laughter.)

8 -- my goodness, this is what we've been
9 asking for, but --

10 MR. KURITZKY: Well, I mean, everybody
11 there did agree to that set of modes, but it wasn't
12 like that was a -- you know, a meaningful --

13 MEMBER BROWN: It's not all-inclusive.

14 MR. KURITZKY: Right. And it wasn't like
15 a major source of discussion. It was -- you know, if
16 we told people, "Hey, you're here, and the output we
17 want from this meeting is to come up with this set of
18 failure modes, and we are going to work for a day and
19 a half until we come up with the perfect set of
20 failure modes," then I would stand up here and hold
21 it, you know, with ribbons on it. But that really
22 wasn't --

23 MEMBER BROWN: Okay.

24 MR. KURITZKY: The main focus was to come
25 up with a statement on the basis, and this was just

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 add-ons.

2 MEMBER BROWN: You had to read the next
3 bullet, John, where it said, "Consensus methods or
4 approaches for identification-specific failure modes
5 do not seem to exist." That is --

6 CHAIRMAN STETKAR: But that is out in the
7 industry. I mean, you know, if you poll the industry,
8 something that you call a failure mode I might call a
9 failure clause, and somebody else might call a failure
10 mechanism. But the impression that I was left with,
11 at least reading the report, I think is the same as
12 Dennis' -- that these guys all lined -- people all
13 lined up on this, and --

14 MR. KURITZKY: And they did. I mean, they
15 all did agree to that set of failure modes, but I
16 just --

17 CHAIRMAN STETKAR: Well, but you didn't
18 necessarily pulse them to challenge them to say
19 whether it's complete or --

20 MEMBER BLEY: "If you were going ahead,
21 would you use this?"

22 CHAIRMAN STETKAR: Yes. "Would this be
23 the list that you would use in your model?"

24 MR. KURITZKY: Right. And that is where I
25 think some people there might say, "Yes, that's the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 list I would use." I think other ones if you sent
2 them back to their offices and gave them a week to
3 think about the problem they may say, "Well, now that
4 I think about it, I might want to change something
5 here." That's the only reason why I don't give it a
6 full, you know, golden endorsement.

7 CONSULTANT HECHT: John, if I could, this
8 is an area where you really have to get application-
9 specific. The people were very smart on generally the
10 study of probabilistic methods applied to computer
11 systems that include software. They did not know
12 about nuclear I&C, and they did not know about, you
13 know, the specific implementations, all of which
14 affect failure modes.

15 So if I would -- if this is a key point, I
16 mean, you start out with this is the conceptual
17 framework, and then, for example, in one of the
18 headings, which is spurious signal, then you get down
19 into further details about how you might break that
20 down based on the failure data that you have in
21 various sources, and not -- certainly including, but
22 not limited to, the LERs, which is certainly a valid
23 source.

24 And on that basis, you can refine the list
25 but there is no -- just like there is no general

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 computer system, and there is specific computer
2 systems, and you have systems for cell phones that are
3 different than systems for eBay.

4 We have to -- failure modes have to be
5 somewhat tailored to the application.

6 CHAIRMAN STETKAR: Well, but I think what
7 we have been struggling for, trying to elicit from the
8 experts, is essentially a reasonable complete, if I
9 can characterize it as that, list of failure modes for
10 which there is some agreement, such that if you are
11 doing an analysis you can use that as a context to
12 think against.

13 For example, simple case, motor-operated
14 valve. It can fail to open, it can fail to close, it
15 can open spuriously, it can close spuriously. Those
16 are the four failure modes that people think about.
17 When I do an analysis of a motor-operated valve, I
18 must think about those four failure modes. I don't
19 need to think of that valve getting up and driving to
20 Pasadena as a failure mode, for example, because that
21 is not a failure mode that we in the risk assessment
22 community have attributed to that type of -- piece of
23 equipment.

24 So I think what we have been struggling
25 for is a reasonably concise list of failure modes,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 such that if you were -- if you were doing an analysis
2 of a particular reactor protection system for a
3 particular plant design, you would say, "Ah, okay, I
4 -- I know now that I need to think about these various
5 failure modes." And some of them might not apply, but
6 you would have some confidence that you are not
7 missing any failure modes from that library.

8 CONSULTANT HECHT: But think about all of
9 the information that is implied in that example that
10 you just gave. Motor-operated valve -- well, that
11 implies that there is a fluid there. That implies
12 that there is --

13 CHAIRMAN STETKAR: No, the fluid is
14 irrelevant. Motor-operated could --

15 CONSULTANT HECHT: I know that. I know
16 that. But I'm saying that software does a lot more
17 things than a valve does, and that, therefore, you
18 have to confine it to a --

19 CHAIRMAN STETKAR: In some sense, if the
20 collective expertise of the people who have spent a
21 reasonable part of their lives trying to understand
22 and model software, if that collective expertise comes
23 to the conclusion that it is impossible to develop a
24 coherent library of failure modes, where that list is
25 not in the millions, it is perhaps in the tens, at

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 most, if the collective wisdom can't develop that list
2 of failure modes, I think we have a very difficult
3 problem trying to develop a practical model for
4 software failures, because you have no framework
5 against which to do that evaluation.

6 CONSULTANT HECHT: I think it certainly is
7 possible --

8 CHAIRMAN STETKAR: Okay.

9 CONSULTANT HECHT: -- but it --

10 CHAIRMAN STETKAR: Okay.

11 CONSULTANT HECHT: -- just --

12 CHAIRMAN STETKAR: It doesn't have to be
13 easy.

14 CONSULTANT HECHT: Yes. I mean, I might
15 tell you that in one of the domains in which I work --
16 you know, satellite attitude control systems -- that
17 is going to be a very different set of failure modes,
18 and it is going to be for a feedwater control system,
19 believe it or not.

20 CHAIRMAN STETKAR: Even that type of
21 information I think would be very, very useful. We
22 haven't seen that type of perspective.

23 I think we'll stop that discussion,
24 because we need to get into the different --

25 MEMBER BLEY: I had my -- my very quick

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 question. Since you brought up the National Academy
2 Committee and their agreement with what your guys have
3 done, any of these guys in your group on that same
4 Committee?

5 MR. KURITZKY: No.

6 MEMBER BLEY: Okay. Thanks.

7 MR. KURITZKY: I was going to mention that
8 before when I said that, but --

9 (Laughter.)

10 CHAIRMAN STETKAR: Let's go on to talk
11 about the different methods, because there is quite a
12 bit of meat here. Louis?

13 MR. CHU: Okay. Now I am presenting our
14 review of the QSRM, quantitative software reliability
15 methods. First, I will give some background
16 introduction. And the second bullet is particularly
17 worth mentioning, because our report has been peer
18 reviewed, and we received comments from different
19 sources. As a result, we modified the report, and so
20 we have one slide highlighting the comments we get and
21 the changes we made to the report.

22 As part of our project, we developed
23 desirable characteristics for --

24 MEMBER BROWN: Were those changes in the
25 draft that we got, or was it subsequent to the --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. CHU: All subsequent.

2 MR. KURITZKY: All subsequent to that.

3 MEMBER BROWN: Okay.

4 MR. CHU: Yes. We are still working on
5 addressing the comments.

6 CHAIRMAN STETKAR: Are they -- just out of
7 curiosity, are they changes to the first part where
8 you go through the desirable attributes, or are they
9 more statements of fact as you characterize the
10 different methods?

11 MR. KURITZKY: I don't think there was
12 that much on the desirable characteristics. There
13 were some on those characteristics. There were some
14 directly on the method or a review of some methods,
15 particularly, as it turned out, by coincidence -- for
16 instance, we went to NASA as a reviewer. They
17 distributed it to a number of different people at some
18 of their space centers and contractors.

19 So through that process a lot of the
20 people that were actually involved in developing some
21 of the methods reviewed ended up being on that peer
22 review --

23 CHAIRMAN STETKAR: Okay.

24 MR. KURITZKY: -- and took exception to
25 some of the statements that --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: Okay. So there are
2 refinements of some of the reviews.

3 MR. KURITZKY: Right, exactly.

4 CHAIRMAN STETKAR: Okay.

5 MR. KURITZKY: Exactly. And it also
6 addressed some of the common issues we have as far as
7 how we define "software failure," and some of the same
8 general issues that we run into, but --

9 CHAIRMAN STETKAR: Okay.

10 MR. CHU: And then, we go on to summary
11 description of different methods we reviewed and
12 provide some comments on it. And then, we will give
13 summary and principal finding discussion.

14 For this presentation, I am going to give
15 the first part of it. When it gets to some specific
16 method, that Dr. Yue will give the discussion, and
17 then I will come back to do the rest of the
18 presentation.

19 Due to state of the art in modeling
20 digital systems, particularly software, there is no
21 commonly-accepted method. So this has implications on
22 quantitative software reliability method. That is,
23 you quantify a software failure rate and probability.

24 What are you using them for? Where do you use it?

25 The objective of our study is to gain

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 comprehensive knowledge about currently-available
2 QSRMs, particularly those that quantify failure rate
3 and failure rate probability that can be used in
4 digital model in a PRA.

5 Our approach Alan has kind of talked about
6 before. We developed desirable characteristics for
7 QSRMs. We went through some search of NRC-sponsored
8 work, NASA-sponsored work, and international
9 organizations' research, and open literature research,
10 to identify the methods.

11 Principal changes in response to peer
12 review -- our review has been -- our report has been
13 reviewed by the NRC staff and a group of peer
14 reviewers, outside peer reviewers. And as Alan
15 mentioned, NASA also is -- since NASA has cooperation
16 with the NRC, they got to review our report also.
17 Some of the NASA staff provided comment on our
18 reports.

19 MEMBER BROWN: Can I interrupt a second?
20 You talk about the organizations you went to, and I
21 guess there was no -- no input from any industry or
22 design group that has actually built and designed and
23 fielded these things, where they have had to do a -- I
24 guess a quality reliability review of their own
25 software in terms of how it performs?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I mean, that is real stuff, as opposed to
2 what I call the -- most of these look like studies or
3 more academic-oriented. That was the one thing that
4 stuck in my brain from -- not real-world application
5 type stuff. And that was kind of reflected in some of
6 the comments.

7 MR. KURITZKY: Yes. Some of these
8 approaches are actually real-world approaches. Some
9 of them are more investigations and studies and are
10 not -- they aren't necessarily applied in a real
11 application. The majority have been applied in
12 various industries, but, in any case, as far as our
13 input from industry, we, under our EPRI memorandum of
14 understanding, we went through EPRI to get review of
15 this.

16 Unfortunately, because of the timing of
17 the review with -- the people involved had other
18 things they had to deal with, and so we didn't
19 actually get any input from them this time. In the
20 past, we have always had comments back from EPRI, and
21 we have also had industry reviewers -- other industry
22 organizations provide feedback through the open public
23 response period.

24 This report didn't have a public response
25 period, so we were relying on our memorandum of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 understanding with EPRI for our review. But,
2 unfortunately, we were not able to get any comments.

3 MEMBER BROWN: I was thinking somebody
4 like Boeing, who has to have the fly-by-wire stuff,
5 and if their planes don't fly, then their software is
6 very critical to them. That's --

7 MR. KURITZKY: Right. And, no, we don't
8 have any -- commercial organizations were not involved
9 in the review.

10 MEMBER BROWN: Not involved.

11 MEMBER ARMIJO: But, Charlie, I think JPL
12 has done an incredible amount of stuff on software
13 reliability for their spacecraft in various
14 experiments.

15 MEMBER BROWN: Yes, I didn't know. It
16 just -- they didn't list it explicitly.

17 MEMBER ARMIJO: You had a JPL guy and --

18 MEMBER BLEY: And JPL has done real-time
19 support for NASA on that.

20 MEMBER BROWN: Yes. When you look at the
21 timeframe for the major -- the shuttle was the biggest
22 one that runs that, at least in my opinion, and that
23 is -- those designs are old. They have been around.
24 They haven't -- they are not as -- they are not of the
25 same --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: But, remember, we are
2 talking about methods for evaluation.

3 MEMBER BROWN: Yes. I'm just saying --
4 I'm saying they have methods, and I'm just saying
5 their methods are applied to --

6 MEMBER ARMIJO: Yes, I -- no, but their --
7 I just worked with them a little bit when we were
8 designing a reactor for use in space, and they were --
9 they had the lead on the software, and mainly because
10 they had amazing capabilities to do things we
11 certainly didn't have. And so I was glad you had
12 representation from that organization.

13 MR. KURITZKY: Yes, we did, and we got
14 quite a bit of comments back from JPL.

15 MEMBER BROWN: You answered my question.
16 Boeing, Lockheed, people like that, were not involved.

17 MR. KURITZKY: No. Commercial
18 organizations we didn't --

19 CONSULTANT HECHT: I would just comment
20 that JPL in fact -- Alan Nikora, who is one of the
21 people that participated in this review and is one of
22 the leads in doing that work at JPL, is looking at
23 satellite systems and more recent satellite systems.
24 It is true that work was done on the shuttle.

25 A lot of work was done by Norm Snyder

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 using that data that he had available, because he
2 worked on that program. But that's not the only
3 source of data that was used. In fact, Norm uses -- I
4 mean, Al uses data from JPL projects, not from the
5 shuttle, not from the Houston software.

6 MR. KURITZKY: Allen Nikora was the
7 principal person from JPL that provided comments to
8 us, so --

9 MEMBER BROWN: Okay.

10 MR. CHU: Okay. Then, let me go through
11 the principal changes as a result of peer review.
12 First one, we added references to NRC-sponsored
13 research on dynamic modeling method. Basically, we
14 got comments that said, "Why didn't you reference
15 them?" The reason we didn't reference them originally
16 was that dynamic methods are modeling methods.

17 While the purpose of our current project
18 is to get methods for quantifying software failure
19 rate and failure probability, so that dynamic modeling
20 methods are not quite quantification methods, but we
21 put those studies in the background/introduction part
22 of our report.

23 The second bullet is -- has to do with our
24 repeated statement in our report that says for
25 protection systems we need demand failure probability

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 model. And for control systems we need failure rate-
2 based models, and failure rate-based model and demand
3 failure probability-based model may well be different
4 models.

5 There were quite a few comments related to
6 that. It seemed -- the statement seemed pretty
7 obvious to me as a PRA guy, but they were comments
8 that -- I guess a reason may be some people are
9 working on methods such as software reliability growth
10 method. They work with failure rate only, and they
11 also argue that for protection systems it is running
12 all the time. Therefore, using failure rate -- it is
13 correct to characterize using failure rate also.

14 CHAIRMAN STETKAR: Louis, is that failure
15 rate -- I don't understand software, so maybe that's
16 good. There are many models that are used even for
17 hardware that apply things like an incipient failure
18 rate and a test interval to infer a failure on demand.

19 You are familiar with the, you know, lambda-T over
20 two type things for an incipient failure rate for
21 failure of a valve to operate on demand, where indeed
22 one could collect actual demand data if you had the
23 number of failures, the number of demands, and just
24 used the raw data.

25 Is that notion involved in people's use of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 software failure rate per hour to estimate a failure
2 per demand, if I can call it that, of the software?
3 In other words, given a set of input conditions, the
4 software will fail to produce the output. Are they
5 simply using the equivalent of an incipient hourly
6 failure rate with some sort of test interval to infer
7 the likelihood that something would not do something?

8 In other words, what I'm asking is, you
9 know, there is this big discussion about failure rates
10 in terms of a lambda per hour versus failures per
11 demand, characterized as probability per demand here.

12 Are those just simply two different contexts for
13 trying to estimate the same thing, or is it really
14 something different, like a pump fails during
15 operation versus start?

16 MR. CHU: I think the behavior of software
17 is different from that of hardware. That is, you can
18 look at it. You supply input to the software, and it
19 generates output. In that sense, you can look at it.

20 It is all --

21 CHAIRMAN STETKAR: To continue to operate.

22 MR. CHU: Continue running every -- every
23 cycle you have input coming in; it generates an
24 output. You can look at that as demands. We have
25 demand coming in. In that sense, you can argue

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 regardless what software you can use the demand
2 failure rate.

3 But looking at I guess -- say software
4 reliability growth method -- people try to estimate
5 failure rates by using data collected during debugging
6 tasks, and there they -- I guess they are just used to
7 the notion of failure rates, and the models were
8 developed based on that consideration.

9 But, in reality, I feel it is a basic
10 difference between software and hardware. Software is
11 somewhat more demand-based. Generally, every cycle
12 you run the software, you have input, and you have
13 output.

14 CHAIRMAN STETKAR: Well, but, I mean, in
15 some sense that process -- you could think of a demand
16 and response, but it -- you could also characterize
17 that as a consumer use operating group. There is
18 probably two elements. I'm just trying to think of --

19 MEMBER BLEY: If we get to the point that
20 we've got well defined failure modes --

21 CHAIRMAN STETKAR: Right.

22 MEMBER BLEY: -- then it will be clear
23 which model is most appropriate --

24 CHAIRMAN STETKAR: That's right.

25 MEMBER BLEY: -- or some other model. But

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 until we have that, we are arguing about something
2 that is kind of undefined.

3 CHAIRMAN STETKAR: Well, I was just trying
4 to get to the notion of what the people who -- the
5 proponents of those lambda failure rate models really
6 mean by what they are.

7 MEMBER BLEY: I understand. And in a PRA
8 over -- they always use a time-based one and --

9 CONSULTANT HECHT: Can I offer some --

10 CHAIRMAN STETKAR: Yes.

11 CONSULTANT HECHT: -- comments on that?
12 As Dr. Chu has mentioned, a monitoring system, which
13 is a safety system, which EPRI has a cycle, every time
14 it monitors, then it's making a decision each time it
15 runs. Let me -- but on the other hand, you could
16 argue that in the abnormal conditions, then it has to
17 make a decision.

18 If I could separate any real-time
19 monitoring or control system into two components, one
20 component which takes the data from the hardware
21 inputs, puts it in the right places, and makes it
22 ready for the application to decide whether or not it
23 should take an action from the application itself,
24 which is deciding whether to take the action.

25 I think when you say "inputs" and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 "outputs," your assumption is that the data is in the
2 right memory locations, and the logic is ready -- you
3 know, is ready for the logic to be exercised.

4 Software failures often occur -- or what
5 is called "software failures" often occurs in that
6 process of acquiring the data or outputting the data
7 to the system, because there is a lot of asynchronous
8 processes happening, race conditions, and things like
9 that. So --

10 CHAIRMAN STETKAR: Which, in principle,
11 would be more accurately characterized by some type of
12 lambda rather than --

13 CONSULTANT HECHT: Right. So you might --

14 CHAIRMAN STETKAR: But, again, as Dennis
15 said, if you had the right notion of what failure
16 modes, you are looking for --

17 MEMBER BLEY: If it fails there because
18 some random process there puts it in the wrong place,
19 then it's more a demand kind of thing. If it happens
20 because something got set up in the timing, and these
21 timing sequences are running all the time, then maybe
22 it's more of a timing issue.

23 I think until we know what we're talking
24 about, as far as what is failing -- and you are real
25 close to it there -- you can't decide that once and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 for all for all kinds of failure modes.

2 CHAIRMAN STETKAR: That's right, yes.
3 Well, but it difficult, then, to make decisions about
4 methods, without knowing that.

5 MEMBER BLEY: I think I've heard that
6 before.

7 CHAIRMAN STETKAR: Have you.

8 (Laughter.)

9 MEMBER BROWN: Let me state that a
10 slightly different way. I mean, on the -- the way I
11 used to look at it, on the demand side you can have
12 your software taking all your parameters -- pressure,
13 power, whatever it is. And it can be going to a logic
14 unit that says, "I want to trip or not trip based on
15 the value going into it."

16 But your software can put you in a
17 position where it is always generating a safe signal,
18 and you don't know it unless you've got some other
19 mechanism of testing that entire processing part of
20 the cycle, such that now when a real demand gets there
21 it is still getting that same safe signal, and you
22 don't get anything.

23 So if you don't -- if you don't have --
24 you have got to look at demand output systems -- that
25 is the only point I'm trying to make -- different than

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 those that have an observable output all the time,
2 like in meter --

3 MEMBER BLEY: Your example is one more of
4 these particular kinds of failure modes that could --

5 MEMBER BROWN: Failure modes, exactly. I
6 just -- as opposed to being more general, I tried to
7 be a little more specific to make it a little bit more
8 at least understandable to those who aren't versed.

9 MR. KURITZKY: On this, it doesn't
10 necessarily resolve that issue as far as whether it
11 should be a failure -- a demand probability or failure
12 rate. In any given case, I think as Dr. Bley
13 mentioned, you know, it is going to be -- you have to
14 have the failure modes identified to know exactly how
15 you want to pursue it.

16 But one thing to keep in mind -- and it
17 goes back also to something that you mentioned before,
18 Dr. Stetkar, about that list of generic failure modes,
19 we are looking at something from a -- now, remember,
20 this is to be incorporated into a PRA for a plant and
21 a system, so what we are really looking at is, what's
22 the impact on the system in its safety function we are
23 trying to accomplish?

24 And we worked back from there to dictate
25 what we want to see. It goes to the failure modes of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the valve. Remember, you said fails to open, fails to
2 close. Where do we come up with those failure modes?

3 Well, those are the different types of failure modes
4 that would exhibit different impacts on the system,
5 and so -- and the same thing with software.

6 We would have to identify the different --
7 we would want the complete set of failure modes that
8 could impact differently on the system. If there is a
9 bunch of different failure modes by name, but all have
10 the same impact, then there is no reason for us to
11 differentiate between them.

12 CHAIRMAN STETKAR: Right.

13 MR. KURITZKY: So we have to identify what
14 it is that we want to accomplish with the system in
15 our PRA, and that would dictate what kind of failure
16 mode we need to look at from the software. And
17 whether that is demand or a failure rate type of
18 model, even given that function, it could be a debate
19 whether -- how you should actually go through the
20 mathematics behind there.

21 One thing, though, to get to the direct
22 point about the comments we received from the peer
23 review is there was comments received that said you
24 can use -- there are ways to take a failure rate
25 approach and convert that to a demand failure

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 probability using something like demand arrival rate
2 or something.

3 So there's ways -- you know, there was
4 comments back that there are ways to consider to
5 transfer between the two.

6 CHAIRMAN STETKAR: As long as you
7 understand what you are trying to apply it to, and
8 what that failure rate measured.

9 MEMBER BLEY: And as long as the data come
10 from --

11 CHAIRMAN STETKAR: That's right. As long
12 as --

13 MEMBER BLEY: -- the process.

14 MR. KURITZKY: Right. And that's a given
15 no matter how -- whatever model you're going --

16 MEMBER BLEY: The one thing I'd say I
17 don't quite agree with with what you've said is even
18 if these failure modes all lead to the same higher
19 level failure effect, if the way you have to model
20 those modes are a little different, I don't think you
21 can combine them all.

22 MR. KURITZKY: That's right. When it
23 comes to quantification, you might have to subdivide.

24 CHAIRMAN STETKAR: Let's see. I wish we
25 had the full day, but we don't. Let's go to the next

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 slide, because I want to get through --

2 MR. KURITZKY: Different methods?

3 CHAIRMAN STETKAR: -- you know, the -- no,
4 the desirable characteristics is worth mentioning, but
5 we do need to spend, you know, some quality time with
6 the different methods.

7 MR. CHU: Okay. The desirable
8 characteristics were developed based on our perceived
9 need for reliability model and was developed based on
10 the knowledge and experience of the team members. In
11 general, they are expected to address general
12 guidelines in the ASME PRA standard.

13 These characteristics can be used to
14 evaluate methods and applications to see if the
15 characteristics are satisfied. But that evaluation is
16 not within the scope of the current report. What is
17 in our report -- we have described the methods, we
18 have comments. The information in the report
19 certainly are related to these desirable
20 characteristics. In that sense, the information -- it
21 would be helpful in evaluating the method.

22 In an ongoing current project, we are
23 doing that. We eventually will come up with a table,
24 you know, methods and the characteristics showing how
25 different methods are satisfied and characteristics.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: What is the schedule on
2 that?

3 MR. KURITZKY: That is that draft NUREG
4 that we are shooting for probably some time in the
5 fall.

6 CHAIRMAN STETKAR: Okay.

7 MR. CHU: And --

8 MEMBER ARMIJO: I'm sorry. But where are
9 the desirable characteristics shown? I didn't read
10 your report, so I apologize.

11 MR. KURITZKY: They are actually in the
12 back of -- we took them out of the main presentation,
13 because we had to reduce the size, but they are
14 actually -- I think they are --

15 CHAIRMAN STETKAR: And you said that the
16 peer reviewed comments that you have received have not
17 challenged those characteristics or --

18 MR. KURITZKY: There were some comments on
19 those characteristics.

20 CHAIRMAN STETKAR: Okay. So you are still
21 thinking about --

22 MR. KURITZKY: Yes, but there wasn't any
23 -- it wasn't like we got -- I mean, it was more like
24 reword this one a little bit, or -- it wasn't like
25 whole-scale changes to the --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: Nobody proposed --

2 MEMBER SIEBER: Nobody rejected.

3 CHAIRMAN STETKAR: -- you just said, "This
4 is -- this should be removed," or "You should add
5 something else."

6 MR. KURITZKY: Not really, no.

7 CHAIRMAN STETKAR: Okay. Thanks. Let go
8 down to the models, because I'm sure there is going to
9 be a lot of discussion about the individual methods.

10 MR. CHU: Okay. I this part I am going to
11 ask Dr. Yue to give the presentation on -- mainly on
12 software reliability growth models, Bayesian Belief
13 Network, and test-based methods. And then, I will
14 come back to the others.

15 MR. YUE: One type of software
16 quantification method is software reliability growth
17 method. It has been pretty popular. It is used to
18 estimate, for example, the software reliability
19 measures, including failure rates.

20 But the main purpose of using this kind of
21 method by industry is to determine whether the
22 software should be released, and then we look at the
23 reliability growth of software determining whether
24 they should give you -- release it to users.

25 In SRGM, software reliability growth

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 methods, the occurrence of the failure is assumed to
2 follow non-homogeneous Poisson process. In general,
3 it is assumed that during the testing the software
4 faults, once they are detected, it would be fixed
5 perfectly or instantaneously. That means it doesn't
6 introduce any new fault into the software, and it
7 would be fixed immediately.

8 And by doing this, the software
9 reliability, it increases, and of course the software
10 failure rate is going to decrease. There are so many
11 different software reliability growth methods, so how
12 failure rates -- exactly how they are decreased over
13 time will be determined by the individual empirical
14 formulas developed by different researchers.

15 And in -- when we were doing a review, in
16 the beginning we just found some references -- the
17 references to the continuous time software reliability
18 growth method, but later we found D-square time SRGMs,
19 but D-square time SRGM is not a topic of this report.

20 In the next draft report, we are going to include it,
21 discuss it.

22 Continuous time SRGMs -- they can be
23 categorized into the three categorizations. The first
24 one is called exponential NHPP, and non-exponential,
25 and also Bayesian model. When we were doing the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 review, we found a lot of people that were -- that
2 have been spending efforts to develop the unification
3 schemes such that you can look at all of the different
4 software reliability growth methods, and from the same
5 point of view, because people realize there are too
6 many methods and also different people that are using
7 different notations.

8 And by developing unification schemes it
9 is -- certainly it is going to help people to have a
10 better understanding of these kind of methods.

11 CHAIRMAN STETKAR: Keep on going. Speak
12 loudly.

13 MR. YUE: The first category of SRGMs is
14 called exponential NHPP, and here specifically the
15 software failure rate is assumed to be proportional to
16 the remaining fault contents, which is similar to the
17 radioactive decay of isotope. Basically, there the
18 decay rate is proportional to the inventory of the
19 isotope.

20 Effectively, the software failure rate
21 will decrease exponentially with time, and here we
22 have a list of different exponential NHPPs. There are
23 all -- they are failure rates. They are all
24 decreasing with time exponentially.

25 Non-exponential NHPP and the software

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 failure rate, they are assumed to be of a different
2 distribution. For example, it follows the shape of
3 probability-density function of a gamma distribution
4 or a wider distribution. So the failure rate is still
5 going to decrease, but not exponentially with the
6 time.

7 And, again, we have a long list of
8 different methods in this category, and I am not going
9 to go into the detail of them.

10 The third is the Bayesian SRGM models.
11 Both exponential NHPP and the non-exponential NHPP,
12 they are all assuming the failure rate will decrease
13 with time deterministically. That means they are
14 proportional to the remaining fault content, and that
15 will certainly decrease. But the Bayesian SRGM, it is
16 -- it is -- the failure rate is modeled as a random
17 variable. It is going to decrease, but in a sense of
18 probabilistic manner or a stochastic manner.

19 So essentially it is exponential NHPP, but
20 it includes the uncertainty of the failure rate in
21 this model.

22 So different -- although they have all
23 different kinds of SRGMs, all of them you have to use
24 the test data or the model data to estimate or
25 parameters of those empirical formula developments.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And there are only three kinds of methods that are
2 available -- maximum likelihood of method, least-
3 squared, and also moment-matching. They are used to
4 estimate the parameter of those empirical formulas.

5 And from all the literatures we have
6 reviewed, only a point-estimate of the empirical
7 formula parameters are estimated. So we don't see any
8 difficulty in terms of including our estimation of the
9 associated parameter uncertainties.

10 Some comments we have on continuous time
11 SRGMs -- it is the most popular software reliability
12 model in -- either in the industry or in the academic
13 areas, because there are simply so many of them.

14 And also, our review shows there is no
15 single SRGM which was always better or superior to the
16 other SRGMs, because they are all empirical formulas
17 applicable -- it might have -- give you a good result
18 in this kind of situation and give you a lousy result,
19 you know, not -- you know, a different situation.

20 And we also noticed that the assumptions
21 for SRGMs are actually quite stringent. For example,
22 it does require the failure occurrence that should be
23 independent of each other when you are doing the
24 testing. Of course, in reality, this might not be
25 true. But, still, many applications have been done,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and it has been demonstrated the SRGM methods are
2 quite robust, although those assumptions are quite
3 often violated, and --

4 CHAIRMAN STETKAR: What does that mean in
5 practice?

6 MR. YUE: Because when they were
7 developing the empirical formulas, they made certain
8 assumptions for them to develop those formulas. And
9 those assumptions, they might be difficult to be
10 satisfied in reality.

11 CHAIRMAN STETKAR: Okay.

12 MR. YUE: For example, the example I just
13 mentioned is -- they are -- when you are doing
14 testing, they require the failure occurrence to be
15 independent of each other. So that means when you
16 treat one failure -- that this planned failure -- that
17 is this failure, it doesn't trigger another failure in
18 the same testing. Because you have different input in
19 the case, that's why you have different failures.

20 But this is not easy to be satisfied, in
21 reality. That's one of the examples of --

22 CHAIRMAN STETKAR: Okay. I understand
23 that part of it. I was curious when you say, "Despite
24 all of that, the models were demonstrated to be
25 empirically robust," does that mean that the model

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 predictive capabilities for the failure rate have been
2 compared with actual observed data and they -- in
3 actual installations that are challenged?

4 MR. YUE: Yes.

5 CHAIRMAN STETKAR: Okay.

6 MR. YUE: Yes.

7 CONSULTANT HECHT: May I explain why?
8 Typically, these studies -- these models were
9 developed and actually used in large systems, started
10 out and is traditionally used in the
11 telecommunications industry. Musa started this work
12 in the late '70s, actually was challenged with the
13 problem -- they were coming out with a new electronic
14 switching system based on UNIX, software-based, and
15 when would it be ready to be released given that they
16 had certain reliability objectives that they wanted to
17 be achieved. So his basic challenge was to make a
18 projection.

19 So when you have large numbers,
20 irrespective of what the underlying phenomenon is,
21 central limit theorem and all the other things that
22 work along with that, help you.

23 CHAIRMAN STETKAR: Okay.

24 CONSULTANT HECHT: And the point is that
25 you have to have the right tool. This -- SRGMs are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 appropriate when you are trying to determine whether a
2 supplier can get to the starting gate. In other
3 words, he is doing -- these are all, as was mentioned,
4 a previous time but based on testing.

5 CHAIRMAN STETKAR: Yes.

6 CONSULTANT HECHT: And so they are
7 typically based on a large variety of test cases that
8 are being done during the integration, various stages
9 of integration, and very heterogeneous data.

10 So you will hopefully see a trend, and you
11 will eventually see it level off to some -- I'll call
12 it the final limit.

13 CHAIRMAN STETKAR: Right. You put it in
14 the box, seal the box off, people go buy it.

15 CONSULTANT HECHT: People go buy it. At
16 that point, the software is stable. It's not going to
17 be changed.

18 MEMBER ARMIJO: When you are saying
19 "testing," do you mean testing and fixing?

20 CONSULTANT HECHT: Yes.

21 MEMBER ARMIJO: Okay.

22 CONSULTANT HECHT: This is --

23 CHAIRMAN STETKAR: But my question was,
24 when you say that those models in the resulting
25 estimated failure rate, the out-the-door failure rate,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 have -- when I think -- you know, if I buy the
2 software and install it in my nuclear powerplant, I
3 don't particularly care how long it took somebody to
4 develop it. I don't care whether it failed constantly
5 for 36 years. I care what the product is and whether
6 I can have confidence that its predicted failure rate
7 indeed will be demonstrated in an actual application.

8 So my question was, you know, since we
9 have this long history, have people gone back and
10 actually confirmed that indeed these out-the-door
11 predictions are -- are they conservative because of
12 the way people do things?

13 And, indeed, the software -- you know, the
14 systems as installed perform better than that? Which
15 is the case in many cases of qualifications testing,
16 to simply say, "Okay. It's good to get out the door,
17 and I'll legally guarantee it to meet some sort of
18 reliability."

19 Or, indeed, in some cases do they
20 underpredict things, because the testing cycles didn't
21 completely test all of the facets, and it was good
22 enough to get out the door. When you say it's
23 empirically robust, that's what I was questioning.

24 CONSULTANT HECHT: In other words, it
25 would fit the data. You can get a curve that -- using

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 these models and get it to fit the data fairly
2 closely.

3 CHAIRMAN STETKAR: Right.

4 CONSULTANT HECHT: So the question is, how
5 -- what you are really asking is, how well does your
6 testing program represent the stresses it is going to
7 see in the real world? That's your real question.

8 CHAIRMAN STETKAR: Well, but you fixed all
9 of those failures, so you have not tested any of the
10 failures that you haven't fixed.

11 CONSULTANT HECHT: Well --

12 CHAIRMAN STETKAR: You have only predicted
13 the frequency of those failures is small enough to get
14 it out the door.

15 CONSULTANT HECHT: That's true.

16 CHAIRMAN STETKAR: And the question is:
17 is that supported by actual operating experience?
18 Indeed --

19 CONSULTANT HECHT: Well, yes. Operating
20 experience -- if the operating -- if the testing
21 program properly reflects the operating environment of
22 the software, then it will be -- it will be a
23 conservative prediction. If it -- if the testing
24 program misses some aspects of the operation regime,
25 then it will not.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: I -- yes, I got that.
2 The question is: in the real world, because, you
3 know, proponents are saying we should use this to
4 predict the failure rates that we would expect out in
5 those real-world applications. So what I'm
6 questioning is, what has been the experience when
7 these systems are installed in the real world?

8 Is our experience enough to give us
9 confidence that indeed the testing regimes are pretty
10 good at identifying the potential failures? In other
11 words, that we are not very often surprised.

12 CONSULTANT HECHT: In the
13 telecommunications industry, it is pretty good.

14 CHAIRMAN STETKAR: Okay.

15 CONSULTANT HECHT: Telecommunications.

16 CHAIRMAN STETKAR: Okay. Thanks.

17 Sorry.

18 MR. YUE: Actually, your mentioning of
19 that case is -- it can be seen from next bullet.
20 Generating test input cases is a big deal in terms of
21 how good testing data is.

22 And the third -- the fourth bullet says
23 demonstration are needed to show that estimated
24 failure rates feed actually operating experience well,
25 because you are supposed to generate test cases --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 test input cases from the expected -- at least the
2 expected operational profile, but in reality when you
3 are doing the testing you might not be able to do
4 that.

5 They all come here and criticize you,
6 don't consider this, don't consider that. That's one
7 of the big issues.

8 And, actually, I think that that's the
9 limitation of almost all of the software reliability
10 quantification methods, because you all have to rely
11 on the testing data, so that's more like an issue of
12 how you are going to do the test.

13 And the next bullet is saying since SRGM
14 is using the test failure data, so for our
15 applications we need to generate a very high
16 reliability. This method might not be able to give us
17 the number, like 10^{-5} . If you have one failure in a
18 number of tests, then your failure probability
19 probably is -- can be pretty high. It's difficult to
20 bring it down.

21 CONSULTANT HECHT: I just wanted to say
22 that my experience is when I use SMERFS or CASRE I
23 generally stop at about 10^{-3} per hour.

24 CHAIRMAN STETKAR: Per hour.

25 CONSULTANT HECHT: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: That would be 10
2 failures per year.

3 CONSULTANT HECHT: Yes.

4 CHAIRMAN STETKAR: Okay. Of course, that
5 depends on what you call a failure.

6 CONSULTANT HECHT: What they called a
7 failure.

8 CHAIRMAN STETKAR: Yes, okay.

9 MR. YUE: And, again, next bullet is
10 related to the previous discussion about the demand
11 failure probability or failure rate. Our review shows
12 the continuous time SRGMs that can be directly used to
13 estimate the failure rate of the software. And the --
14 for our RPS system, the demand failure probability is
15 of interest.

16 In this kind of situations, continuous
17 time SRGMs might be still -- we might be still able to
18 use the continuous time SRGMs. But we either have to
19 come out with numbers -- for example, the frequency of
20 the challenging the RPS is going to have -- oh, we
21 have to reinterpret as testing data, because
22 continuous time SRGMs, testing data is in the format
23 of number of failures in the time period.

24 And the data is in this kind of format.
25 It is -- failure rate is a natural product of this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 kind of method.

2 MEMBER BLEY: Meng?

3 MR. YUE: Yes.

4 MEMBER BLEY: I'm just having trouble with
5 this whole discussion because of a few things, and
6 maybe I'm wrong in my underlying assumptions, but help
7 me out. This kind of approach, I can see how it would
8 be useful in testing. I expect during testing that
9 some software diagnostics are built in that aren't
10 there when you run later, so I expect failures in the
11 field maybe aren't as clear is exactly what happened
12 is it might be during a testing program.

13 We don't have a system when it is no
14 longer in test where if you have a failure it gets
15 fixed immediately and is tested to make sure it is
16 really fixed. So a lot of the assumptions underlying
17 this seem to me not to apply unless it is run out
18 until the end of testing and you use that as a
19 constant failure rate from then on, and certainly
20 don't project that it is going down.

21 MR. YUE: Yes. When you release the
22 software to the, for example, nuclear powerplants --

23 MEMBER BLEY: Then, you're done.

24 MR. YUE: -- that is the -- you will
25 consider the --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: Okay.

2 MR. YUE: -- failure rate at the end of
3 the -- applying this method will be the constant
4 failure rate when you are --

5 MEMBER BLEY: From then on you just use
6 that constant failure rate.

7 CHAIRMAN STETKAR: That's why I was
8 asking, you know, where are you on that asymptote.

9 (Laughter.)

10 MEMBER BLEY: Exactly.

11 MR. YUE: And also, we just mentioned
12 discrete SRGMs can be used to give you direct answer
13 of demand failure probability. But that will be
14 addressed in the next phase of the research.

15 Another category of this is called the
16 Bayesian Belief Network. It is -- basically, it is a
17 probabilistic graphic model. It consists of a set of
18 nodes representing the random -- represented by the
19 set of random variables, and their condition -- their
20 dependency on each other will be reflected by the
21 relative age between these nodes.

22 A basic assumption is the condition or
23 independency of the Bayesian Belief Network. That is,
24 given the node, it is conditioned or independent of
25 its non-descendants nodes, given its parents' nodes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 This is basically reflected in the next formula here.

2 You have a set of random variables
3 represented by V_i , the joint distribution. If you
4 have Bayesian Belief Network, they can be reduced to
5 this formula here, given the parents' nodes obviously,
6 of this node. It is conditionally independent of the
7 non-descendants' nodes.

8 And when we are -- when we need to do the
9 Bayesian updating, we just update this equation using
10 the observed evidence, and we have a lot of different
11 types of tools, software tools, to help us perform
12 this kind of inference.

13 And also, it is -- we should mention
14 building Bayesian Belief Network, it has to be
15 application-specific. And there is no general rules
16 how you should -- how you should build it. And also,
17 there is no general guideline to tell you whether the
18 correctness of the dependency between different nodes
19 has been considered in your model.

20 It is peer reviewed by different experts
21 that are basically from different domains. One is BBN
22 -- one domain is the BBN, and another one is the
23 application-specific, and you have to make use of the
24 data, the statistical data and also the experts'
25 knowledge.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Some comments on BBN method -- and we can
2 see the principal strength of the BBN method is it is
3 capable of incorporating both qualitative evidence
4 that is experts' subjective opinions, and also the
5 qualitative evidence -- there is quantitative evidence
6 that -- there is statistical data either from tests or
7 from operational.

8 One thing is, if you want to update it --
9 if you want to use the Bayesian Belief Network to give
10 you the failure rates or failure probability you are
11 looking for, you have to quantify the qualitative
12 evidence. You have to determine how much impact to
13 software -- for example, how much impact the software
14 development process has on the failure rate or failure
15 probability of your software.

16 Unfortunately, there is no standard method
17 or procedure to do this kind of conversion -- convert
18 the qualitative evidence into the quantitative
19 evidence. We have reviewed some literatures in
20 different areas, and they are using different methods,
21 but basically the way to convert a qualitative
22 evidence to quantitative evidence is kind of
23 subjective, and it is determined by the different
24 groups of experts.

25 I also characterize independencies between

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 nodes. It is also -- it is also dependent on the
2 analyst's judgment and the knowledge and is -- quite
3 often it is difficult to verify. This can lead to a
4 large uncertainty of the results.

5 Test-based methods -- and just like
6 software reliability growth methods or BBN test-based
7 methods, they also make use of the test data. And so
8 the limitation of this method generally is applicable
9 to other software quantification methods, because they
10 are using the test data.

11 The way of -- test-based methods, you
12 apply the standard statistical analysis to the test
13 data, and so you can obtain the software reliability,
14 and different kind of testings are generally
15 performed.

16 The first one is called the white box or
17 glass box or gray box, and the second one is the black
18 box testing. In the first white box testing,
19 basically it is -- accounts for the internal
20 structure, the software executed in the past. You
21 have to understand the logic and the details of your
22 software design to perform this kind of test.

23 You are -- you have to make sure you are
24 visiting all of the paths, execution paths, all of the
25 nodes, in your software. Black box testing is like a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 functional testing, and here we have two approaches to
2 handle the data. One is called a frequentist
3 approach. Another one is called Bayesian approach.
4 That is basically how you interpret as a probability,
5 two ways to interpret as a probability.

6 Implementation of this kind of method
7 consists -- of course, you need to generate a testing
8 input case based on operational file. That is what we
9 expect. And you perform the test, and you apply the
10 standard of statistical analysis to quantify the
11 software reliability.

12 Some comments on these -- on test-based
13 models, we just mentioned that for software test cases
14 should be generated from the operational profile. The
15 difficulties sometimes is not available. We may not
16 know that.

17 Some people are also saying, "You have
18 software. When you are doing tests, you have
19 software. You remove the fault." Basically, it makes
20 this software a different version of the previous
21 software. How can you apply the previous testing
22 results to the current version of the software? That
23 is also one of the issues.

24 When you are doing tests -- when you are
25 doing testing, basically you are -- you fit the test

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to -- input cases to your program and also the Oracle
2 you build. This -- then, you compare the outputs of
3 your program, your software program and your Oracle --
4 compare whether they are consistent. If they are the
5 same -- if they are giving you the same results, you
6 are saying this is a success test.

7 The thing is, Oracle is also built based
8 on the requirements in the specification. So if the
9 requirement of the specification has a problem, this
10 -- the testing is not going to uncover that.

11 And the last one is a large number of
12 tests have to be performed if you want a very high
13 reliability parameter.

14 Two specific methods we are going to
15 discuss here. One is this correlation method.
16 Another one is the CSRM, which will be presented in
17 the next cut of slides.

18 The first one is the correlation method.
19 This one is built based on the past software
20 development practices, and this method is implemented
21 to a commercial tool. It is called a Frestimator. It
22 consists of proprietary data based on the previous
23 software development practice. This database, from
24 our understanding, is collected from -- by doing the
25 survey from software managers and software engineers.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Then, the methods make use of regression
2 analysis to process the data to -- with respect to the
3 density, the defect density. That is, the number of
4 defects per thousand lines of the code.

5 And, finally, you need to convert the
6 number of defects into a failure rate using an
7 empirical formula.

8 Comments on this method. The general
9 concept is very reasonable, because the past software
10 developed practice certainly is going to tell you
11 something about your current software project. The
12 difficulty here is commercial software. We don't have
13 very detailed information about this method, and we
14 cannot evaluate this method in a very detailed manner,
15 because availability of detailed information of this
16 database, and also what kind of correlation regression
17 analysis method is used in the software.

18 Potential limitation includes survey of
19 software development practice could be subjective, and
20 also, as we just mentioned, it used an empirical
21 formula to convert the fault -- the defect density
22 into the failure rate. This empirical formula might
23 lead to a larger uncertainty.

24 MR. KURITZKY: Meng, if I can, just -- one
25 follow-on point to the -- I guess to the second bullet

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 or the -- yes, the second bullet. While the concept
2 of using regression analysis and typing -- well, the
3 concept of considering the quality of software life
4 cycle activities and other aspects of developing
5 software to a failure rate is a reasonable one and it
6 makes sense that, you know, how well you do those
7 activities shouldn't affect what your failure
8 likelihood is for your software.

9 The problem with this approach is there is
10 all kinds of reasons why the experience with some
11 other software doesn't apply to your software.

12 CHAIRMAN STETKAR: Sure.

13 MR. KURITZKY: So, you know, the general
14 concept is good, in some respects, but there is issues
15 in the applicability -- you know, applying it like it
16 was done in this approach. I think this is our last
17 slide on here, so just to note we got -- as part of
18 our peer review on this report, we got some comments
19 back from some of the NASA reviewers that pointed out
20 that while there was a general feeling that this had
21 some promise when they first were using it, they were
22 starting to back away from their endorsement of
23 this --

24 CHAIRMAN STETKAR: The concept is good,
25 but --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. KURITZKY: Right.

2 CHAIRMAN STETKAR: Yes.

3 MR. KURITZKY: Right.

4 CHAIRMAN STETKAR: Okay.

5 MR. KURITZKY: So --

6 CHAIRMAN STETKAR: Okay.

7 MEMBER BLEY: Primarily because of the
8 lack of being able to verify what is --

9 MR. KURITZKY: Exactly. The lack of
10 transparency was a big issue, and also there was --
11 they did some kind of a project where they compared
12 the failure rates that they would obtain through this
13 method with some other methods, and with actual data,
14 and this one was coming off well out of sync with the
15 other approaches.

16 CHAIRMAN STETKAR: That would be important
17 information.

18 MEMBER BLEY: Yes.

19 CONSULTANT HECHT: This approach was tried
20 in the '80s. This is what I call the classical period
21 of empirical software engineering. It is -- you know,
22 funding dried up shortly thereafter, partially for
23 reasons like this.

24 There is -- basically, everybody would
25 love to do this, but -- and everybody would love -- if

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 they can't do it on the basis of software development
2 processes, would love to do it on the basis of some
3 kind of structural aspects of the code before actually
4 having the code to run and test.

5 And none of the thousands -- literally,
6 thousands of projects that have been done in this area
7 have stood up.

8 CHAIRMAN STETKAR: So since you haven't
9 done the evaluation yet, you are not sure where this
10 will fall, but --

11 MR. KURITZKY: That wasn't one that we
12 were leaning towards.

13 Let me just point out real quick before,
14 Meng, you strike this -- context-based software risk
15 model. Another big change from what was done
16 originally, what you see in your draft report, this
17 isn't an approach that was -- that NASA has pursued
18 and was pursuing it for their Constellation program.
19 Of course, that is now kind of disappearing, but this
20 approach was being -- they have been pursuing it for a
21 few years, and have applied it more and more
22 frequently recently.

23 Now, we had it originally in the draft
24 version that you were going to see, but the report
25 that we had reviewed that had the information on this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 approach was -- had sensitive information in it, and
2 so we had to -- at the last minute we had to yank it
3 all out of the draft report.

4 Since that time, NASA -- well, the report
5 was labeled that it might have sensitive information.

6 So we had --

7 (Laughter.)

8 Since that time, they went and actually
9 did an official review of it and determined, verily,
10 it is not -- does not have sensitive information, so
11 we are sticking it back. And so the new version of
12 the report will have a new chapter or section on this
13 approach. You didn't see this in your --

14 MEMBER BLEY: Oh. When will we get to see
15 that, or can you get it to us sooner? Because it
16 would -- it is -- this one I would really like to see.

17 MR. KURITZKY: Well, you know, I can get
18 you the publicly available report. Well, actually, I
19 don't know if it's publicly available, but it's just
20 not sensitive, but --

21 CHAIRMAN STETKAR: Let's talk about
22 schedule.

23 MR. KURITZKY: Oh, okay.

24 CHAIRMAN STETKAR: Let's see if we can get
25 through the thing and --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. KURITZKY: Okay. So this is going to
2 be in the final report, so just -- so you're not
3 surprised. Go ahead, Meng.

4 MR. YUE: Context-based software risk
5 model, CSRM, is a modeling method. It basically
6 incorporates the software behaviors and considers its
7 contribution to the risk into PRA. And the concept is
8 context-based scenarios.

9 As it claims, it is able to identify
10 hardware failures of normal conditions under which the
11 software are supposed to work or respond correctly,
12 but it doesn't. So it is basically a PRA modeling
13 tool. It doesn't have its own quantification method,
14 although it can be used in conjunction with the
15 quantitative estimation process, like SRGMs or
16 Bayesian Belief Network or test-based methods.

17 The first bullet, we have said that, and
18 another one is the principal advantage of the CSRM.
19 It covers the estimation of the frequency of a system
20 entering the contacts to faulting condition, and there
21 is the frequency and the failure probability of the
22 software.

23 Basically, it is more like a test method.

24 If the frequency of this kind of scenario doesn't
25 happen, it is very low, then probably you don't need

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to do too many testing to determine like your software
2 has a very high reliability.

3 Thereby, this method, using this method,
4 potentially reducing the test to -- the testing burden
5 here. Potential limitations include -- one issue is
6 you might have a very large number of contacts, and
7 the one you are doing the testing input cases, you
8 have to manually generate all the input cases. If you
9 have a lot of contacts, you have to consider this
10 could be very difficult to implement.

11 Another issue is complex software. It
12 might contain thousands and thousands of variables,
13 and each variable might have a large -- a different
14 number of states, let's say. And, therefore, there
15 must be a significant tradeoff between the accuracy of
16 your model and the complexity of your model here.
17 Those are potential limitations of this method.

18 MEMBER BLEY: This might be an
19 opportunity, though, for something like your last
20 exercise with the experts, but something like a PERT
21 process to generate, what could be the most like to be
22 important context to limit this from a massive problem
23 to an approachable one, and could really get at some
24 of the odd things that crop up that might be really
25 important.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And I guess the one I keep -- when I read
2 places where software has gone awry -- it's not always
3 the software -- you get these cases where the inputs
4 come in well outside of the range of testing and just
5 oddball things happen. And, you know, that is one
6 that none of these other methods quite addresses,
7 because they haven't seen that yet.

8 And so the testing program didn't see the
9 stuff outside of the test, and one day it happens and
10 you get some interesting things. So this one smells
11 like something that could help us for the really nasty
12 cases, if you could find a way to control the scope.
13 And it's awfully easy to dismiss something that looks
14 like the scope could blow up, when there might be good
15 ways to limit it and get something useful out of it.

16 MR. KURITZKY: Yes, I think with this
17 approach, one of the key aspects of this approach was
18 that -- or the fundamental concept here was that
19 software is good at performing under its nominal
20 conditions. In other words, this can be tested under
21 those nominal conditions and so it's -- it's going to
22 be fine.

23 It when you get some off-nominal
24 conditions that all of a sudden it has to -- it is
25 exposed to a situation that the designers didn't think

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 about, and all of a sudden now it doesn't work right.

2 So what this approach does is tries to identify all
3 of those likely off-nominal conditions.

4 It takes for granted that if you are under
5 nominal conditions, the failure -- the likelihood of
6 failure of the software is very low, and that is not a
7 big issue. Okay. And that, in fact, it is really
8 just under the off-nominal conditions that you want to
9 try and determine the failure rate or probability.

10 MEMBER BLEY: I would just urge you not to
11 be frightened by the "all."

12 MR. KURITZKY: Yes, that's --

13 MEMBER BLEY: To rote "all" into something
14 controllable and useful.

15 MR. KURITZKY: Right, right. A good
16 point. But just to explain, on this approach, so they
17 identify likely, essentially, hardware failures that
18 could impact -- you know, that puts you in a context
19 that the software is not used to seeing. And then,
20 what they do is they have a simulator, so they can go
21 in and set up that context, and then they can run a
22 whole bunch of cases, varying the applicable
23 parameters around.

24 So they essentially get a demand failure
25 probability for that software to be able to operate

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 under that condition. And then they can, you know,
2 piece all of those together. The probability of
3 failure of that -- whatever that context was times the
4 software failure probability.

5 MEMBER BLEY: And plus our computing
6 capability, something like you described. Even with a
7 fairly large number of cases, this might not be
8 prohibitive like it would have been a few years ago.

9 MR. KURITZKY: Right. But there is --

10 CHAIRMAN STETKAR: Or even as a contextual
11 thought process to get your hands around -- even if
12 you don't have to go run that simulator.

13 MR. KURITZKY: Right. But if you do want
14 to generate the numbers, you have to: a) have a
15 simulator, which unfortunately is something that we're
16 in the nuclear field, you know, we're not probably
17 going to have one. And then, also --

18 CHAIRMAN STETKAR: Build the box.
19 Eventually you can fill it with numbers.

20 MR. KURITZKY: Right. So anyway, to get
21 back to the -- so what they do here in CSRM is
22 actually it is -- they use a method to identify the
23 failure paths or what would be the different
24 conditions you need to consider for the software in
25 off-nominal cases, and they use the dynamic flowback

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 method, the same one that was used for the dynamics --
2 because the company that did that asked -- a company
3 out of California. The company that does the CSRM
4 methods, also the one that was the subcontractor to
5 ask about doing the DFM approach in that other study.

6 MEMBER SIEBER: No wonder he is not here.

7 MR. KURITZKY: Sergio Guarro, right.

8 So --

9 (Laughter.)

10 MEMBER SIEBER: He couldn't make it.

11 MR. KURITZKY: He specifies that you do
12 not have to use DFM in order to identify the various
13 contexts to go test, but they have the software with
14 that, they are familiar with it, so that's what they
15 use in their test case. So they use the DFM to
16 identify those cases. Then, they use that simulator
17 to try and generate the failure data.

18 As Meng mentioned, if they don't have that
19 data, if you don't have a simulator or the data, they
20 are going to use just the standard -- you have to go
21 to some other type of quantitative software
22 reliability method, test-based, you know, Bayesian
23 Belief, that is something else to just stick it in.
24 So in that regard it really wasn't a separate QSRM.

25 It is an overall method for modeling that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 includes QSRM in it, but it -- outside of this testing
2 with the simulator on the context-based testing it
3 really wasn't a separate QSRM. But, nonetheless,
4 because it is something that NASA had been pursuing
5 quite heavily, it does have a lot of association with
6 the work we are doing.

7 We wanted to at least have it, and we have
8 reviewed it in this report, even though it wasn't
9 purely a QSRM.

10 That's it.

11 CONSULTANT HECHT: So it is basically a
12 form of accelerated testing.

13 MR. KURITZKY: Yes, that --

14 CHAIRMAN STETKAR: When used in that
15 context --

16 MR. KURITZKY: Right.

17 CHAIRMAN STETKAR: -- that's right.

18 MR. KURITZKY: Right.

19 CHAIRMAN STETKAR: But there might be
20 elements of the thought process that are useful for
21 other --

22 CONSULTANT HECHT: It is an integrated
23 hardware-software approach, because what you're saying
24 is basically tell me what the abnormal system states
25 are. And if I can determine what the probabilities of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 those abnormal system states are, and then I determine
2 the probability -- you know, some kind of upper limit
3 on my failure rate in that state, then I guess the
4 total probability failure or -- is the probability of
5 that state occurring in the system times the
6 probability of the software responding properly, or
7 improperly, to give you a failure.

8 MEMBER ARMIJO: But if the software isn't
9 tested with that abnormal input, then you don't know
10 how it will respond. So, you know, and I heard now
11 that there is no -- software is kind of tested to
12 nominal --

13 CONSULTANT HECHT: No, software can be
14 tested and should be tested under abnormal states
15 and --

16 MEMBER ARMIJO: Or it is like a stress
17 test in the material --

18 CONSULTANT HECHT: Every safety-critical
19 standard is going to tell you to do that.

20 MEMBER ARMIJO: Yes.

21 CONSULTANT HECHT: I think what I saw in
22 the -- when I read the report on that satellite, I
23 forgot which satellite it was, it was -- was simply
24 that they have a formal way of showing how they got
25 there, got the abnormal states. That's worth

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 something.

2 MR. KURITZKY: And that is the DFM part of
3 it actually is what -- under CSRM, it was actually DFM
4 application that identified the states.

5 Anyway, I'm sorry, go ahead.

6 MR. YUE: Other QSRMs, here we have three
7 of them. The first one is so-called metrics methods,
8 and this kind of method estimated the software
9 reliability using individual software engineering
10 measures. It's SEMs.

11 From our review, one of the key
12 inconsistencies we found is the application. For
13 example, it does claim you should make use of -- it
14 should account for the facts of other SEMs when you
15 are doing assessment, but in this NUREG and -- in 6884
16 it is just using individual SEMs in the application.

17 Another one is a rule -- a standard-based
18 method, basic IEC 61508. And it assigns the
19 relationship between qualitative requirements and
20 quantitative requirements of SIL level, S-I-L, SIL
21 level 123 or something.

22 The issue with this method is this
23 assignment is kind of subjective, and it needs to be
24 further validated or investigated.

25 The last one is not really -- also, it is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 not a QSRM method. It is N-version programming,
2 although it does attempt to address the common cause
3 issue in the software development. And the N-version
4 program, basically, it follows the same requirement
5 and specification, but it gives the task to different
6 development teams, so they can develop different
7 software to implement at the same specification here.

8 The results has shown that it does improve
9 the reliability in terms of addressing the common
10 cause failure, but the issue is -- it is difficult to
11 quantify how much impact it might have on reduction of
12 the common cause failure probability, and also,
13 different versions of the software that might not fall
14 completely independently.

15 For example, you might have -- because
16 they are following the same specification, if the
17 specification is too detailed, a different development
18 team, they might steal -- develop the software with
19 the same problem. This limits the diversity of the N-
20 version program here.

21 MR. KURITZKY: Louis, you wanted to --

22 CHAIRMAN STETKAR: You're up.

23 MR. KURITZKY: Last one.

24 MR. CHU: Okay. I have just two slides
25 providing a summary. Of these QSRM we look at, most

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 of them were not developed specifically supporting --
2 for supporting modeling of digital systems to be
3 integrated at a nuclear powerplant. However, they do
4 assume a failure rate or failure probability of the
5 software and use that in making the decision they had
6 to make, like release of the software.

7 Many of these methods use empirical
8 formula, and they are not mathematical laws.
9 Therefore, the general applicability or accuracy of
10 this formula is limited.

11 The third bullet talks about the level at
12 which software failure rate and probability is
13 quantified. Most of them, not all, are looking at
14 system-level failures. In most cases, there is no
15 definition of, you know, what the specific data -- it
16 is just systems data is the event of interest.

17 MR. KURITZKY: So that kind of goes back
18 to the comment we had before about the level of detail
19 and breaking down the different failure modes. Many
20 of these approaches may not have the fidelity to go
21 down to a -- you might be able to apply it if you try
22 to at a lower level, but many of them -- it may be
23 just inherent in the nature of that approach that you
24 don't have that fidelity to go into separate failure
25 modes. So that could be one inherent limitation.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. CHU: BBN method has been said to be a
2 promising method, but, you know, the development of
3 such a model is subjective, especially keeping in mind
4 of the conditional independence embedded in such a
5 model.

6 Also, in one situation, Littlewood
7 published a paper showing a BBN in which some
8 counterintuitive results were obtained. So the --
9 this is to say you need to be very careful about the
10 dependency that is reflected in the structure of your
11 BBN. On top of that, development of such a model
12 requires expert knowledge and also elicitation of
13 experts in deriving conditional probability tables.

14 Test-based method used statistical method
15 and software testing, and operating data, if
16 available. But there are limitations of testing
17 method, and other QSRMs tend to use data. They all
18 try to use data or test data. This limitation of
19 test-based method is also applicable to other methods.

20 The most basic one is you collect some data, and use
21 it in the standards that -- of this method to quantify
22 software reliability.

23 An assumption is that these tests were
24 performed by sampling from the operational profile.
25 But if you look at the actual way testing is done, it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 may not be a good representation of what the real
2 operational profile is. The operational profile may
3 not be well known or may not be well defined.

4 I think for that reason it was the
5 experience of Sizewell B, a committee decided the
6 tests done on the system -- on the reactor protection
7 system cannot be used in quantifying system
8 reliability -- software failure probability of the
9 system.

10 The problem with the Frestimate is that
11 the data is not available. The detailed information
12 about the past projects are -- the information is
13 proprietary. It is not possible for us to look into
14 it and see if that was done right. I guess in general
15 the idea I think is a very reasonable one, but we
16 couldn't scrutinize the implementation of it.

17 MR. KURITZKY: I think these last four
18 bullets are just a repeat of what Meng ended up his
19 presentation with, so I don't think we need to go into
20 them one by one.

21 CHAIRMAN STETKAR: I do want to interrupt
22 you. Charlie, go on.

23 MEMBER BROWN: No, go ahead. I was going
24 to -- I was trying to address another test method that
25 didn't seem to be addressed in the report.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: Okay. Let --

2 MEMBER BROWN: Just to see if it had any
3 relevance to the discussion. So go ahead, and I'll --

4 CHAIRMAN STETKAR: In the report, I -- and
5 I haven't read the NUREG, so I'm not as sensitive as
6 you are to the limitations, but there is some
7 discussion of the general category of software
8 engineering methods, SEMs.

9 That is -- you know, as kind of a simple-
10 minded, poor farm boy, was intriguing to me because it
11 seemed to identify specific characteristics of the
12 software that could indeed I guess be tailored to be
13 application-specific without necessarily a very let me
14 call it "elegant" mathematical model for predicting
15 failures.

16 So it was -- it seemed encouraging in that
17 way, and yet the discussion seemed to say, "Well,
18 because I may not be able to treat subtle dependencies
19 between each of these metrics, I can't do it." In
20 other words, I can't be very precise with it.

21 I was wondering whether it -- how -- are
22 those methods applied in practice, and do they work
23 reasonably well?

24 MR. KURITZKY: I think I'll let --

25 CHAIRMAN STETKAR: I mean, and, you know,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we kind of challenged a couple of the other ones.
2 When I was sort of doing my mental ranking, this was
3 closer to the top than it was to the bottom. So, for
4 example, I was curious why I did -- it seems to be
5 closer to the bottom if I can read between the lines
6 in your --

7 MR. KURITZKY: I mean, I --

8 CHAIRMAN STETKAR: I know you haven't done
9 the evaluation yet.

10 MR. KURITZKY: Right, right.

11 CHAIRMAN STETKAR: So that's premature,
12 but --

13 MR. KURITZKY: Well, you've read between
14 the lines probably pretty well. I mean, how much
15 effort -- how much words it gets in the presentation
16 is probably a function of how much we think of it.
17 But I think that that's an area that does have some
18 possibility. I'm going to mention a couple of words,
19 and then I'm going to let Louis or Meng fill in the
20 gaps.

21 But, really, our concern there was that
22 they talk about having to consider multiple of these
23 metrics together in order to come up with an
24 appropriate characterization of the software and try
25 to come up with the likelihood of failure.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And their application they did in the
2 NUREG looked at them one by one individually, and
3 didn't do that. So that was more of an inconsistency.

4 We are not totally aware right now why that was done
5 that way, and so that's something we can explore.

6 In fact, that is -- one of the reasons why
7 I had that last box put on here is because I want to
8 say, "Hey, if this is what we are leaning towards,
9 what do you think?" And so I like that feedback,
10 because maybe that metrics method is something that
11 needs a little more attention.

12 It is one of the methods -- going back to
13 what someone had mentioned before, have these things
14 been tested out in the real world, or are these, you
15 know, academic exercises right now? That one is an
16 academic exercise.

17 CHAIRMAN STETKAR: Oh, okay.

18 MR. KURITZKY: But doesn't mean that it
19 isn't something that should be pursued. And so, you
20 know, gentlemen, you guys looked in more detail at
21 that approach. Is there anything about that approach
22 that would steer us away from it?

23 MR. CHU: Well, as we pointed out, the
24 inconsistencies, it is an issue. But the overall idea
25 of using software engineering measures to estimate

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 software failure -- software reliability is
2 reasonable.

3 You can actually look at that as something
4 similar to what Frestimate does, or similar to what
5 some people do using BBN, in the sense that you look
6 at the quality -- how good a job you have done in
7 developing the software. And, in that sense, you can
8 kind of link these different methods together.

9 You asked a question about activities
10 carried out, how good a job they have done in doing
11 so, and somehow use that information to reflect that
12 in your model. But when it comes to the specific
13 metrics method, one of the methods that we look at is
14 said to be based on defect density.

15 Looking at it, it looks like it is -- it
16 is another white box testing method. Basically, you
17 look at paths and nodes inside the software. You look
18 at the structure of it, and then you estimate how
19 likely -- how frequently they go to the path or how
20 frequently you visit the node. And then, for each
21 path or node, you somehow estimate or do tests to find
22 failure rate -- failure probability associated, and
23 you aggregate it to get a system-level reliability.

24 CHAIRMAN STETKAR: Okay.

25 MR. CHU: That -- in essence, it is a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 reasonable thing --

2 CHAIRMAN STETKAR: Let me ask -- Myron,
3 since I am well out of my knowledge base -- have you
4 jumped into any of --

5 CONSULTANT HECHT: Yes.

6 CHAIRMAN STETKAR: -- those types of
7 methods?

8 CONSULTANT HECHT: Yes, I have, and I was
9 just trying to -- and I am quite familiar with the
10 work, and I can't remember her name -- who was the --

11 CHAIRMAN STETKAR: Carol Smidts?

12 CONSULTANT HECHT: Yes, Carol Smidts. I
13 started out with some work being done at Lawrence
14 Livermore, and then Carol took it over, and Carol
15 basically started -- Lawrence started with 40 I think
16 software engineering methods and then reduced it to --
17 I mean, Carol reduced it to five, and there it stood.

18 I was just thinking about everybody wants
19 to do this so badly, and the reason why everybody
20 wants to do this is because you can measure effort.
21 You can measure, did people test? Did people do peer
22 reviews? Did people, you know, do all of the trace
23 requirements, manage the configuration? All of those
24 things that relate to good software engineering.

25 Furthermore, these same methods -- you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 know, we are interested in failure rates or failure
2 probabilities and output. But another even more
3 important output to the community as a whole is cost,
4 and there are at least two major families of cost
5 prediction models, one which is called SEER/SEM
6 developed by Galorath, another one which is CoCoMo
7 developed by the University of Southern California
8 under Barry Bean. And there is also a third one which
9 I am forgetting, and I apologize.

10 But all of those methods basically assumed
11 that there is some kind of relationship between the
12 way in which software is developed and either its cost
13 or its schedule or its reliability.

14 For costs and schedule, people use it
15 because, quite honestly, whether it costs \$3 million
16 to develop or \$4-1/2 million to develop is not a life-
17 critical situation. It may cost somebody their
18 career, but it is not life-critical.

19 With respect to going into safety, I was
20 just thinking about an example, and this is one
21 example which will demonstrate I think the difficulty
22 of the approach.

23 There is a very highly recognized standard
24 in the avionics community called RTCA DO 178B now, and
25 that is basically the standard that is used in the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 civil aviation industry for developing software. And
2 what they have is they have a number of levels. They
3 go from Level A through Level E, where Level E is
4 basically inconsequential, D is minor, C is major, B
5 is hazardous, and A is catastrophic.

6 So if we look for -- it has 66 what they
7 call objectives, which are basically software
8 engineering or software development methods,
9 everything from making sure that you don't have any
10 dead code in the system to making sure that the
11 requirements are traceable all the way into the
12 software structure, as just being opposed to the
13 tester, things like that.

14 But the interesting one is, if you go from
15 10^{-5} to 10^{-7} probability, which is going from Level C
16 to Level B, or Level B to Level A, there is only one
17 method which is different from going 10^{-7} per hour
18 probability to 10^{-9} , and that is a certain kind of
19 structural testing called modified condition decision
20 coverage.

21 CHAIRMAN STETKAR: Okay.

22 CONSULTANT HECHT: The standard says
23 specifically nothing that we say here about going from
24 Level B to Level A can be used to infer the
25 reliability of the software. It prohibits it. Yet,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 in fact, that's what we are doing. That's what the
2 FAA is doing, because they are saying that that one
3 additional test method is going to reduce the failure
4 probability by a factor of --

5 CHAIRMAN STETKAR: A hundred.

6 CONSULTANT HECHT: -- a hundred. People
7 want to do that. I mean, we do want to do that very
8 badly, but I don't think we can.

9 CHAIRMAN STETKAR: Okay.

10 MEMBER BROWN: Because of cost or --

11 CONSULTANT HECHT: No, no. It is -- there
12 is no basis. Nobody can say that because you are --

13 CHAIRMAN STETKAR: Just by inference,
14 that --

15 CONSULTANT HECHT: It's so small.

16 CHAIRMAN STETKAR: Okay, thanks. I just
17 wanted to get some feedback on that.

18 We are getting close to time here, and --
19 Rob? Rob, speak.

20 MR. AUSTIN: Rob Austin, EPRI. Just two
21 informational points and then a question. The first
22 is I will look into the status of the EPRI review on
23 this and at least let you know how come we didn't give
24 you anything.

25 We do have an upcoming deliverable this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 year, which is an offshoot of work that was actually
2 done a couple of years ago under the Task Working
3 Group format on estimating reliability for use of PRA
4 of digital systems. I'm not sure of the details.
5 I'll get those to Alan. I believe it is based upon
6 operational experience from one of the European
7 fleets, so real data. But I will get some information
8 on that.

9 And then, as a question for possible
10 methods, did you look at the population of human
11 reliability methods? And the idea that, basically, at
12 the end these are typically people making mistakes as
13 opposed to something else happening.

14 MR. KURITZKY: Yes, I will let Louis field
15 that. I know in our initial discussion during one of
16 the earlier NUREGs we have talked about software
17 failure, we proposed things like the failure
18 likelihood index method, you know, FLIM, or Bayesian
19 Belief type approaches, which are things that are
20 considered in the HRA-type world.

21 But, Louis, did you want to --

22 MR. CHU: Yes, you've pretty much said it.
23 We -- at one point we suggested using some kind of
24 failure likelihood index method, using the similarity
25 between human reliability and software reliability.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 In such a model, you are looking at factors that
2 affect reliability of software, and then you calculate
3 some index and convert it into some kind of failure
4 rate or failure probability. That is kind of learning
5 from the human reliability analysis.

6 MR. KURITZKY: Is that reflected by any of
7 the other approaches we have here, or is that like a
8 totally distinct approach that we would want to
9 consider, or we made a conscious decision not to
10 consider it.

11 MR. CHU: I guess it is not a QSRM. It is
12 an HRA method. Therefore, we didn't quite include it
13 in our review, but it is certainly another possible
14 method. That way, you can account for probability of
15 developing activities, for example, and expert
16 opinion. They can all come in in that kind of
17 framework.

18 MR. KURITZKY: I think -- and the common
19 thing with an approach like that, with the SEM, with
20 the metrics methods, with the Frestimate, all these
21 things, it comes down to using qualitative
22 information, because it is available and we can
23 measure it, and it is something that we just know
24 intuitively it has got to be -- if we do a good job
25 with that, it should be -- your software should be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 better.

2 But it is that conversion, it is that --
3 taking that qualitative information and flipping it to
4 a number is where it gets tough -- that anchor point
5 or whatever it is that you are going to use to make it
6 from quantitative to qualitative. And I think that
7 is, unfortunately, a common problem with most of those
8 approaches.

9 CHAIRMAN STETKAR: Let's see. We've got
10 -- I'm going to try to get in this -- you know, maybe
11 five minutes early. I don't think I'll make it, but
12 see if we can wrap up pretty quickly here.

13 Dennis, you had -- a couple of questions.
14 Your introduction said that the final version of the
15 letter report, which I assume will include CSRM and
16 input from the peer review, will be available summer
17 2010. Summer started a couple of days ago, so --

18 (Laughter.)

19 -- when during the summer?

20 (Laughter.)

21 MR. KURITZKY: More towards the solstice
22 definition of "summer."

23 (Laughter.)

24 CHAIRMAN STETKAR: All right.

25 MR. KURITZKY: September.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: If that's the case, is
2 there any way that we can get a -- the current version
3 of the draft report with the CSRM folded into it?

4 MR. KURITZKY: Well, we don't actually --
5 see, right now, in fact, as soon as we walk out of
6 this meeting and have lunch, Louis and I are going
7 back to huddle for the next couple of days to respond
8 to comments. So we are working on that. We are
9 reviewing that -- we are adjusting that report right
10 now, accounting for the comments that came in.

11 CHAIRMAN STETKAR: Okay. Why don't we
12 just -- Christina, if you could --

13 MS. ANTONESCU: Yes.

14 CHAIRMAN STETKAR: -- you know, work with
15 them, keep in touch, so -- the earlier we could see
16 that, it sounds something interesting, and it isn't
17 something that we have seen, so --

18 MR. KURITZKY: Right. We can --

19 CHAIRMAN STETKAR: -- we would appreciate
20 kind of a -- you know, as soon as we can see it, it
21 would be useful I think.

22 MR. KURITZKY: Right. One of -- the first
23 point we will get to is where we are going to send it
24 for management review, hopefully in a few weeks,
25 depending on whether or not we continue that same

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 version for --

2 CHAIRMAN STETKAR: Yes, just work with
3 Christina and see --

4 MR. KURITZKY: Okay.

5 CHAIRMAN STETKAR: -- see what we can get.

6 The second thing is that on your agenda
7 here it says you are going to issue a draft of the
8 NUREG some time in the fall.

9 MR. KURITZKY: It's kind of -- that is
10 probably going to slide correspondingly, but it --

11 CHAIRMAN STETKAR: Okay.

12 MR. KURITZKY: -- will be some time in --

13 CHAIRMAN STETKAR: Okay. Because I think
14 this is -- I feel really badly because we got
15 truncated, you know, yet again to a half day. I think
16 that there is quite a bit of interest among the
17 Subcommittee members on what you have in hand now and
18 the direction that you are headed. And I would not
19 like to let our subcommittees' meetings, you know, be
20 one per year.

21 I think I'd like to schedule something in
22 the fall timeframe, but I want to make sure that we --
23 you know, we know what we'll have at that time, so it
24 is premature to schedule anything right now, but I
25 think -- I think we would probably like to look at

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 another Subcommittee meeting.

2 And depending on what is available,
3 perhaps a full day meeting, but I guess I would
4 encourage, Christina, if you can work with them and
5 see, you know, over the next month or so, see what
6 might be available and what we can actually have on
7 our plate.

8 MR. KURITZKY: Right. I think our
9 limiting factor there is that the Committee typically
10 -- or somebody typically wants to have a product to
11 look at. So that's why we scheduled it for after that
12 draft NUREG is available, and that is --
13 unfortunately, we will have no product to give you
14 until that draft NUREG is --

15 CHAIRMAN STETKAR: Well, that's -- and
16 that's why I was asking about what "fall" and what
17 "summer" means.

18 MR. KURITZKY: Right.

19 CHAIRMAN STETKAR: But it is -- the
20 message is I don't want to wait until another year
21 goes past before we have at least some sort of
22 interchange.

23 MR. KURITZKY: Okay.

24 MEMBER RAY: John, before you bang the
25 gavel --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN STETKAR: No, I was going to go
2 around the table as we usually do. I just wanted to
3 get sort of the planning schedule.

4 MEMBER RAY: -- I wanted to ask him a
5 question, but if I can do that --

6 CHAIRMAN STETKAR: Sure.

7 MEMBER RAY: -- when we go around, that's
8 fine.

9 CHAIRMAN STETKAR: Yes, let's do it going
10 around the table. John?

11 MEMBER SIEBER: No.

12 CHAIRMAN STETKAR: Myron, I'm going to
13 skip you. You're a consultant.

14 Harold?

15 MEMBER RAY: We talked about testing a
16 lot. I am out of my depth when we were talking about
17 this mostly, but I have one question that sometimes
18 gets a surprising answer when I ask it. Does the
19 testing assume, for example, an external event like a
20 loss of offsite power or something that causes a lot
21 of things to happen at the same time, so that you are
22 looking at information overload or interactions that
23 occur simultaneously in assessing the probability that
24 you are modeling.

25 MR. CHU: In case of our feedwater control

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 system, we consider a steady-state condition under
2 which we model the system. No testing is involved.

3 When it comes to system like reactor
4 protection system, we were reading about Ocone
5 digital upgrade, trying to find out what tasks are
6 involved. I would characterize that kind of testing
7 would be functional testing. You know, in this
8 condition, you need to have a trip, a large LOCA, and
9 you have a trip.

10 MEMBER RAY: So the PRA isn't looking at
11 the reliability of the system given an external event?

12 MR. CHU: Okay. If you look at it that
13 way, the word "context" comes into play. That is, for
14 example, for reactor protection system, given the
15 external event, the first question you ask in a PRA is
16 reactor protection, do you have a reactor trip?

17 So you can say this is a context that
18 challenges the software of the RPS. But how the
19 system is tested I don't know. I don't have the
20 detailed knowledge, but it --

21 MEMBER RAY: Well, that's why I say I
22 often get a surprising answer when I ask this
23 question.

24 MR. KURITZKY: Well, I think you asked the
25 question, how does it get tested?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER RAY: Yes. Basically, I'm
2 interested in when we develop the information that you
3 are seeking to obtain, is it applicable to risk
4 assessment given external events that the plant is
5 designed to withstand?

6 MR. KURITZKY: You see, the thing is, the
7 people doing the testing -- do you want to --

8 CHAIRMAN STETKAR: Be careful. Are you --

9 MEMBER RAY: I'm done.

10 CHAIRMAN STETKAR: No. In the context of
11 external events, are you just talking about inputs
12 from any combination of signals, or are you talking
13 about external events and the jargon that PRA people
14 talk about, external events?

15 MEMBER RAY: I'm talking about loss of
16 offsite power. We were talking about stage, did we
17 define the abnormal stage sufficiently when we were
18 looking at the reliability. You know, like I say, I'm
19 out of my depth. My point is --

20 CHAIRMAN STETKAR: The context could be a
21 small LOCA with a stuck-open relief valve, so you get
22 a cooldown.

23 MEMBER RAY: Right.

24 CHAIRMAN STETKAR: So don't necessarily
25 think fires, floods --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER RAY: Right.

2 CHAIRMAN STETKAR: -- you know, tornadoes
3 or -- but it could also be them.

4 MEMBER RAY: Right.

5 MR. KURITZKY: The point is, in the model,
6 in a PRA model, how we would tend to want to model it
7 is we would -- that would be the context in which we
8 would look at the software.

9 So if we had the RPS software, and we were
10 going to consider its failure likelihood, it is the
11 first node in the event tree, we could theoretically
12 have a separate quantification for that node for some
13 different initiating event, because they would
14 represent different contexts, whether it's a loss of
15 offsite power or a feedwater trip or whatever,
16 earthquake, we might have a different value here.

17 But, in reality, when you ask, "How are
18 these things tested?" we are not doing -- the PRA
19 model isn't going to do the testing. That is the
20 software developer or the device to whatever, and what
21 they are -- how they are going to go about testing
22 that system, and whether they are going to consider
23 all of those different conditions or contexts when
24 they test, that I can't tell you. I would like them
25 to, but, I mean, it's not my call.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER RAY: Well, all right, but --

2 MEMBER SHACK: With your guidance, we will
3 eventually get to that point presumably.

4 MEMBER RAY: Yes. When you come back here
5 with the guidance, I am going to ask you again, and --

6 MR. KURITZKY: Or the guy who replaces me
7 when I'm retired.

8 (Laughter.)

9 MEMBER RAY: All right.

10 CHAIRMAN STETKAR: I remind the
11 Subcommittee that you guys eat, I don't.

12 MEMBER BROWN: I just want to amplify
13 Harold's question, if I could, okay, since it is not
14 my turn yet.

15 CHAIRMAN STETKAR: Right.

16 MEMBER BROWN: But loss of power in these
17 systems creates some unusual circumstances as all the
18 various level power supplies decay, because your
19 different memory devices, micro -- they all start
20 operating in different modes, if they start shutting
21 down or not processing data in the normal manner.

22 So it can create some very unusual states
23 in terms of what it is starting to tell the rest of
24 the systems to do. And I'm not saying that there's an
25 answer for that. I'm just saying that relative to the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 context of the question it is a good question, and
2 I'll bet you the testing that we do doesn't really
3 address that for the most part. It's very difficult
4 to do that, because it's always different every time
5 you power it down. Abrupt, gradual, what? It's very
6 different.

7 MEMBER SIEBER: It looks like analog is
8 best.

9 MEMBER BROWN: So anyway, I will wait now.
10 Go ahead. Sorry.

11 CHAIRMAN STETKAR: Dennis?

12 MEMBER BLEY: All this talk about context
13 makes me hope you will give a little more thought to
14 those contextual methods and ways you might make them
15 practical. And I think that is really worth a look.
16 You might be able to do some of the same thing within
17 Bayesian Belief Networks, and probably you can. But
18 that idea seems an important one to me. Otherwise, I
19 -- thanks for the presentation. There were a lot of
20 good things presented.

21 CHAIRMAN STETKAR: Sam?

22 MEMBER ARMIJO: Yes, I just had a question
23 on -- you went through a process with your expert
24 panel to come up with these 10 desirable
25 characteristics of what these QSRMs are supposed to be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 able to do. I was just wondering if the final two
2 methods that you are looking at have to meet these
3 characteristics, or did you -- did you rank them?

4 MR. KURITZKY: Well, just as a point of
5 clarification, we didn't actually have -- the expert
6 panel didn't actually come up with those. That was
7 based on the BNL --

8 MEMBER ARMIJO: Okay.

9 MR. KURITZKY: But, nonetheless, in this
10 version of the report, in this version at this stage
11 of the project, we have not done that. They are doing
12 that now -- right now as part of the next phase of the
13 work where they are actually comparing the -- they are
14 going to make a table where it compares all of the
15 different approaches to those desirable
16 characteristics, and then theoretically will come up
17 with what we feel are the one or two most, you know,
18 promising approaches to pursue.

19 Right now, I said just initially I wanted
20 to throw those two up there, because I wanted to see
21 what people thought about those and get any initial
22 feedback. Like Dr. Stetkar mentioned, there is a time
23 lag between when we're doing work and when we come to
24 the Committee. And to the extent that we could hear
25 something now, it would be a lot better than hearing

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 it eight months down the road. So, but no, we haven't
2 done that comparison yet.

3 MEMBER ARMIJO: Okay. Thanks.

4 CHAIRMAN STETKAR: Charlie.

5 MEMBER BROWN: Relative to -- two things.
6 One, relative to that you one you didn't any comment,
7 if -- when I read the report and went through -- and I
8 see your suggestion up there as to where you'd like to
9 go -- it didn't seem like those popped up as the most
10 desirable ways to go. They seem to be as part of the
11 total mish-mash of everything else. They were all
12 relatively undesirable. I'm choosing that -- that's
13 humor, okay?

14 They are all relatively difficult to
15 predict in terms of what their performance would be,
16 and there is down sides to all of them, and that they
17 -- those two just did not pop up in my own mind as
18 they went -- I'm not sure what I would have picked
19 either.

20 MR. KURITZKY: That was going to be my
21 follow-on comment.

22 MEMBER BROWN: Yes, I was going to say I
23 think that --

24 CHAIRMAN STETKAR: What Alan was saying is
25 that they would appreciate a little bit of feedback if

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there was something that they --

2 MEMBER BROWN: Yes, I couldn't figure it
3 out from some of the things. I didn't come to that
4 conclusion.

5 The second point relative to the testing
6 methods, I am a test guy, okay, I like tests as
7 opposed to what I call more cerebral approaches to
8 doing things. Hammer and tongs is nice and
9 comforting. And there are test methods that are
10 complex. You talked about plant interactions, which
11 is a concern, and, you know, do they reflect the plant
12 operational modes in terms of how that feeds into the
13 way the software performs.

14 And there are methods of testing where you
15 take a simulator that takes the reactor plant and the
16 balance of plant all together, and you feed a full
17 suite of all of the I&C through emulators that then
18 generate the outputs, looking like the detectors would
19 be, along with all of the appropriate switches from
20 the main control room.

21 And then, you then can hook all of that
22 stuff up. It has got to be the real stuff and the
23 real software, and you then run it through all of the
24 plant operations -- the startup/shutdowns, all of the
25 other types of things, losses of this, losses of that,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 power-downs, everything else. You get some very
2 interesting results when you do that. It's very
3 complete.

4 It does work. I can only say that from
5 personal experience. But it does require a tremendous
6 amount of effort, but you get probably the most
7 complete -- in my personal opinion, a very, very
8 complete look at how the plant and all of the --
9 because now you have defined your conditions. You
10 know, what switches do what, what you can put them in,
11 all kinds of conditions, and there is a lot of
12 variations/combinations.

13 But they are finite in reality and --
14 relatively finite. Okay. I wanted to caveat that.
15 Okay? It gets the stuff that is out in the plant into
16 the testing mode, which is more difficult to do in the
17 -- what I would call the more cerebral approach to
18 doing this with models.

19 Go ahead.

20 MEMBER SHACK: It sounds to me like all of
21 us sort of liked this context notion. We have
22 different ways of expressing it, but somehow this
23 thing has to capture context and make sure that we
24 look at a wide enough range of context to do it.

25 MR. KURITZKY: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER SHACK: I have a simple-minded
2 question. You have all sorts of slides on continuous
3 SRGM, and then you recommend discrete.

4 (Laughter.)

5 Can you give me a one-paragraph
6 description of discrete?

7 MR. KURITZKY: I'll let Louis do that.
8 But the simple thing is it's going to give us the
9 demand failure probability as opposed to the failure
10 rate.

11 MEMBER SHACK: Oh, okay.

12 CHAIRMAN STETKAR: It is the mathematical
13 conversion of lambda into not lambda.

14 MEMBER SHACK: Okay. That's good enough.
15 That's good enough.

16 CHAIRMAN STETKAR: I think, as a wrap-up,
17 I will -- and I echo both Dennis' and Bill's interest
18 in the CSRM. I mentioned earlier the SEM, because
19 that seemed to be a pragmatic, simple approach, but I
20 am not well enough founded on, really, its
21 limitations, because they weren't very well described
22 in the letter report.

23 But in terms of, you know, the population
24 of things, I actually -- you know, personally, I
25 wasn't in favor of the SRGM, but I couldn't be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 convinced otherwise.

2 MR. KURITZKY: Okay.

3 CHAIRMAN STETKAR: And with that, Bill
4 Stillwell, if you are still on the line, sorry, you
5 don't get a chance to talk, but bye.

6 And, with that, I would like to thank you
7 all for the presentation. I think it was really
8 informative. I think you did a really excellent job
9 under the time constraints, and we really appreciate,
10 you know, your difficult work to kind of compress all
11 of this into a four-hour time period.

12 And I really look forward to -- Dennis?

13 MEMBER BLEY: Two quick things. One, I
14 was going to -- if Bill is still listening to you, if
15 he has written comments, we would love to see them.

16 CHAIRMAN STETKAR: Ah, that's a good --

17 MEMBER BLEY: And are you going to ask for
18 public --

19 CHAIRMAN STETKAR: Thank you for reminding
20 me. Appreciate that. Does anyone in the audience
21 have any more comments?

22 (No response.)

23 Okay. And I understand there will be
24 public meetings on this, so I appreciate it, and look
25 forward to hopefully a little bit more time to get

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 together and continue the discussion some time in the
2 fall.

3 And with that, we are adjourned.

4 (Whereupon, at 12:38 p.m., the proceedings in the
5 foregoing matter were adjourned.)

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



Digital I&C PRA

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 23, 2010

Alan Kuritzky
Division of Risk Analysis
Office of Nuclear Regulatory Research
(301-251-7587, Alan.Kuritzky@nrc.gov)

Outline of Presentation

- Background
- Objective
- Digital system risk modeling activities
- Milestones and future interactions

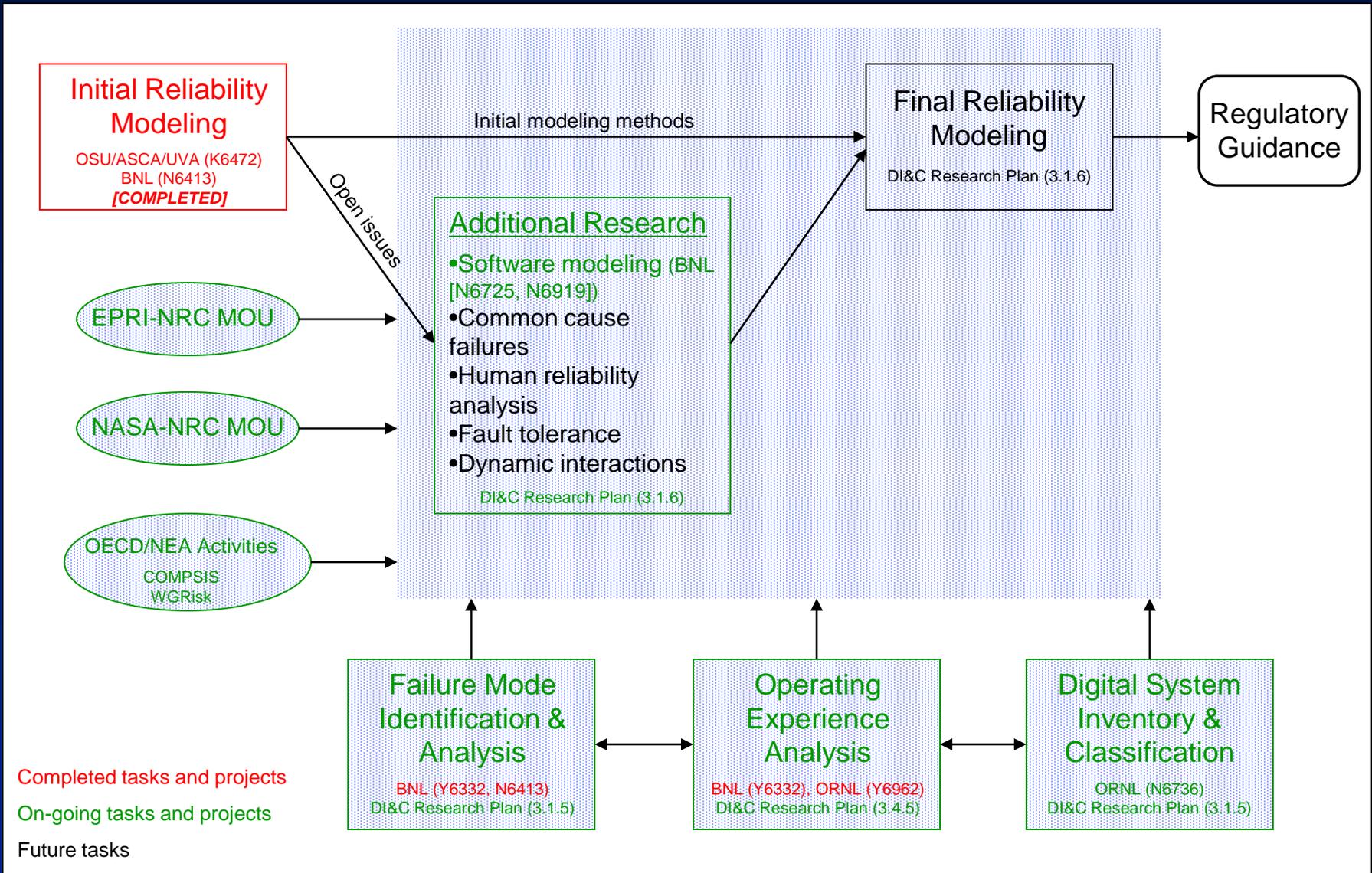
Background

- Current licensing process for digital systems is based on deterministic engineering criteria
- Commission's 1995 probabilistic risk assessment (PRA) policy statement encourages use of PRA to the extent supported by the state-of-the-art
- Risk-informed analysis process for digital instrumentation and control (DI&C) systems has not yet been satisfactorily developed

Objective

- Identify and/or develop methods, analytical tools, and regulatory guidance for:
 - Including digital system models into nuclear power plant (NPP) PRAs
 - Using information on the risks of digital systems to support NRC's risk-informed licensing and oversight activities

Digital System Risk Modeling



Current and Near-Term Activities (1 of 3)

- NRC/Brookhaven National Laboratory (BNL) currently pursuing incorporating software failure into digital system reliability models
 - For the purposes of this research, one way that software failures can be thought of is as “faults or inadequacies of the software that, under certain conditions, result in, or contribute to, the host system failing to accomplish its safety function or initiating an unwanted action”
 - Workshop on philosophical basis (completed)
 - Basis was established for modeling software failures probabilistically
 - Review of quantitative software reliability methods (QSRMs)
 - Desirable characteristics for QSRMs for use in PRAs
 - Identification of QSRMs
 - NRC-sponsored research
 - NASA-sponsored research
 - Research performed at international organizations
 - Open literature research
 - Major categories of reviewed QSRMs
 - Software reliability growth methods
 - Bayesian belief network methods
 - Test-based methods
 - Other methods (e.g., Frestimate and Context-based Software Risk Model [CSRM])
 - Recently completed peer review

Current and Near-Term Activities (2 of 3)

- NRC/BNL currently pursuing incorporating software failure into digital system reliability models (continued)
 - Plan to develop one or two technically sound approaches to quantifying software failures in terms of failure rates and probabilities
 - Assuming such approaches can be developed, plan to apply them to an example software-based protection system in a proof-of-concept study
- Initiate research to address other “gaps” in the state-of-the-art
 - Data, data, data
 - Common cause failures
 - Fault tolerant features
 - Dynamic interactions
 - Human reliability analysis

Current and Near-Term Activities (3 of 3)

- Activities that support DI&C PRA
 - Digital system inventory and classification (ORNL – N6736)
 - Preliminary classification/categorization structure of digital systems in current and future NPPs
 - Inventory of digital systems and components used in current and future NPPs
 - Failure mode identification and analysis
 - Electric Power Research Institute (EPRI)-NRC Memorandum of Understanding (MOU) – Failure analysis guideline
 - National Aeronautics and Space Administration (NASA)-NRC MOU – Technical Interchange Meeting (Summer 2010)
 - Organisation for Economic Cooperation and Development (OECD) Nuclear Energy Agency (NEA) Working Group on Risk Assessment (WGRisk) – Failure mode taxonomy
 - NRC Digital System Research Plan FY 2010-FY 2014 – Task 3.1.5 (Analytical Assessment of DI&C Systems)
 - Operating Experience Analysis
 - OECD/NEA – Computer-based Systems Important to Safety (COMPSIS) project
 - NRC Digital System Research Plan FY 2010-FY 2014 – Task 3.4.5 (Operating Experience Analysis)
- Caution: It is expected that reliability models of digital systems (including software) can be developed and quantified, but it is not clear whether it will be practical and useful to do so.

Milestones and Future Interactions

- Issue final letter report on review of QSRMs (Summer 2010)
- Issue draft of first NUREG/CR for peer review (Fall 2010)
 - Selection of QSRMs for trial application
 - Description of proof-of-concept system
 - Description of how selected QSRMs will be applied to proof-of-concept system
- Brief ACRS Digital I&C Subcommittee (Winter 2010/2011)



APPLICATION OF TRADITIONAL PRA METHODS TO A DIGITAL FEEDWATER CONTROL SYSTEM

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 23, 2010

Tsong-Lun Chu
Brookhaven National Laboratory
(631-344-2389, chu@bnl.gov)

Brookhaven National Laboratory
U.S. Department of Energy

- Previous NRC projects (2004-2009) have:
 - Identified desirable characteristics for reliability models of digital systems
 - Applied various probabilistic reliability modeling methods (traditional and dynamic) to a digital feedwater control system (DFWCS)
- This research is documented in a series of NUREG/CR reports
 - Traditional reliability modeling methods (NUREG/CR-6962 [2008], NUREG/CR-6997 [2009])
 - Brookhaven National Laboratory (BNL)
 - Dynamic reliability modeling methods (NUREG/CR-6901 [2006], NUREG/CR-6942 [2007], NUREG/CR-6985 [2009])
 - Ohio State University (OSU), ASCA, University of Virginia

[Note: For the purposes of this research, dynamic methods are defined as those that explicitly attempt to model (1) the interactions between a plant system and the plant's physical processes, and (2) the timing of these interactions.]

NUREG/CR-6997

Key Findings (1 of 2)

- The level of detail of the DFWCS model is adequate for capturing many of the system design features, while not being too complicated to be developed and solved.
- However, at this level of detail, the study requires a deterministic simulation tool (model) to determine the component-level sequences resulting in system failure.
 - This simulation tool should not be confused with the simulation of the controlled plant processes used in developing the “dynamic” models of the DFWCS.
- The use of the simulation model to determine component-level failure sequences reduces the event tree/fault tree (ET/FT) and Markov models solely to means for quantifying system reliability.
- Performing a failure modes and effects analysis and running the simulation tool revealed two failure scenarios (one involving differences in signal delay times, and the other involving both central processing units [CPUs] operating in tracking mode) that were not identified by the plant hazards analysis.



NUREG/CR-6997

Key Findings (2 of 2)

- The order in which component failure modes occur can affect the impact the failures have on the system.
- The Markov method can easily account for the order in which component failure modes occur, and was used for quantification.
- Due to modeling limitations (including lack of a model for incorporating software failure), as well as the weakness of publicly available digital component failure data, the current model and results cannot be used to support decision making.
- The approach applied in this study to the DFWCS should also be applicable to protection systems.



NUREG/CR-6997

Automated Tool (1 of 3)

- The automated tool developed is a simulation model based on the software of the modules of the DFWCS.
- In this way, the performance of the software of the DFWCS given the occurrence of one or more component (hardware) failure modes is accounted for.
- This detailed model allows a realistic representation of the system.
- Interactions with the rest of the systems of the nuclear power plant are not included.
 - This is why the approach is considered “traditional,” as opposed to “dynamic,” per the earlier definition.
- The model could be expanded to include these interactions.



NUREG/CR-6997

Automated Tool (2 of 3)

- System failure is defined as loss of automatic control of the feedwater loop associated with the DFWCS.
- Given a combination of failure modes of components as input, the tool automatically determines whether system failure occurs or not using criteria provided by the analysts.
- The criteria specify the conditions that cause system failure.
- The tool was used to analyze:
 - 421 individual failure modes
 - 128,779 combinations of two failure modes
 - 36,844,679 combinations of three failure modes.

NUREG/CR-6997

Automated Tool (3 of 3)

- Timing of occurrence of failure modes is roughly approximated, i.e., one mode occurs after the other.
- The order in which failure modes occur was found to be relevant because of fault-tolerant features that cause automatic re-configuration of the system. For example:
 - A failure mode of the main CPU causes system failure, so it is a single failure.
 - Another failure mode of the main CPU does not cause system failure, but it is detected, and the backup CPU takes control of the system.
 - When the first failure mode occurs after the second, the system does not fail because the main CPU is not controlling.



NUREG/CR-6997

Areas of Potential Additional Research

- Improved approaches for defining and identifying failure modes of digital systems
- Software reliability methods for quantifying software failure rates and probabilities, and addressing software common cause failure
- Better data for hardware failures (both independent and common cause) and a break down of the failure rates by failure modes of digital components
- Methods and parameter data for modeling self-diagnostics, reconfiguration, and surveillance, including using other components to detect failures
- Methods for human reliability analysis associated with digital systems
- Determining if and when a dynamic model of controlled plant processes is necessary in developing a reliability model of a digital system



Integration into a Plant PRA

- Use of Markov quantification methods raises some issues with regard to integration with a plant PRA that is based on the ET/FT method (e.g., treatment of “non-minimal” cutsets that occur due to the need to consider the order of component failure events).
- Due to resource limitations and competing priorities, work on integration of digital system models (such as the Markov model of the DFWCS developed in this study) into a full plant PRA have been postponed.
 - Note, some work on integrating the dynamic DFWCS models developed by OSU, et al., is documented in NUREG/CR-6942 and NUREG/CR-6985.



Establishing a Philosophical Basis for Modeling of Software Failures

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 23, 2010

Tsong-Lun Chu
Brookhaven National Laboratory
(631-344-2389, chu@bnl.gov)

Brookhaven National Laboratory
U.S. Department of Energy

Background

- In 1997, a National Research Council committee completed a study requested by the NRC on application of digital instrumentation and control (I&C) technology to commercial nuclear power plant operations. It concluded that:
 - 1) *“Explicitly including software failures in a PRA [probabilistic risk assessment] for a nuclear power plant is preferable to the alternative of ignoring software failures”*
 - 2) *“As in other PRA computations, bounded estimates for software failure probabilities can be obtained by processes that include valid random testing and expert judgment.”¹*
- In April 2008, the ACRS Subcommittee on Digital I&C Systems recommended:
 - 1) *“The staff should explore the fundamental philosophical aspects of software failures and their use in developing a probabilistic model of a digital system.”*
 - 2) *“The staff should consider the relevant aspects of developing and evaluating a reliability model of a digital system that integrates hardware and software failures...”*

¹Committee member Nancy Leveson did not concur with this conclusion.



A Workshop of Software Reliability Experts

- NRC/Brookhaven National Laboratory (BNL) organized and convened a workshop involving experts with knowledge of software reliability and/or nuclear power plant (NPP) PRA in May 2009.
- Workshop objectives:
 - Obtain a consensus, or at least agreement among the majority of workshop participants, on the “philosophical basis” for incorporating software failures into digital system reliability models for use in PRAs.
 - Discuss issues associated with methods for modeling software in a reliability model and quantifying software failure rates and probabilities.



Panel of Experts

- Mr. Steven A. Arndt, NRC
- Mr. Bob Enzinna, AREVA
- Dr. Hyun Gook Kang, Korea Atomic Energy Research Institute
- Prof. Michael R. Lyu, Chinese University of Hong Kong
- Prof. Bev Littlewood*, City University, London
- Dr. Allen P. Nikora, Jet Propulsion Laboratory
- Prof. Martin L. Shooman, Polytechnic Institute of New York University
- Prof. Nozer D. Singpurwalla, George Washington University
- Prof. Kishor S. Trivedi, Duke University

*Prof. Littlewood was unable to attend the meeting, but did provide responses to a questionnaire.



A Philosophical Basis for Modeling Software Failures Probabilistically

- Software failure is basically a deterministic process. However, because of our incomplete knowledge, (e.g., the number and nature of residual faults, and occurrence and timing of fault-triggering inputs) we are not able to fully account for and quantify all the variables that define the failure process. Therefore, we use probabilistic modeling to describe and characterize the software failure process.
- The above basis is essentially the same basis for many other probabilistic processes, e.g., tossing a coin. In the case of a coin toss, if one can control all aspects of the toss and repeat it each time, the result will always be the same. However, due to our inability to precisely repeat all aspects of the toss, the outcome is uncertain and can be modeled as a random variable.



How Do Software Failures Occur?

- Software can fail because it provides a service, and the service may not be delivered correctly or the software may perform an undesired action. This can be considered as a failure of the software.
- Faults are introduced into software during the software life cycle. It is not possible to identify and eliminate all faults of a non-trivial software. Therefore, residual faults always exist in the software.
- During operation of the software, if a certain input state occurs which interacts with the internal state of the digital system to trigger a fault in the software, the software may respond incorrectly.



How Do We Include Software in a Reliability Model of Digital Systems, i.e., in a PRA?

- Most panelists agreed that hardware and software failures can be modeled separately in the same reliability model provided that the dependencies between them are appropriately accounted for.
- The majority believed generic software failure modes can be used to model the contribution of software failures to the risk of an NPP, but believed that additional failure modes may need to be defined when studying failure behavior of application-specific software.
 - Although some methods were suggested by the panelists, consensus methods or approaches for identification of specific failure modes do not seem to exist.
- The panelists had very diverse opinions regarding the determination of the right level of detail of probabilistic modeling, which may depend on factors such as data availability.



Methods for Quantifying Software Failure Rates and Probabilities of Digital Systems

- A constant failure rate (or probability) is appropriate for characterizing software failure; however, two panelists warned that it may not be pertinent for periods that are demanding for the software.
- The panelists discussed the feasibility of quantifying probabilistic parameters, and proposed the testing of software, the main method used worldwide by scientists and practitioners for this purpose.
- The quality of the development of the software during its life cycle is important and is related to the probability that the software fails.
- Expert judgment also was suggested, especially to evaluate safety-critical software.
- If the same software is used in redundant parts of a digital system, and all the redundant software receive the same input, it is conservative but reasonable to consider in a PRA model that if one part of the system fails due to a software fault then all redundant parts of the system will also fail, i.e., with conditional probability 1.



Workshop Conclusions

- There is a philosophical basis for incorporating software failures into a PRA.
- Probability theory and associated reliability methods can be used to model software failures.
 - Need to account for the unique characteristics of software
- Quantitative methods can be used to quantify software failure rates and probabilities.



REVIEW OF QUANTITATIVE SOFTWARE RELIABILITY METHODS

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 23, 2010

Tsong-Lun Chu
Meng Yue

Brookhaven National Laboratory
(631-344-2389, chu@bnl.gov)
(631-344-7140, Yue@BNL.gov)

Brookhaven National Laboratory
U.S. Department of Energy



Outline of Presentation

- Introduction
- Principal changes in response to peer review
- Desirable characteristics of quantitative software reliability methods (QSRMs)
- Quantitative software reliability evaluation methods:
 - Software reliability growth methods (SRGMs)
 - Bayesian belief network (BBN) methods
 - Test-based methods
 - A correlation method using software development practices (Frestimate)
 - A context-based software reliability method (CSRm)
 - Other QSRMs
- Summary and principal findings

Introduction

- No commonly accepted methods exist for incorporating software behavior into digital system reliability models for use in probabilistic risk assessments (PRAs).
- The objective of the study is to gain comprehensive knowledge of available QSRM methods, especially those emphasizing the quantification of software failure rates and demand failure probabilities that might be employed in reliability models of digital systems for nuclear power plant (NPP) PRAs.
- The approach to performing the study includes:
 - Development of desirable characteristics of QSRMs for applications in NPP PRAs
 - Identification and review of existing QSRMs from a search of NRC-sponsored research, research performed by other U.S. government organizations and international organizations, and open literature studies



Principal Changes in Response to Peer Review

- Additional referencing of NRC-sponsored research on dynamic modeling methods
- Additional clarification on how different types of digital systems (e.g., control and protection) and different failure modes (e.g., failure to actuate on demand and inadvertent actuation) are modeled in a PRA.
- Added discussion on the “context” of software failures (i.e., the influence that the operating conditions of the software have on the likelihood of software failure)
- Modified the review of the “Correlation Method Using Software Development Practices” (Frestimate), based on additional concerns raised by peer reviewers
- Re-incorporated a review of the Context-based Software Risk Model



Development of Desirable Characteristics of QSRMs

- The desirable characteristics were developed based on the perceived need for reliability models of digital systems in a PRA and the knowledge and experience of the study team in performing research and literature reviews on modeling of digital systems.
- They are expected to address the general guidelines provided in the American Society of Mechanical Engineers (ASME) standard for PRA for NPP applications.
- The desirable characteristics can be used in evaluating available QSRMs and their applications to determine if the characteristics are satisfied.
- Although an itemized evaluation of the methods against the desirable characteristics is beyond the scope of this study and is planned to be included in the next phase of the research, the QSRM review report is useful in performing such an evaluation.

Software Reliability Growth Models

- SRGMs have been used to estimate software reliability measures, such as failure rates, based on test data and to determine whether the software should be released.
- In an SRGM:
 - The occurrence of software failures is modeled as a Non-Homogeneous Poisson Process (NHPP).
 - It is usually (but not always) assumed that, during testing, the detected software faults are fixed perfectly and instantaneously such that the software failure rate decreases and reliability increases with time.
 - How the failure rates decrease is determined by the empirical formula of the SRGM.
- Both continuous- and discrete-time SRGMs* exist.

* Discrete SRGMs will be addressed in the next phase of this work.

Continuous-Time SRGMs (1)

- Continuous-time SRGMs can be categorized into Exponential NHPP, Non-exponential NHPP, and Bayesian models.
- Unification schemes for various NHPP SRGMs have been developed by, e.g., expressing the accumulated number of software faults in similar forms.
- For exponential NHPP models:
 - It is assumed that software failure rate is proportional to the remaining fault content, which is analogous to the rate of radioactive decay of an isotope being proportional to the inventory of the isotope.
 - Effectively, the software failure rate decreases exponentially with time.
 - Exponential NHPP models include Musa's Basic model, Schneidewind's model, Goel's NHPP model, the Generalized Exponential model, Shooman's Exponential model, and Jelinski-Moranda's model, etc.

Continuous-Time SRGMs (2)

- For Non-exponential NHPP models:
 - It is assumed that software failure rate follows the shape of a probability density function of a different distribution, e.g., a Gamma distribution.
 - Non-exponential NHPP models include Musa's Logarithmic Poisson Execution Time Method, Duane's model, (delayed or inflection) S-shaped reliability growth models, etc.
- For Bayesian SRGM models:
 - It is assumed that the failure rate decreases probabilistically/ stochastically with time.
 - The models essentially are an exponential NHPP model that explicitly includes the uncertainty of the failure rate in the model.
- Parameter estimation of SRGMs
 - Maximum likelihood method, Least-square method, and Moment-matching method are commonly used.
 - Usually only point estimate of model parameters is performed but there exists no inherent difficulty in determining the associated uncertainties.



Comments on Continuous-Time SRGMs

- SRGMs are the most popular software reliability methods/models.
- There exists no single SRGM that is universally superior to others, because all are based on assumed empirical formulas that are not applicable to all situations.
- In real applications, the assumptions for individual models are often violated, still many models were demonstrated empirically to be robust.
- Demonstrations are needed to show that the estimated failure rates fit actual operational experience well considering the fact that test inputs do not necessarily reflect operational environment well.
- Since SRGMs are driven by test-failure data, it may not be possible to use these models to demonstrate very high reliability.
- Continuous-time SRGMs can be directly applied to estimate software failure rates. If failure probability per demand is of interest, continuous time SRGMs can still be used but not in a straightforward manner, i.e., it may be possible to generate demand-based results by including the frequency of demands in the failure rate estimation of an SRGM, or re-interpret the time-based failure data used in an SRGM as demand-based data.

Bayesian Belief Network Models

- A BBN is a probabilistic graphical model depicting a set of random variables and their conditional independencies via a directed acyclic graph.
- A basic assumption for BBNs is that a node is conditionally independent of its non-descendent nodes, given its parent nodes.
- For a BBN, Jensen [*Bayesian Networks and Decision Graphs*, Springer, 2002] proved that the joint distribution of all variables $\{V_i\}$ is

$$P(V_1, V_2, \dots, V_n) = \prod_{i=1}^n P(V_i \mid \text{parents}(V_i)).$$

- Bayesian inference is performed by updating the above equation using the acquired evidence; there exists a spectrum of software tools for the inference.
- Building BBNs is application specific and there exists no general guideline to guarantee the correctness of dependencies in the BBN.
- Usually, a BBN model is built by a group of experts in domains of both BBN and specific applications based on information or evidence from experts' knowledge and statistical data.

Comments on the BBN Method

- The principal strength of the BBN method is its capability of incorporating both experts' subjective opinion (qualitative evidence) and quantitative evidence in a single BBN application model.
- Qualitative evidence (e.g., the impact of software development quality on software reliability) needs to be quantified.
- There exists no standard method/procedure to quantify qualitative evidence in BBN models.
- Characterizing the dependence between nodes, which is a fundamental concept of the BBN method, is heavily dependent on analyst judgment and knowledge, and can be difficult to verify, which can lead to large uncertainty in the resultant estimates.

Test-Based Models

- All QSRMs use test data and thus are subject to many of the limitations of test-based methods.
- Test-based models apply standard statistical methods to analyze software testing results and/or software operational data to obtain software reliability.
- Two types of testing may be performed, namely
 - White-box (or glass-box or gray-box) testing: account for internal structure and paths of software execution paths,
 - Black-box testing: frequentist approach and Bayesian approach.
- Implementation of a test-based method consists of (1) generating test cases based on the expected “operational profile” of the software; (2) performing the test; and (3) quantifying the software reliability.

Comments on Test-Based Models

- For software, test cases should be generated from the operational profile, which may not be well known.
- A software with a fault removed during test is considered a modified version of the original software and the previous testing results may not be directly applicable.
- Testing may not uncover incorrect requirements or specifications of software.
- A large number of tests may be required to obtain confidence in a low-valued reliability parameter.



A Correlation Method Using Software Development Practices

- “Frestimate” is a software tool implementing a method which:
 - Includes a proprietary database of software development practices (e.g., use of coding standards) of past projects obtained by surveying software managers and engineers,
 - Uses a regression analysis to estimate the defect density (number of defects per thousand lines of code) of a target software system based on system-specific practices, and
 - Converts number of defects to a failure rate using an empirical formula.

Comments on the “Frestimate” Method

- The general concept of performing correlation/regression analyses using past software development experience is reasonable.
- However, because of the unavailability of detailed information on the past software development projects and the correlation/regression analyses used to construct the predictive model, this methodology could not be evaluated in detail.
- Potential limitations include:
 - Subjectivity in the responses to the survey of software development practices
 - Large uncertainties associated with the process for determining the ratio between inherent defects and failure rate



Context-based Software Risk Model

- CSRM is a modeling method for incorporating software function contributions to risk into a PRA.
- It is based on the concept of “context-dependent” software risk scenarios, essentially identification of hardware failures or other off-normal conditions that require the software to operate under conditions that may not have been thought of by the system and software designers.
- CSRM is a PRA modeling tool; it is not a specific approach for generating software failure rates or probabilities, though it can be used in conjunction with quantitative estimation processes.

Comments on the CSRM Method

- CSRM does not have its own/new quantification method for software failure rates and probabilities, but relies on existing QSRMs.
- A principal advantage of CSRM is that it decouples the estimation of the rate at which a given system may enter a context-forcing condition from the frequency or probability that the digital system does not respond correctly given the occurring system condition or “context,” thereby greatly reducing the testing burden.
- Potential limitations include
 - There may be a large number of contexts that have to be evaluated individually.
 - Defining the context-specific input space for testing would have to be done manually.
 - Complex software can contain hundreds or thousands of variables, which can lead to significant trade-offs between modeling complexity and effort versus modeling accuracy.

Other QSRMs

- Metrics methods (NUREG/GR-0019, NUREG/CR-6864): Software reliability was estimated using a few individual software engineering measures (SEMs).
 - A key inconsistency of the application of metrics methods in NUREG/CR-6864 is that the methods are based on individual SEMs and do not account for the effects of other SEMs.
- Rule/standard based methods: International Electrotechnical Commission (IEC) Standard 61508 specifies requirements of software and hardware systems and provides guidance on assigning safety integrity levels (SILs).
 - The relationship between the SILs' qualitative requirements and the associated quantitative requirements/targets is assigned subjectively, and needs to be validated.
- Quantification methods for software diversities: N-version programming uses multiple software development teams to develop software according to the same specification.
 - The results of N-version programming experiments show that N-version programming can improve reliability. However, different versions of software do not necessarily fail completely independently (e.g., due to the specifications containing too much information, leading to a limited diversity).

Summary and Principal Findings (1)

- Most of the existing QSRMs were not developed specifically for supporting quantification of software failure rates and demand failure probabilities to be used in reliability models of digital systems. However, they do estimate software failure rates or probabilities, and use them in supporting decision making during software development.
- Many of the QSRMs (i.e., the SRGMs, Frestimate method, and metrics methods) use empirical formulas that are not mathematical laws, and therefore, their general applicability is limited.
- Most applications of QSRMs only considered failure of the software system as a whole, not broken down by software failure mode.
- BBN methods have the advantages that they allow aggregation of disparate information about a piece of software and they include parameter uncertainties as a part of the modeling. However, the expert judgment required to characterize the dependence between nodes, can lead to large uncertainty in the resultant estimates.
- The test-based methods use standard statistical methods with software testing and, conceivably, with operating data if available. Limitations of the methods are also applicable to any other methods that use test data.

Summary and Principal Findings (2)

- Frestimate may be difficult to use due to the unavailability of detailed information on the past software development projects and the correlation/regression analyses used to construct the predictive model.
- CSRM identifies contexts for performing tests, but does not provide a new method for quantifying software failure probabilities.
- A key inconsistency of metrics methods is that they are based on individual SEMs and do not account for the effects of other SEMs.
- IEC Standard's assignment of failure rates and probabilities remains to be validated.
- N-version programming can improve software reliability but different versions may not fail completely independently.

For the next phase of this research, we are currently leaning towards proof-of-concept application of BBN and discrete-SRGM.



BACKUP SLIDES



Desirable Characteristics of QSRMs for Applications in NPP PRAs (1)

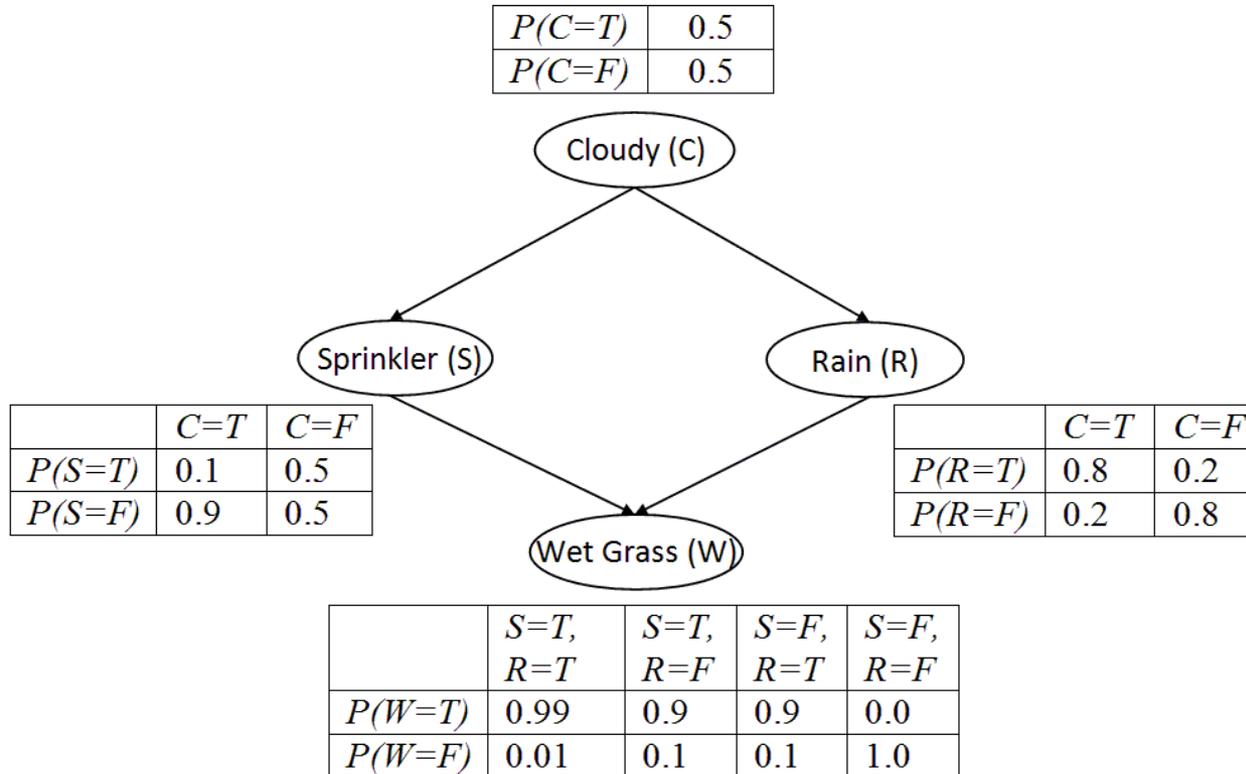
- The methods should be able to produce software failure rates or failure probabilities on demands that can be used in digital I&C system reliability modeling.
- The description of the methods and the applications should be comprehensive and understandable.
- The assumptions of the methods should have reasonable bases.
- The methods should allow for consideration of specific operating conditions of software.
- The methods should take into account the software development life cycle activities.
- The method should make use of available test results and operational experience.



Desirable Characteristics of QSRMs for Applications in NPP PRAs (2)

- The method can address epistemic uncertainty.
- The method has been successfully applied to real systems to demonstrate its usefulness in supporting reliability modeling of digital systems.
- The method is capable of demonstrating the high reliability of a safety-critical system (e.g., a failure on demand probability on the order of 10^{-5} , commensurate with an analog RPS).
- The method should be able to estimate parameters to account for software common cause failures (CCFs), for example, a beta factor that accounts for the software dependency between two redundant channels of a digital system or two redundant digital systems.

An Example Bayesian Belief Network Model [Murphy 1998]



Murphy, K., "A Brief Introduction to Graphical Models and Bayesian Networks," 1998, available online at <http://www.cs.ubc.ca/~murphyk/Bayes/bnintro.html>.

Building Bayesian Belief Networks

- An example process of building a BBN:
 - (1) Start from the target node which is of interest,
 - (2) Draw edges between the target node and the intermediate nodes that affect it, and
 - (3) Continue the expansion of the network by drawing edges from the intermediate nodes to nodes that affect them until all of the end nodes that represent observable properties about the application are reached.

Bayesian Belief Network Applications (1)

- Littlewood's multi-legged arguments with each leg supports different reliability claims for software-based systems:
 - The study shows that adding a diverse second leg can increase confidence in a dependability claim.
 - The study also describes some counter intuitive results which are claimed to be due to "subtle interplay between assumptions and evidence both with and between legs.
 - The study reveals the complexity of an even very simple BBN and warns against naively trusting in the numerical results of a BBN.
- BBN applications to reactor protection system software performed by KAERI:
 - A feasibility study of the BBN model the is used to assess the quality of the RPS software requirement specification based on the characteristics that describe software's functions and development processes.
 - A generalized BBN template based BBN model for an evaluation of the number of residual defects in software considering both the introduction and fixes of defects in each phase of software development life cycle.

Bayesian Belief Network Applications (2)

- BBN applications to software reliability of M-ADS and digital motor protection relay performed by VTT present three types of BBN structures:
 - A BBN model that accounts for both qualitative and quantitative evidences via an integration of (1) a higher level BBN that is linked to low level BBNs (more detailed BBN models) and represents the “quality”-part (mainly used to provide priors) and (2) A BBN representing the “testing”-part (mainly used to update the priors).
 - A BBN representation of the revision process of a software through its operating life in terms of a lognormal-Poisson model that uses expert judgments to formulate a prior of the failure rate of the first version of software and the failure data of the operation of the software to update the prior. The posterior distribution is used as the prior of the next version.
 - A BBN based on (1) consideration of four different software design phases, (2) estimation of the failure rate distribution of a failure mode for each design phase by combining expert estimated medians and percentiles, (3) merge of the failure rate distributions of the design phases into a single prior distribution for the failure mode, and (4) update of the prior based on the failure data of the software operation.

Limitations of “Dynamic” Modeling Methods

- State explosion - Modeling timing and physical processes add dimensions to the modeling need and its degree of difficulty. There is a trade off between the accuracy of a model and the ease of solving the model.
 - Representing a physical parameter using only a few possible values may not be an accurate representation of the real process. It would be difficult to build a simplified model without a supporting physical modeling tool.
 - It is particularly difficult to model software that has complex logic.