

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (not applicable)

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005

SISP REVIEW COMPLETE

Location: Rockville, Maryland

Date: Tuesday, June 14, 2005

Work Order No.: NRC-461

Pages 1-296

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

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

TR02

DISCLAIMER

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

June 14, 2005

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on June 14, 2005, as reported herein, is a record of the discussions recorded at the meeting held on the above date.

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

1
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

+ + + + +

TUESDAY,
JUNE 14, 2005

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory
Commission, Two White Flint North, Room T2B3, 11545
Rockville Pike, at 8:30 a.m., George E. Apostolakis,
Chairman, presiding.

COMMITTEE MEMBERS:

- GEORGE E. APOSTOLAKIS, Chairman
- MARIO V. BONACA, Member
- SERGIO B. GUARRO, Consultant
- THOMAS S. KRESS, Member
- JAMES D. WHITE, Consultant

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

(202) 234-4433

www.nealrgross.com

1 ACRS STAFF PRESENT:

2 SAM DURAISWAMY

3 MICHAEL R. SNODDERLY

4 ERIC A. THORNSBURY

5

6 NRC STAFF PRESENT:

7 STEVEN A. ARNDT, RES

8 RICHARD BARRETT, RES

9 JOSE A. CALVO, NRR

10 NORBERT N. CARTE, RES

11 CHRIS GRIMES, NRR

12 WILLIAM E. KEMPER, RES

13 PAUL LOESER, NRR

14 EVANGELOS MARINOS, NRR

15 ROMAN SHAFFER, RES

16 GEORGE TARTAL, RES

17 MICHAEL E. WATERMAN, Sr., RES

18

19 ALSO PRESENT:

20 MING LI, University of Maryland

21

22

23

24

25

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

(202) 234-4433

www.nealrgross.com

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

A-G-E-N-D-A

Opening Remarks and Objectives

G. Apostolakis, ACRS 3

W. Kemper RES 4

Reconciliation of Comments on Draft Research Plan

M. Waterman, RES 7

J. Calvo, NRR 65

Draft Review of Reg Guide 1.97

W. Kemper, RES 103

G. Tartal, RES 105

Software Quality Assurance (3.2)

W. Kemper, RES 125

Assessment of Software Quality (3.2.1)

N. Carte 142

M. Li, UMd 157

Digital System Dependability (3.2.2)

S. Arndt, RES 213

R. Shaffer, RES 215

Self-Testing Methods (3.2.3)

S. Arndt, RES 275

Risk Assessment of Digital Systems (3.3)

S. Arndt, RES 281

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

8:30 a.m.

CHAIRMAN APOSTOLAKIS: The meeting will now come to order. This is the first day of the meeting of the Advisory Committee on Reactor Safeguards Subcommittee on Digital Instrumentation and Control Systems.

I'm George Apostolakis, chairman of the subcommittee. Members in attendance are Mario Bonaca and Tom Kress. Also in attendance are two of our consultants, Dr. Sergio Guarro and Mr. James White.

The purpose of this meeting is to discuss the NRC staff's Draft Digital Systems Research Plan, the staff's approach to revising Regulatory Guide 1.97, and two specific research programs discussed in the plan, software quality assurance, and the risk assessment of digital systems. The subcommittee will gather information, analyze the relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full committee.

Mike Snodderly is the designated federal official for this meeting. Eric Thornsbury is the cognizant staff engineer. The rules for participation in today's meeting have been announced as part of the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 notice of this meeting previously published in the
2 Federal Register on May 31, 2005. A transcript of the
3 meeting is being kept, and will be made available as
4 stated in the Federal Register notice. It is
5 requested that speakers first identify themselves and
6 speak with sufficient clarity and volume so that they
7 can be readily heard. We have received no written
8 comments or requests for time to make oral statements
9 from members of the public regarding today's meeting.
10 I should note that the staff briefed the full
11 committee on May 6 of this year.

12 We will now proceed with the meeting, and
13 I call upon Mr. William Kemper of the Office of
14 Nuclear Regulatory Research to begin the
15 presentations. Bill?

16 MR. KEMPER: Thank you George. My name is
17 Bill Kemper. I'm the section chief of the
18 Instrumentation and Control Engineering Section of the
19 Office of Research. We have numerous topics to cover
20 in the next day and a half, and we have several
21 presenters of the material. There's an agenda
22 floating around. I presume everybody has that.

23 So before we begin, since we have some new
24 members on our staff, I thought it would be productive
25 to introduce at least the members of our staff that

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 will be making presentations over the next day or so.
2 So Mike Waterman is here who will start out the
3 reconciliation of comments on the draft research plan.
4 George Tartal is in the back there. George, will you
5 stand up, please? George joined our section about a
6 year ago from the industry. He'll be talking about
7 Reg Guide 1.97.

8 We also have Steve Arndt. Everybody knows
9 Steve, I'm sure, he's been around for awhile. Steve
10 will be talking about two or three of the
11 presentations. Norbert Carte back there. Norbert
12 joined us about six months ago from the industry as
13 well. Norbert will be talking about software quality.
14 Is Dr. Ming Li here by any chance? I guess he hasn't
15 joined us yet. Okay, he'll be here later, from the
16 University of Maryland. Roman Shaffer should be --
17 there he is in the background. Roman will be talking
18 about digital system dependability. And Todd
19 Hilsmeier, is Todd here? Okay, great. Todd's going
20 to be talking about, tomorrow, dependability and
21 analysis of digital system failure data. And he has
22 Mr. Chu with him from Brookhaven National Lab. And
23 also we have Professor Tunc Aldemir from Ohio State
24 who will be talking to us later also about his
25 research and investigation of digital system failure

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 assessment methods.

2 So, as you say, we're here to brief the
3 ACRS subcommittee on various topics contained within
4 our new Draft Safety Systems Research Plan, which
5 covers 2005 through 2009. We briefed the full ACRS
6 committee of this plan in May, and subsequently we
7 were asked to provide more information on the research
8 plan to the I&C subcommittee. So that is what we're
9 here to do. Research has been working proactively
10 with our stakeholders in NRR, NSIR, and NMSS to
11 improve the draft research plan. We also hope to work
12 closely with ACRS to improve our research program
13 itself.

14 We appreciate the fact that ACRS has
15 formed a subcommittee to support this area, and we
16 look forward to our interactions with you all. We
17 hope that these briefings that we're going to provide
18 to the ACRS and its subcommittee on the draft research
19 plan will result in ACRS endorsement of the plan, for
20 our updated program plan, just as you did for the
21 previous program plan. So unless there's any
22 questions, at this point I'd like to go ahead and get
23 started with the first presentation with Mike
24 Waterman.

25 MR. WATERMAN: Good morning. My name is

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

(202) 234-4433

www.nealrgross.com

1 Mike Waterman. I'm with the Instrumentation and
2 Control Section of the Engineering Research
3 Applications Branch in the Division of Engineering
4 Technology. Let's see hee, background. I was with
5 NRR's I&C section for about 14 years, and then I
6 joined Research about a year ago. And one of the
7 tasks I was given was to try to put together a
8 research plan.

9 We started the plan about last year. We
10 solicited comments in December/January timeframe. We
11 received the comments. We incorporated comments from
12 three supported offices, the Office of Nuclear
13 Security and Incident Response, the Office of Nuclear
14 Materials Safety and Safeguards, and the Office of
15 Nuclear Reactor Regulation. And so today I'm going to
16 go over how we addressed those comments briefly. So
17 with no further ado.

18 In this overview, just a brief summary of
19 the NRC licensing bases combined with the NRC
20 licensing process, specifically NRR, because that's
21 where my experience comes from. Talk a little bit
22 about our emphasis on improving communications, and
23 we'll get into the comment disposition summary table,
24 and disposition of comments, and a little bit of a
25 summary.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 Briefly, just summarizing, you'll see
2 later on, we had 34 formal comments received from the
3 offices of NRR, NMSS, and NSIR. Thirty-one of the 34
4 comments were incorporated into the research plan, and
5 the remaining three comments addressed topics that are
6 really outside the scope of the research plan, or just
7 required nothing to be done to the research plan.
8 The first of those comments dealt with a suggestion
9 that we put metrics into the research plan to measure
10 the effectiveness of the research projects relative to
11 the NRC's strategic plan. The second comment involved
12 incorporating human factors considerations in our
13 PRAs. We thought that would probably be better suited
14 for the Human Factors Branch to deal with that in
15 their research plan. And the final comment was
16 something about NRR SRP is considered sufficient
17 guidance for the fuel cycle people in NMSS, and didn't
18 know what to do with that, so we just, you know, let
19 it ride.

20 CHAIRMAN APOSTOLAKIS: But this is an
21 important comment, though, isn't it? I mean, I read
22 some of the memos, well, all of them actually, from
23 the various offices to you, and I guess they all feel
24 that what they're doing now is sufficient.

25 MR. WATERMAN: Well, I'll get into that,

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

1 Dr. Apostolakis, as I go through the discussion.

2 CHAIRMAN APOSTOLAKIS: No, but I mean the
3 way you dismissed this last sub-bullet, I don't know.
4 You said 'I don't know what to do with that.' I mean,
5 that's a pretty serious comment. They're saying what
6 we're doing is good enough. When you form a research
7 plan, don't you have to take that into account?

8 MR. WATERMAN: Yes, sir, we do. And I'll
9 talk about that as we go on, and you'll see how all
10 that folds out.

11 MR. KEMPER: Yes, we're going to address
12 that as a common theme through several of our
13 presentations.

14 CHAIRMAN APOSTOLAKIS: All right.

15 MR. WATERMAN: Essentially what the NMSS
16 comment was was that they're moving toward a more
17 qualitative risk-informed review, similar to what the
18 NRR SRP already has in it. And what we're trying to
19 do is get more specific than just qualitative, 'This
20 is a swell system' or 'This is a good enough system,'
21 things like that. So I'll get into that in a minute,
22 Doctor.

23 RES revised the research plan to reflect
24 the need for additional information in several areas
25 on the basis of communications with the supported

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 offices. The research plan will continue to be
2 updated in response to communications with the
3 supported offices as new needs are identified, and as
4 research projects are completed. And what I mean by
5 that is the research plan ought to be a living
6 document, not something we do once every five years,
7 and then five years later go back and revise it. It
8 should be a document such that as research is
9 completed, we pull that research project out of the
10 Section 3 of the plan, if you will, and have an annex
11 where we describe -- summarize the results of that
12 research, so that if somebody picks up the research
13 plan, not only do they see where we're at and where
14 we're going, but they can also get a flavor for what
15 we've done and where we've been. So that's our vision
16 of what the research plan ought to be, is something
17 that continues to change as situations change.

18 MEMBER WHITE: Excuse me, I'd like to ask
19 a question. As I was reading your plan last night, I
20 was myself wondering about metrics by which you would
21 evaluate your research effectiveness. In your slide
22 here you say that that's outside the scope of the
23 research plan. Of course any plan should have
24 metrics, or goals, or targets. So is there some other
25 document then that I can look at to see how you are

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 measuring your research effectiveness? If it's not
2 covered in this presentation?

3 MR. WATERMAN: Well, we have NRC internal
4 reviews of programmatic effectiveness that we're
5 already using in the various offices. And primarily
6 the reason I didn't incorporate the metrics to
7 evaluate research effectiveness of the research plan,
8 if I got into a long, lengthy discussion about how
9 each of these things would be measured, if we're using
10 PART, which is the Office of Management and Budget
11 procedure, or something like that, we sort of divert
12 attention away from the research into more attention
13 devoted to actually measuring research effectiveness
14 relative to the strategic plan. So it might be a good
15 topic for a supplementary document that we can use to
16 evaluate our research effectiveness, but I don't know
17 that it goes into the research.

18 MEMBER WHITE: I think I understand what
19 you're saying, but from a technical point of view, you
20 surely have technical goals by which you would do a
21 self-assessment of how well you're doing relative to
22 those technical goals. And is that part of the
23 presentation, and if not is there another --

24 MR. WATERMAN: It's not part of this
25 presentation at all.

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

(202) 234-4433

www.nealrgross.com

1 MEMBER WHITE: Okay, thank you.

2 MR. WATERMAN: Briefly, the NRC licensing
3 bases depend upon the Code of Federal Regulations,
4 Commission policy statements, standard review plans,
5 Branch technical positions, consensus standards,
6 regulatory guides that endorse consensus standards and
7 take other positions, topical reports, and research
8 reports. Now, these sources of guidance and
9 requirements identify the safety system attributes
10 that must be reviewed, and provide guidance regarding
11 minimum acceptable standards of performance and
12 quality. In a way, these documents, if you will are
13 similar to technical specifications, for those of you
14 who are familiar with those, which identify limiting
15 conditions for operation, action statements, set
16 points, surveillance requirements, and technical
17 bases. The acceptance criteria identified in NRC
18 regulations, guidance, standards, and technical
19 reports are similar to surveillance requirement
20 acceptance criteria. For example, nuclear power
21 plants have a tech spec surveillance requirement to
22 perform a heat balance, if you will, and use the
23 results of that heat balance to adjust their nuclear
24 power range instrumentation. Now, nuclear power plant
25 procedures, not the tech spec, specify how the heat

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 balance is to be obtained, how the result is to be
2 compared to nuclear power range instrumentation, and
3 how the adjustment of nuclear power range instruments
4 is to be performed. And similar to technical
5 specifications, NRC regulations, reg guides,
6 standards, the SRP, technical reports, prescribe
7 surveillance requirements, if you will, but generally
8 do not provide specific procedures for performing
9 those surveillances. A major focus of this research
10 plan is to produce the supporting surveillance
11 procedures which will augment and supplement our
12 existing process. We're not trying to replace
13 process. We're simply trying to augment and
14 supplement those with actual procedures such that no
15 matter who does the review, they follow the same
16 process, step by step, as much as possible. And right
17 now those step-by-step procedures just, you know, they
18 aren't there. I can say that from 14 years'
19 experience of doing this that generally I had what was
20 called an NRC audit assistant tool which didn't
21 provide procedures but at least it guided me in what
22 questions to ask. What we're trying to do is to
23 formalize that process a little bit more so that no
24 matter who does the review we get the same result.
25 And that we're reviewing all of the things that we

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 need to review.

2 CHAIRMAN APOSTOLAKIS: But again, the
3 standard review plan doesn't do that?

4 MR. WATERMAN: No, sir, it doesn't. The
5 standard review plan has guidance that says you should
6 check the correctness of a system through the various
7 lifecycle phases, but it doesn't really go into the
8 details of what does that mean, "correctness", what
9 actual process do you go through to come to the
10 conclusion that yes, the system is correct enough.
11 All it does is it gives guidance. It's great
12 guidance. I worked on doing -- I worked on writing
13 the standard review plan with Gary Johnson out of
14 Lawrence Livermore National Lab, and if you talk to
15 Gary, he'll say the same thing I'm doing. The
16 standard review plan was never meant to be a review
17 procedure. It was meant to put bullets up of things
18 that ought to be checked. The intent back when we
19 wrote that branch technical position was to follow it
20 up with actually writing procedures that describe when
21 we say "correctness" what does that mean, how do you
22 go through the process of assessing correctness,
23 robustness, completeness, understandability. All of
24 those attributes that you find in HICB-14, the branch
25 technical position. All that we're really trying to

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 do is to augment and supplement the guidance that's in
2 the SRP such that a reviewer can pick up that guidance
3 and procedures and go through it.

4 If you go out to the regions, you know,
5 they have inspection procedures for everything they
6 do, and they do it -- they have an inspection
7 procedure for a reason. It's so that every inspector
8 does exactly the same thing so that the results are
9 consistent. So that's what we're trying to do is to
10 supplement and augment our existing procedures,
11 especially now that we have large systems coming in
12 that are going to require a lot of effort to review.

13 The NRC licensing process, the
14 regulations, guidance, standards, and technical
15 reports identify several hundred important attributes
16 and associated criteria that must be addressed
17 appropriately for digital systems to be licensed for
18 safety-related applications. The emphasis there is
19 several hundred attributes. The purpose of conducting
20 research is to investigate current and emerging
21 methods and knowledge, and where appropriate to
22 augment and supplement NRC processes to enable NRC
23 staff to evaluate digital systems consistently and
24 effectively. We're already doing an effective job of
25 licensing these systems, but the systems are getting

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 bigger, and if we don't start proceduralizing this
2 review process, it's going to slow us down, and there
3 is a potential there for being inconsistent in our
4 reviews.

5 Now, with regard to additional emphasis on
6 communications, the research plan was revised to
7 provide additional emphasis on development of research
8 products, review procedures, tools, etcetera, that
9 augment and supplement existing NRC review plans and
10 processes as part of a general process improvement
11 initiative. Also we provided additional emphasis on
12 enabling communications between research and the
13 supported offices during the initial stages of
14 research project planning to identify specific
15 research products that must be developed, and during
16 performance of research to keep the supported offices
17 informed on the progress of Research.

18 Now, meetings have been held with
19 supported offices to describe the research plan. We
20 had presentations for the Office of NSIR, the Office
21 of NMSS. We offered to present the research plan to
22 the Office of NRR. They elected to not receive a
23 presentation. That was back in the December/January
24 timeframe where we wanted to just roll it out ahead of
25 time, say this is what it's got, what do you think.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 Two of the offices elected to see that, and they
2 provided their input to us, and the other office
3 elected not to.

4 CHAIRMAN APOSTOLAKIS: So what's TAG? T-
5 A-G?

6 MR. WATERMAN: Oh, I'm sorry. In the
7 future, what we want to do is set up technical
8 advisory group meetings with participants from each
9 office so that we can identify issues that are coming
10 up, get the ball rolling on starting to do research to
11 address those issues, or perhaps one office has an
12 issue that another office has already addressed.

13 MR. KEMPER: The intent here is the
14 research plan does not have the specificity needed to
15 really sit down and write a statement of work. So the
16 idea is it would provide a framework, general areas of
17 research and specific topics that we could agree --
18 come to a conceptual agreement on. And then we would
19 form the TAG and really flesh out the details of the
20 specific scope and the applicable agency areas that
21 are applicable to that in a TAG environment before we
22 kick off a new project.

23 CHAIRMAN APOSTOLAKIS: There would be a
24 number of these advisory committees, or just one
25 advisory committee?

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. KEMPER: No, they would be periodic,
2 but certainly ad hoc as needed, basically to initiate
3 any new work.

4 CHAIRMAN APOSTOLAKIS: I mean, it would be
5 one group that will have representatives from NRR,
6 NMSS, and so on? Or you will have one group from NRR,
7 one group with NMSS?

8 MR. KEMPER: We haven't fleshed that out
9 completely yet, but my desire would be to have all
10 three offices in one TAG.

11 CHAIRMAN APOSTOLAKIS: I think that's a
12 good idea.

13 MR. KEMPER: But you know, it may be that
14 some projects supply more to one office than the other
15 two, so you know, they could spend some unnecessary
16 time in meetings.

17 CHAIRMAN APOSTOLAKIS: Yes.

18 MR. KEMPER: So we'll have to work through
19 that and see what's the best environment for that.

20 CHAIRMAN APOSTOLAKIS: All right.

21 MR. WATERMAN: Now, as an example of
22 communicating, NRR identified an issue recently on the
23 need for regulatory bases that specify appropriate
24 system architectures for digital safety systems, and
25 the impact of those architectures on defense-in-depth.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 A preliminary discussion between NRR and Research has
2 identified the basic needs. Discussions will refine
3 the objectives of the research and identify the
4 products to be produced. We have yet to do that. I'm
5 working on presentations on how I'm incorporating
6 comments right now. Once I get through that I can get
7 back to that work. This issue will be incorporated
8 into the research project that addresses diversity and
9 defense-in-depth. I haven't quite rolled that into
10 the research plan yet, but that will be. It's a very
11 interesting project brought up by Paul Loeser, and NRR
12 identified it. It's if somebody is proposing to
13 incorporate an RPS and SFAS all in one same
14 microprocessor, so your trip and your mitigation
15 systems all in one processor. It's just like, that's
16 like all of your eggs in one basket. The
17 microprocessor hangs up, you've lost trip and
18 mitigation for that channel. I don't know, there's
19 just something that doesn't ring true about that. So
20 Paul's identified that. He's concerned about it, and
21 he and I will be working together to try to hammer
22 that out and see what we can do with it.

23 Well, the following slides summarize the
24 disposition of the 34 formal comments RES received
25 from NRR, NMSS, and NSIR. These are the formal

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

(202) 234-4433

www.nealrgross.com

1 comments. We're also working with NRR to get some of
2 their informal comments incorporated into the research
3 plan as much as possible. The comments range from
4 general comments on the contents of the plan to
5 recommendations for revisions, additions, and
6 modifications of scope. We anticipate that additional
7 research plan changes will be made as specific
8 research project needs are identified in the future.
9 Again, this living document concept of the plan ought
10 to be flexible enough to incorporate new research into
11 it to be revised on a periodic basis.

12 The next three slides will show you a
13 table of how -- this just kind of gives you an
14 overview of the extensiveness of the comments, and how
15 we address those comments. I really don't want to get
16 into any discussion on the format of the table, or
17 anything like that. It's just to kind of give you a
18 flavor for how extensive the comments were, and how we
19 changed the research plan to address those comments.
20 Again, 31 out of 34 of the comments were incorporated.
21 The other three, just couldn't fit them into the plan,
22 so. But none of the comments were rejected,
23 incidentally.

24 CHAIRMAN APOSTOLAKIS: Did you get any
25 input from the offices regarding prioritization?

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

(202) 234-4433

www.nealrgross.com

1 MR. WATERMAN: No, sir.

2 CHAIRMAN APOSTOLAKIS: Do they feel that
3 some of these are much more urgently needed than
4 others?

5 MR. WATERMAN: No, sir, we didn't.

6 MR. KEMPER: No, we hope that a TAG
7 environment will address that. That's when we can
8 really get the stakeholders together, and we can
9 discuss that priority.

10 CHAIRMAN APOSTOLAKIS: When will you start
11 implementing this plan? Have you already started?

12 MR. KEMPER: Well, some of the projects
13 are already in progress. Obviously, they're carried
14 forth from the last research plan. And as resources
15 become available, and the timing is right, then we'll
16 convene a TAG and we'll start the next.

17 CHAIRMAN APOSTOLAKIS: Now, I have the
18 impression, and I'm asking whether you feel the same
19 way, that this is a fairly ambitious plan, and you
20 probably won't have sufficient resources to do
21 everything that is in it. So somehow you have to
22 prioritize.

23 MR. KEMPER: That's correct.

24 CHAIRMAN APOSTOLAKIS: Maybe getting input
25 from the offices as to their urgent needs, although

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 they don't seem to need anything, judging from what
2 I've read. That probably would be a good input to
3 your process.

4 MR. KEMPER: Thank you. That's a good
5 comment. We did make an attempt to resource-load the
6 research plan, if you will. If you look back in
7 Section 4 of the document itself, it provides detailed
8 schedules, if you will, and the priority for each one
9 of them. So we took a swag at the priority, if you
10 will, based on our own intuition. But you're right,
11 we have to confirm that with our stakeholders as we
12 get into the details of these projects.

13 MR. WATERMAN: And that will definitely
14 require a TAG, because I'm sure there's competing
15 resources going on there. So one office may feel
16 their priorities are a little bit higher than another
17 one's.

18 CHAIRMAN APOSTOLAKIS: Well, even within
19 the topics that are of their concern, I mean they
20 should still give you some idea as to what the
21 priorities should be.

22 MR. WATERMAN: Yes, sir.

23 MR. KEMPER: Absolutely.

24 MR. WATERMAN: So in the table, the
25 revised information means the existing discussion in

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

(202) 234-4433

www.nealrgross.com

1 the research plan regarding background issues,
2 etcetera, was correct. In other words, if there was
3 something that was factually incorrect in there,
4 somebody caught it, and we corrected that. The added
5 information means -- in the next column means
6 additional discussion or amplification of the existing
7 discussion was provided to clarify. That's, if you
8 will, a perfective change to the research plan. And
9 the revised scope column means the proposed scope of
10 the research was revised in response to supported
11 office comments. Some places where we thought we had
12 the right scope, somebody pointed out it's not the
13 correct scope, so we changed the scope in the plan on
14 the next revision of the plan to incorporate that
15 comment.

16 The following slides briefly summarize the
17 comments received from the three offices, and the
18 disposition of the comments. These slides only
19 summarize the formal comments we received. I'm very
20 anxious to also incorporate any informal comments we
21 receive, verbal or whatever, into the research plan to
22 address issues that were not conveyed perhaps clearly
23 enough.

24 CHAIRMAN APOSTOLAKIS: Is there a reason
25 why there are informal comments in addition to the

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

(202) 234-4433

www.nealrgross.com

1 formal comments?

2 MR. KEMPER: Well, we've had several
3 meetings with our stakeholders, as I said, to flesh
4 out the comments.

5 CHAIRMAN APOSTOLAKIS: These are what you
6 get in the meeting?

7 MR. KEMPER: Exactly. So the dynamics in
8 the meeting, it fleshes out additional issues, and we
9 certainly want to, you know, embody all those into the
10 research plan that we possibly can. So that's what we
11 mean by that.

12 MR. WATERMAN: And that's part of that
13 communications thing that I think is really important.
14 If we're not talking to our customer, if you will,
15 then we're not really supporting our customer the way
16 we should be supporting them. So that communications
17 perspective, I've been given the privilege of actually
18 writing up the office letter on memorandum of
19 understanding of Research between us and NRR in this
20 case here. And I have some ideas for how to improve
21 that so we have a much more formalized process of
22 communicating, and working together, and developing
23 projects together up front so that when we actually
24 get into the research it's going down the road that
25 our supported offices actually need it to go down.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: Well surely though
2 -- this is not a comment that directly refers to you,
3 but surely Research has done work for NRR in the past
4 and developed plans. So there must be some sort of
5 communications process in place. You're speaking as
6 if there is nothing there.

7 MR. WATERMAN: No, no, no. It's not that.
8 I'm interested in process improvement as much as
9 possible. I was over in NRR for awhile, and there
10 were some things that I thought might be better
11 implemented, and I want to incorporate ideas of
12 process improvement into our research program, and one
13 of those process improvements is improving
14 communications with our customers.

15 Now, this is -- in the following slides
16 the comments are addressed in the order of the
17 research plan sections -- in other words, Section 3.1,
18 Section 3.2, Section 2, whatever -- beginning with a
19 general comment on this first slide, the progressing
20 through each research program. Within the body of the
21 slides, each comment is summarized as a major bullet,
22 which would be that bullet up there in white. And the
23 research action to address the comment is then
24 summarized in subordinate bullets, which, like green
25 right here.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 Now, this first comment regards how the
2 research plan should be related to the NRC's strategic
3 objectives and supporting strategies. And so, "In
4 Section 4 of the Research Plan, each research project
5 is linked to specific NRC strategic plan supporting
6 strategies for achieving the NRC goals of safety,
7 security, openness, and effectiveness." The other
8 goal was management, but I really had a hard time
9 working these projects into management. An in-depth
10 discussion relating each research project to
11 corresponding strategic plan supporting strategies
12 would have been repetitive and ultimately distracting
13 when you've got 24 projects and you're saying the same
14 thing over and over for each project. The tabular
15 format in Section 4 was considered the best
16 alternative for succinctly relating the strategic plan
17 goals to the research projects. So that's the way we
18 went. At one time I was going to try to roll in those
19 supporting strategies for discussion in our NRC
20 strategic plan document. I just, after about five or
21 six of those projects I thought, gee, I keep saying
22 the same thing over and over. So we just put it down
23 there as identifying it by number, which you can then
24 pick up the NRC strategic plan.

25 CHAIRMAN APOSTOLAKIS: Is there -- It

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

(202) 234-4433

www.nealrgross.com

1 seems to me the hard part would be to take any one of
2 the projects you are proposing and prove that it does
3 not relate to the strategic plan. I mean, safety,
4 security, effectiveness, and openness. Just about
5 anything you say is related to one of those, so I
6 don't understand this comment. It doesn't make sense
7 to me.

8 MR. KEMPER: Well, we might have gone
9 overboard, but we really try to put an effort into
10 each project back in Section 4 of not only identifying
11 the goal, but also the supported strategies. So, yes,
12 might have overdone it, but we thought it was an
13 effort well spent.

14 CHAIRMAN APOSTOLAKIS: Actually, the
15 research plan, it seems to me what you really want to
16 see is what the differential would be, what the
17 improvement would be as a result of each project in
18 safety area, security, and so on, not if they are
19 related. I mean, they are related. We know that.
20 These four objectives of the strategic plan are so
21 broad that just about anything you want is related to
22 those. But when you talk about research plan, you
23 really want to know is it going to revolutionize one
24 area, are we doing nothing there and we're going to
25 know what to do, or as Mike said, we know that we have

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

(202) 234-4433

www.nealrgross.com

1 to follow some high-level process, but the details are
2 not there. This is really what's important, I think,
3 for the research plan to make sure that the reader
4 understands. The reason why we're proposing this
5 project is because in this area we have this need, and
6 that's how we're meeting it. At least that's my
7 impression.

8 MR. WATERMAN: Yes.

9 CHAIRMAN APOSTOLAKIS: So.

10 MR. WATERMAN: Part of linking this to the
11 NRC strategic plan was it's historically that's the
12 way we've always done it in the past.

13 CHAIRMAN APOSTOLAKIS: I understand. I
14 see the word "stakeholders" is not there. Now, is it
15 openness? Was it replaced? There used to be
16 "stakeholders" someplace. Public confidence. Public
17 confidence is now openness.

18 MR. WATERMAN: Those are the title of, you
19 know, the objective --

20 CHAIRMAN APOSTOLAKIS: I'm not asking you
21 to revise that.

22 MR. KEMPER: Thank you.

23 CHAIRMAN APOSTOLAKIS: These are your
24 boundary conditions.

25 MR. KEMPER: Thank you.

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

1 MR. WATERMAN: Now, Section 2, we changed
2 some things in Section 2, which is Objective and
3 Scope. The first comment was to schedule periodic
4 formal briefings for the supported offices on the
5 interim results and status of the tasks. Research is
6 developing more formal processes to improve
7 communications with the supported offices, for example
8 by the creation of a Technical Advisory Group or
9 Groups, project development meetings, project status
10 reviews. One suggestion I have that we may
11 incorporate is to take our monthly status letter
12 reports that we get from our contractors and extract
13 relevant information from those and send it via email
14 to our technical monitors, just so they're kept
15 apprised on a month-to-month basis of what the process
16 -- what project is going on, and how the progress is
17 on that project, and things like that. So those
18 things, that's a good comment there, and it's one that
19 I fully support.

20 The next comment is, "Advanced
21 instrumentation and controls research would also be
22 beneficial for existing plants undergoing digital
23 retrofits." And that recommendation was incorporation
24 in Section 2.2, and out in Section 3.6, which is the
25 Advanced Reactor Section.

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

(202) 234-4433

www.nealgross.com

1 CHAIRMAN APOSTOLAKIS: When do you think
2 we're going to see this revised plan? I don't think
3 we have it.

4 MR. WATERMAN: That's a good question. I
5 think we intend to have all the comments incorporated
6 by the end of this month.

7 CHAIRMAN APOSTOLAKIS: Okay. So sometime
8 in July maybe.

9 MEMBER KRESS: Yes, sometime in July.

10 MR. WATERMAN: Most of them have already
11 been incorporated, but it's just, you know --

12 CHAIRMAN APOSTOLAKIS: That's fine.

13 MR. WATERMAN: And I'd also like to vet it
14 with my supported offices before we send it out to
15 make sure I got their comment correctly, and that I've
16 met all of their concerns, obviously.

17 So anyway, on the second bullet there,
18 these sections were revised to reflect the potential
19 applicability of advanced reactor research products.
20 It was just, I think, adding in a sentence or two on,
21 you know, it could be useful for existing plants.

22 Then we got into Section 3.1, which is the
23 System Aspects of Digital Technology. And the first
24 comment was, "The justification of Section 3.1.1 is to
25 'reduce licensing uncertainty.' And the justification

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 should be focused on safety, improved efficiency,
2 effectiveness, and realism, or openness." And when I
3 went back to look at it, I said yes, heck of a catch
4 there. I incorporated that into Section 3.1.
5 Additional focus was placed on safety, although,
6 because licensing uncertainty is a key issue in the
7 nuclear industry with regard to digital retrofits, the
8 focus on reducing licensing uncertainty was retained
9 in there.

10 MEMBER KRESS: It seems to me like
11 reducing licensing uncertainty, it is kind of a focus
12 on safety, and efficiency, and effectiveness. That's
13 what you have to deal with.

14 MR. WATERMAN: That's correct, but I think
15 the issue with reducing licensing uncertainty revolves
16 around that producing of review procedures. So that
17 when a licensee submits a report, they know how it's
18 going to be reviewed step-wise.

19 MEMBER KRESS: I see.

20 MR. WATERMAN: So that, you know, right
21 now, you know, one of the things a licensee or a
22 vendor asks when they do their kick-off meeting, they
23 come in and they present their topical report, or
24 whatever they're proposing that they're thinking about
25 implementing. One of their questions near the end of

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

(202) 234-4433

www.nealrgross.com

1 the meeting is always who's going to do the review.
2 Now why would they ask a question like who's going to
3 do the review? What difference does it make, right?
4 Well, the reason they ask that is they know different
5 reviewers have different slants on things, and they'd
6 like to know what game they're going to be playing.
7 So, you know, we're trying to reduce some of that
8 uncertainty there. We'll all follow the regulations,
9 but you know, some people are a little bit more tuned
10 to one area than they are to another area. That's
11 just human nature.

12 CHAIRMAN APOSTOLAKIS: Maybe some people
13 are uncomfortable with the words "reduce licensing
14 uncertainty". Maybe you can turn it to a more
15 positive statement, and say "contribute to regulatory
16 stability." Would that be better?

17 MR. WATERMAN: Yes.

18 MR. KEMPER: Sure.

19 MR. WATERMAN: I don't like to put
20 negatives.

21 CHAIRMAN APOSTOLAKIS: Because you know,
22 this implies there is now uncertainty, and why do you
23 have uncertainty, this and that. Whereas if you say
24 I want to improve stability, that's more positive.

25 MR. WATERMAN: Although there's an

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

(202) 234-4433

www.nealrgross.com

1 implication there that we -- I know what you mean.

2 MR. KEMPER: Good comment, thank you.

3 MR. WATERMAN: Let's see. I'm going to
4 get the transcript anyway, so I'll pick it up out of
5 the transcript.

6 CHAIRMAN APOSTOLAKIS: Yes, we have a type
7 of redundancy here. See both of you are taking notes,
8 and there's going to be a transcript.

9 MR. WATERMAN: The next comment was, "The
10 Research Plan and Statements of Work should include
11 digital technology involving byproduct materials."
12 When I went back through there, I realized, wow, I
13 left a lot of our byproduct materials users out of the
14 plan unintentionally. And so I incorporated, you
15 know, 'This research will support nuclear power plant
16 licensing and byproduct materials users,' things like
17 that. I did that in Sections 3.1.3, 3.1.6, 3.2,
18 3.3.2, and other sections as appropriate to bring that
19 stakeholder more into the Research plan.

20 Now, "The state-of-the-art in software
21 engineering may not be sufficiently matured for" and
22 I put in brackets there "[quantitative] digital safety
23 system reviews. This concern applies to the
24 activities described in Sections 3.1.3, 3.2.1, 3.2.2,
25 3.3.4, and 3.6.3." And the recommendation was

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 incorporated. That statement was incorporated into
2 those sections, and various methods will be validated
3 as part of research and before recommendations are
4 made to develop digital safety system review
5 procedures. So the state-of-the-art may not be
6 sufficiently matured, but that's what research is
7 there to do, is to mature the process, and find out if
8 that statement is in fact true.

9 CHAIRMAN APOSTOLAKIS: But I don't
10 understand the meaning of this statement. It means
11 the state-of-the-art is not sufficiently matured,
12 therefore do nothing? Is that really the implication
13 here?

14 MR. WATERMAN: Well, I didn't want to say
15 that.

16 CHAIRMAN APOSTOLAKIS: This is probably
17 the only comment that tells you that you need the
18 plan.

19 MR. KEMPER: Well, I think the comment
20 really was rooted in this. This technology may not be
21 sufficient to implement these types of tools and
22 processes that we're considering here. But as you
23 say, it's -- that's exactly why we're doing --

24 CHAIRMAN APOSTOLAKIS: This is the only
25 comment --

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

(202) 234-4433

www.nealrgross.com

1 MR. KEMPER: -- and develop the
2 technology, and you're going to hear many different
3 versions of that in the next several presentations
4 that we're going to make over the next day and a half.

5 CHAIRMAN APOSTOLAKIS: However, there is
6 an implication perhaps that other people are
7 developing the state-of-the-art, and all we do is take
8 it and adapt it to our needs? I don't believe that.
9 Because a lot of the models we're using were developed
10 under the sponsorship of the Office of Research. Not
11 out of the blue, of course. I mean, they are always
12 building on existing methods, but this is really a
13 strange comment. For the Research plan. It's a true
14 statement, but for the Research plan it's a strange
15 comment.

16 MR. WATERMAN: Well, it was a response to
17 the Research plan from one of the supported offices.
18 And we're working on that issue there, but you know,
19 mind you, the comment was a lot bigger than this. And
20 I think what Bill said was -- what the supported
21 office was trying to say is that we're talking about
22 going out and getting tools, for example. Well, how
23 do we know the tools are even mature enough to do
24 this. So, you know. And so that's part of our job is
25 to find out.

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: That's what
2 Research is all about.

3 MR. WATERMAN: That's right.

4 CHAIRMAN APOSTOLAKIS: You make them
5 mature.

6 MR. KEMPER: I think we're all --

7 CHAIRMAN APOSTOLAKIS: And besides, you
8 know, we never rely on a single method in this agency.
9 I mean, you know, quantitative methods may be one
10 input to the integrated decision-making process.
11 Words made famous by this agency.

12 MR. KEMPER: Exactly.

13 MR. WATERMAN: And the final comment in
14 Section 3.1 dealt with Section 3.1.6. "Section 3.1.6
15 is not clear on how proprietary restrictions for 'COTS
16 operating systems' can be resolved in a way that can
17 improve the assessment of digital systems." So
18 Section 3.1.6 was revised to reflect that comment,
19 that not all operating systems are proprietary, and to
20 address issues regarding features of operating systems
21 that may adversely affect safety. What we really want
22 to know is for those operating systems you can look
23 at, what things ought you to be looking for that could
24 adversely affect safety such that you can bring it to
25 the vendor's attention so that the vendor can correct

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 that potential safety issue.

2 And nuclear industry digital system
3 developers have expressed a willingness to allow
4 access to proprietary operating system design and
5 development. The platform vendors have all done that.
6 They've opened it up, and we review whatever we want
7 to look at. It's when you get somebody like, say, an
8 Allen-Bradley, a PLC goes in for a load sequencer,
9 Allen-Bradley is a little bit more reluctant to allow
10 us to peel back the lid, if you will. They have a
11 small stake in the nuclear industry. They sell most
12 of their stuff to much bigger customers. Dealing with
13 those kinds of vendors is an issue, and I think that
14 was probably the focus of this comment, was that when
15 somebody is coming in with -- load sequencer is the
16 one that comes to mind. People are going to digital
17 load sequencers. They'll get an Allen-Bradley PLC, or
18 Modicon, or something like that. And those vendors
19 just, sometimes they don't want us looking at their
20 operating system. That's proprietary information and
21 they -- we have to do other things, like COTS-
22 dedication process and things like that.

23 Now this first comment in Section 3.2
24 actually belongs in the next section on PRA. It just
25 goes to show you how PRA can sneak into software

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

(202) 234-4433

www.nealgross.com

1 quality assurance issues. I'll address this comment
2 in the next slide, so we'll start with the second
3 bullet that says, "Link the objective of Section 3.2.3
4 to safety, improved efficiency, etc., and explain how
5 NRC reviews can be improved to assess self-test
6 features." Section 3.2.3 was lengthened to discuss
7 the development of technical guidance regarding the
8 use and review of self-testing features in digital
9 safety systems. I suspect in future conversations
10 we're going to have with our supported offices that
11 section may be enhanced some more. What we're really
12 trying to address here is, like operating systems,
13 what features in self-testing do you need to look at,
14 what features are appropriate for self-testing, and
15 which features probably ought to not be used in self-
16 testing.

17 My experience with the digital safety
18 system failures that I've seen in the nuclear industry
19 is it's always been self-testing features that have
20 caused the cotton-picking failure. When we go out to
21 review these systems, typically we don't have enough
22 time to review every requirement in the system, so
23 naturally we start by looking at the safety
24 requirements, right? And we do our threat audits on
25 safety requirements. Well, when you compare how much

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

(202) 234-4433

www.nealrgross.com

1 software addresses safety systems, and how much
2 addresses self-testing, you're like holy smokes.
3 You've got this little bit of safety feature software,
4 and this great big chunk of self-testing software
5 that's supposed to make the product more reliable, and
6 all the errors seem to be cropping up over in self-
7 testing. So maybe we need some additional guidance on
8 how to approach -- get our arms around that self-
9 testing issue a little bit better.

10 The two failures I can think of that were
11 caused by self-testing that I was directly involved in
12 was the Turkey Point load sequencer. The self-testing
13 feature locked out HPI in the system, with the intent
14 that since it was continuous testing, it would only be
15 locked out a little bit, and then if a signal came in,
16 you know, nobody addressed what happens when a trip
17 signal came in. That was one of those systems that
18 it'd just stop the self-testing and start the process,
19 as opposed to the approach that's now being taken by
20 all of the vendors. And sure enough, the HPIs didn't
21 get unlocked, and Turkey Point discovered that when
22 Unit 4 was down, and one of their tests is to see if
23 they can use Unit 3 HPI, and the crazy thing wouldn't
24 start because the load sequencer wouldn't unlock.

25 CHAIRMAN APOSTOLAKIS: I read about it in

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

(202) 234-4433

www.nealrgross.com

1 the report, and it was very, very interesting. And
2 then the question came to my mind, to what extent is
3 operating experience, nuclear and non-nuclear, driving
4 the plan. Do we need to know that, or it's something
5 -- it's just another project?

6 MR. KEMPER: Actually --

7 CHAIRMAN APOSTOLAKIS: This pointed out to
8 me, you know, the real need of understanding the
9 timing of things, and so on. So?

10 MR. WATERMAN: I think NRR's got a pretty
11 good handle on the timing issues. I mean, when I
12 reviewed the Siemens Teleperm XS, that was a big
13 issue, was how are they timing all of this, what gets
14 scheduled in for calculating trip, how do they
15 schedule in the software testing stuff. Paul's done
16 the same thing.

17 CHAIRMAN APOSTOLAKIS: But the question is
18 broader though.

19 MR. KEMPER: Well, the use of operating
20 experience for digital systems failures is certainly
21 an essential element of trying to put together a
22 priority system and specific tasking of the Research
23 plan. Unfortunately, there's not a good user-friendly
24 source, if you will, a readily available source of
25 that information available to us. There's numerous

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 places, you know. We have our LER database, INPO has
2 its EPIX, etcetera, etcetera. But when you go look at
3 these information sources, it's very common that
4 there's just not enough detail to fully understand and
5 appreciate the mechanics of the failure itself. In
6 fact, we've got a project which we've kicked off
7 called the COMPSIS project. We're working with the
8 Halden Reactor program to put together such a
9 database, you know, with several international
10 organizations participating for just this reason, so
11 we can use it to better refine our research efforts in
12 the deterministic world as well as the probabilistic
13 world.

14 CHAIRMAN APOSTOLAKIS: Does the non-
15 nuclear world have any general conclusions from their
16 operating experience that we can take advantage of?

17 MR. KEMPER: Well, I believe that Todd
18 will speak to that a little bit in his presentation
19 tomorrow afternoon. That's one of the taskings in his
20 project. But there are problems with that. I'll just
21 kind of -- I don't want to steal too much of your
22 thunder here, but different systems are qualified to
23 different levels of quality, right? We in the nuclear
24 industry of course set very high standards of quality,
25 so when you try to compare failures of the same

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 platform being deployed across the process controls
2 industry as a whole, it's difficult really to make a
3 key judgment on the reliability of that equipment.

4 MEMBER WHITE: But what conclusion do you
5 draw from that? Do you conclude therefore that you
6 shouldn't look at that information, or just that it's
7 hard to do?

8 MR. KEMPER: No. You should look at it,
9 but you have to really evaluate it carefully to make
10 sure you fully appreciate the ramifications of what
11 you're seeing.

12 CHAIRMAN APOSTOLAKIS: We'll hear about
13 it.

14 MR. KEMPER: Yes.

15 MR. WATERMAN: The other failure that I
16 could think of is the ABB-Combustion Engineering
17 developed an oscillation power range monitor for
18 boiling water reactors. And that was a system that
19 used master-slave microprocessors to check each other,
20 make sure the channel was operable. And there was a
21 problem on the 286 microprocessor chip that they were
22 using with baton-passing. I don't want to get into a
23 lot of detail on it, but what happened was because
24 they had a slave processor, a self-testing feature if
25 you will, the priority baton-passing down at the chip

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 level had a defect in it, and sometimes it wouldn't
2 pass the priority baton back to the other features in
3 that microprocessor, hung the microprocessor on a
4 random basis depending on when you interrupted. And
5 it took them about 10 months to work out that problem.
6 That was all because they implemented a self-testing
7 feature. So there's some issues with self-testing
8 that we really need to get our arms around, and maybe
9 do some more study on that.

10 In Section 3.3, which is Risk Assessment
11 of Digital Systems --

12 CHAIRMAN APOSTOLAKIS: That's not a good
13 title, is it? What do you mean by digital system?
14 Building the hardware?

15 MR. WATERMAN: Yes, sir. It's hardware
16 and software. It's not just software.

17 CHAIRMAN APOSTOLAKIS: But not the
18 hardware -- not just the computers.

19 MR. WATERMAN: Well, it's not just the
20 computers, that's right sir. For me a digital system
21 is a system that consists of microprocessors
22 supporting hardware, and the software integrated into
23 that. It's not just software and hardware. It's the
24 software integrated with the hardware.

25 CHAIRMAN APOSTOLAKIS: Some people might

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

(202) 234-4433

www.nealrgross.com

1 argue that even for that digital system you shouldn't
2 really talk about risk assessment, that you should
3 talk -- I mean, if you want -- you should talk about
4 a high-pressure injection system that utilizes digital
5 technology and see then -- you do a risk assessment of
6 the whole system, and eventually the whole plant.
7 That prejudices what the -- I know that you don't have
8 any ulterior motives behind this, but I'm just
9 pointing out that there is some --

10 MR. WATERMAN: We know the device is
11 digital safety systems, so I thought putting "safety"
12 in there was kind of redundant. And I could have said
13 "risk assessment of software and hardware, and
14 software integrated with hardware" but for me "digital
15 systems" pretty much wraps that up.

16 CHAIRMAN APOSTOLAKIS: Anyway, we'll see.
17 We'll see --

18 MR. KEMPER: Steve is going to provide an
19 overview later on today of what this is all about,
20 this section of the plan.

21 MR. WATERMAN: So the first comment is
22 "The plan should recognize that integrating digital
23 systems into PRAs may not be practical and that a PRA
24 may not be an efficient or accurate tool for digital
25 system reviews." Of course, that's always one outcome

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 of your research. And we acknowledge that potential
2 conclusion. We incorporate it into the plan that, you
3 know, we may find out that PRAs are not the
4 appropriate way to do it. But this issue ultimately
5 will be addressed by the risk research projects.

6 The second bullet is "Include the
7 integration of external events, environmental, and
8 security issues unique to digital system risk into the
9 discussion of PRAs." Section 3.3.2 was revised to
10 state that these failure modes will be evaluated as
11 part of the investigation of digital system failure
12 assessment methods. However, the initial development
13 efforts will exclude these external events, etc.,
14 until the methodology is sufficiently developed to
15 address these additional issues. We're not just going
16 to throw everything into the pot and then try to do
17 one big research job with all of these different
18 factors in there, you know. So small steps. Get to
19 where you do something well, and incorporate the next
20 issue.

21 The next two comments are, "The goal of
22 the Section 3.3.3 research should be to provide
23 methods for incorporating a digital component or
24 system into a PRA. And in addition, acceptance
25 guidelines should be considered as part of the

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

(202) 234-4433

www.nealrgross.com

1 deliverable." And we agree with that, and we went
2 ahead and incorporated those comments.

3 CHAIRMAN APOSTOLAKIS: What acceptance
4 guidelines are these?

5 MR. WATERMAN: It's the acceptance
6 guidelines for -- Steve can address that much better
7 than I can.

8 MR. ARNDT: These would be issues such as
9 what is the level of detail that you need for a system
10 reliability model that includes digital components,
11 what level of interactions between the process and
12 between the various variables are necessary, if you're
13 going to use the 1.7.4 criteria how do you interpret
14 it for digital systems, or do you need to interpret it
15 for digital systems.

16 CHAIRMAN APOSTOLAKIS: So you're really
17 referring to the quality of the analysis?

18 MR. ARNDT: Yes.

19 CHAIRMAN APOSTOLAKIS: I think maybe you
20 should use those words. Because acceptance guidelines
21 usually means, you know, delta CDF.

22 MR. ARNDT: Yes, but there are other
23 things included, like how do you interpret the
24 defense-in-depth requirements in 1.7.4. But yes,
25 we'll take that into consideration.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: It's important not
2 to use a word for too many meanings -- with too many
3 meanings.

4 MR. ARNDT: Okay.

5 MR. WATERMAN: So as I interpret really
6 your comment, Professor Apostolakis, is we need to
7 define what acceptance guidelines are.

8 CHAIRMAN APOSTOLAKIS: Well, use other
9 words.

10 MR. WATERMAN: Flesh that out a little bit
11 more.

12 CHAIRMAN APOSTOLAKIS: We don't need --
13 because usually, you know, in this context we mean
14 guidelines regarding the acceptability of the change
15 in terms of the risk metrics, or something else.
16 Because the same thing applies to -- I mean, it's like
17 Regulatory Guide 1.200, along those lines? What do we
18 expect to see in the analysis?

19 MR. ARNDT: Yes. It's also along the
20 lines, if you look at 1.75, 1.76, 1.77, those kinds of
21 issues.

22 CHAIRMAN APOSTOLAKIS: Yes, yes, okay,
23 good.

24 MR. WATERMAN: The next comment, "Section
25 3.3.3 should be clarified to reflect potential

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

(202) 234-4433

www.nealrgross.com

1 capabilities and to ensure 'risk' is not used in the
2 plan as a synonym for 'safety.'" And Section 3.3.3
3 was revised to reflect the comment, and then the
4 Research plan was revised to ensure that the term
5 "risk" is used where "risk" is required, and "safety"
6 is used where the term "safety" is required. And
7 there were places where that had to be changed.

8 The next comment, "Risk assessment should
9 investigate advantages and disadvantages of analog and
10 digital system architectures, and implementation
11 characteristics in our PRAs." Section 3.3.4 was
12 revised to include a discussion on evaluation of an
13 analog Reactor Protection System, and an analog
14 feedwater control system for comparison with
15 equivalent digital systems to see what the delta was
16 between looking at a PRA for your good old analog
17 system, and how does a digital system change that PRA.
18 So we've already got something in the shop for doing
19 that, and we just needed to include that discussion in
20 the plan. And so ongoing research is addressing the
21 suggested approach.

22 And the last bullet in Section 3.3 is
23 "Justify Section 3.3.4 statement that digital
24 reliability assessment methods will reduce staff
25 review effort by 20 to 30 percent." You know, I don't

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

(202) 234-4433

www.nealrgross.com

1 where I got 20 to 30 percent to tell you the truth.
2 We threw it out of there, took it out. At one time I
3 thought that was a good number, but I was thinking
4 about tools, and how much they might have been able to
5 allow me to review so much more. And I came up with
6 an estimate, but I took it out of there, because I
7 really couldn't back it up by anything really hard and
8 firm.

9 CHAIRMAN APOSTOLAKIS: Actually, they went
10 on and said that in fact you may increase staff review
11 effort. You remember that?

12 MR. WATERMAN: I would expect us to
13 increase.

14 CHAIRMAN APOSTOLAKIS: At the beginning
15 you should.

16 MR. WATERMAN: Yes.

17 CHAIRMAN APOSTOLAKIS: Because you're
18 adding more. But an important element -- I mean, the
19 staff review effort should not be the only metric
20 here. We also want to do it right.

21 MR. WATERMAN: As a matter of fact, I
22 don't think tools are ever going to replace the old
23 eyeballs on the review. They'll augment. They'll do
24 some things for us that maybe we couldn't do as fast,
25 but when I went through reviews of a safety system,

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 and I was going through a threat audit, where I found
2 most of the mistakes wasn't in like the design
3 document, or the requirements document, it was at
4 interface. All the mistakes start cropping up in
5 those interfaces. How did you get from, you know,
6 requirements to design. And I don't know of any tools
7 that can actually pick that up. And sometimes, to
8 tell you the truth, some of the problems I found, it
9 was just a feeling I had when I reviewed it that
10 something didn't seem right. I don't know a tool
11 that's ever going to replace that, and when I dug
12 deeper, I started uncovering, well, this is where they
13 ran out of money on --

14 CHAIRMAN APOSTOLAKIS: Let me give you a
15 little bit of advice here. When your contractors in
16 the future come to you with Markov models, tell them
17 what you just told us. And see how a Markov model can
18 model that. I'll tell you, it can't. But I'm willing
19 to listen.

20 MR. WATERMAN: of course, in the process
21 of developing the model you learn something about the
22 system.

23 Section 3.4, which is the Security Aspects
24 of Digital Systems. We had some very good comments
25 coming out of this. I'm still working with the Office

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 of NSIR to incorporate additional comments. This is
2 a whole new issue for us, really. The first comment
3 was, "Support development of 10 C.F.R. 73 requirements
4 that implement NRC post-9/11 security-related orders
5 and regulatory guidance." And that wasn't in the
6 original security plan. That took Eric Lee working
7 with me to help flesh that out, and we're working on
8 that now.

9 The other bullet was "Support NSIR
10 development of a comprehensive cyber security plan,"
11 and Eric and I are just now starting to work up the
12 work breakdown structure on that. We had a couple of
13 different ideas, and we need to hammer that down once
14 I get off of the Research plan project.

15 "Section 3.4 should include research that
16 supports industry implementation of NUREG/CR-6847,
17 which is Cyber Security Self-Assessment Method. 6847,
18 if you will, is similar -- when I read it, it
19 impressed me as something very similar to a standard
20 review plan, if you will. It identified things you
21 needed to look at, and what was important, and those
22 kind of things. But when it got right down to, well,
23 how do I actually do that, it was like hmm. I don't
24 know. Well, NSIR has stated that a tool is being
25 developed outside through a multi-agency agreement, I

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

(202) 234-4433

www.nealrgross.com

1 guess, that will implement the NUREG/CR-6847 guidance,
2 and they'll use that tool on installations that
3 already have networks. I don't know about -- I think
4 we need to do some research on the networks that are
5 being designed right now so we can catch problems
6 early before they get installed into a plan. But
7 we're focusing a lot more of our research on
8 supporting this NUREG 6847 stuff, and I'll be rolling
9 more of those comments into the plan as I get time
10 before the end of the month, obviously.

11 Next comment was "Section 3.4.2 does not
12 directly support NSIR plans, but it seems prudent to
13 conduct research." This is on electromagnetic
14 vulnerabilities, attack vulnerabilities. And "Though
15 the Commission has not considered EM weapons as a
16 credible threat to nuclear power facilities, some
17 limited anticipatory research in this area is likely
18 to be warranted." In other words, you know, as we
19 find time, it's probably a low priority issue here.
20 As we find time, we should be considering what do we
21 do about low-energy radiofrequency attacks and high-
22 energy radiofrequency attacks.

23 A related comment. "Section 3.4.2
24 describes an assessment of electromagnetic
25 vulnerabilities. How does this activity relate to

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

(202) 234-4433

www.nealrgross.com

1 TEMPEST programs?" TEMPEST is an acronym that came
2 out in like the '60s and '70s. It's dated now. It's
3 the Telecommunication Electronic Material Protected
4 from Emanating Spurious Transmissions. And what
5 TEMPEST really is designed to do is military and all
6 the industries are now looking at, you know, people
7 monitoring from a remote area, and picking up keyboard
8 emanations, and things like that, and being able to
9 take secure information out of a place by remote
10 monitoring. That's what TEMPEST was designed to
11 address, whereas what we're proposing in the research
12 for electromagnetic attack vulnerabilities is
13 completely different. I mean, instead of us worrying
14 about what they're listening to, we're worried about
15 what they're going to do to the instrumentation in the
16 plant. That's the difference between those two. So
17 apparently there was some misperceptions about what
18 electromagnetic vulnerabilities involve, so I tried to
19 clarify that in the Research plan with additional
20 discussion.

21 And the next comment, "Wireless technology
22 and firewalls should be subsets of a network security
23 research project." That was a heck of a good comment,
24 and so what I did was we used to have a Section 3.4.3
25 on wireless network security, and a Section 3.4.4 on

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

(202) 234-4433

www.nealrgross.com

1 network security I believe it was, or something like
2 that. Firewalls. And what I did was I combined
3 those, per the recommendation, I combined those into
4 a single section that is just titled network security.
5 So Section 3.4.3 was renamed network security, and the
6 discussion 3.4.4 was then just rolled up as a subset
7 of that research. So that now the new focus, this is
8 one of those revised scope things. The new focus of
9 the new Section 3.4.3 is to address network security
10 issues, including wire communications, wireless
11 communications, and firewalls.

12 The next comment regarding security is
13 "Section 3.4.3 should reference NUREG/CR-6847 which
14 covers the assessment of wireless devices. The
15 proposed research projects described should be
16 informed with the assumption that licensees will
17 implement the cyber security self-assessment tool
18 described in the NUREG." And a related comment,
19 "Firewall Security" -- remember, 3.4.4 is rolled up
20 into 3.4.3 now -- "should state that the NUREG/CR-6847
21 can be applied to assess all digital devices,
22 including firewalls, in nuclear power plants." I
23 guess we'll wait and see how well the tool works out
24 on that. "Revise the proposed research project to
25 develop regulatory guidance on the use of firewalls

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 and expand review guidance to assist reviewers in
2 evaluating the security risk of different firewalls."
3 A terrific comment, and we're going to roll that into
4 the Research plan also.

5 The Section 3.5, Emerging Digital
6 Technology and Applications. "Discuss use of system
7 diagnosis, prognosis, and online monitoring for
8 virtual instrumentation and parameter estimation."
9 And right now, the first version of the Research plan
10 only talked about how it's being used for the
11 diagnosis, prognosis, and stuff. And the comment was
12 brought out that one of the other proposals for using
13 this SDPM is to create virtual instrumentation where
14 you use several different inputs to come up with a new
15 output that could be calculated by it. And so Section
16 3.5.1 was revised to include a discussion on the
17 advantages and disadvantages of using virtual
18 instrumentation. The research objectives essentially
19 remain the same because they were sort of generic
20 objectives, keeping in mind that the purpose of the
21 Research plan was to lay out broad areas, and then
22 when we got into actual research projects we would
23 nail down exactly what products had to be done. So
24 throughout the plan we tried to keep the products
25 generic enough that the plan remained usable for

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 whatever project we got into.

2 The next comment, "The regulatory
3 applicability is not clear for the confirmatory
4 studies of radiation-hardened integration circuits in
5 Section 3.5.2." We've had discussions with the
6 commenter on it -- point out that microprocessors, you
7 know, the old let's radiation-harden it was let's hit
8 it with everything we've got, good hard radiation,
9 we'll see how well it works out. Now, some of the new
10 microprocessors, they're kind of immune to the hard
11 radiation, but if you put them under low dose, over
12 time they kind of go to pieces. Kind of an
13 interesting phenomena that they have more sensitivity
14 to low dose rates than they have to high dose rates.
15 I don't know the reasons for that, to tell you the
16 truth, but you know. It is interesting. So when I
17 brought that out, I think we're hammering that comment
18 out. The tasks and products were revised to reflect
19 the focus on guidance for the staff, and discussions
20 with the supported offices, you know, as I say, we are
21 clarifying that issue. You know, our old techniques
22 of environmental qualification for radiation may need
23 to be amplified somewhat to account for this low dose
24 rate sensitivity.

25 And the next comment was -- this is all in

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

(202) 234-4433

www.nealgross.com

1 Emerging Digital Technology and Application --
2 "Application Specific Integrated Circuits and Field
3 Programmable Gate Arrays described in Section 3.5.5
4 are not currently used in generically-qualified safety
5 platforms." That comment was wrong, but the original
6 comment before it was revised brought out that we've
7 already reviewed some of this stuff. But all I had to
8 go on was this comment until I actually talked to Paul
9 Loeser and he showed me how it was misconstrued.

10 "Include, early on, an assessment of the
11 existing or potential uses of this equipment in power
12 reactors." The first paragraph was revised to
13 reference current and future applications of ASICs and
14 FPGAs. For example, I believe ASICs were used in the
15 old Westinghouse 7300 Reactor Protection System.
16 Westinghouse did a lot of work on Ovation. I think
17 Eric Lee reviewed that when he was over in NRR.
18 Ovation was an ASIC application. Toshiba I believe is
19 coming in with field-programmable gate arrays platform
20 applications. So the stuff is there, it's getting
21 pretty close, and we probably should've started this
22 research some time ago, but you know, nothing like now
23 to get started.

24 Section 3.6, Advanced Nuclear Power Plant
25 Systems. "Advanced instrumentation and controls

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

(202) 234-4433

www.nealrgross.com

1 research would also be beneficial for existing plants
2 undergoing digital retrofits." And that
3 recommendation was incorporated in there. I added
4 some additional words in there, but we addressed that
5 earlier.

6 We had some general comments from NMSS
7 fuel cycles people. "Review guidance in NRR SRP has
8 been used recently by NMSS/FCSS for digital system
9 reviews." Remember, I added that comment earlier, and
10 Professor Apostolakis practically pointed out the
11 unusualness of that comment. And so I revised Section
12 1.4 to state that NRC is conducting research to
13 continually augment and supplement NRC capabilities.
14 I can't emphasize that enough. We're augmenting and
15 supplementing. We've got processes in-house. What
16 we're trying to do is improve processes.

17 "NMSS/FCSS Regulations in 10 C.F.R. 70 are
18 based on a risk-informed approach supported by
19 qualitative acceptance criteria. Therefore,
20 quantitative safety assessments and quantitative
21 acceptance criteria may not be useful for the fuel
22 cycle needs." And that's kind of strange. You know,
23 it sort of sent me back. The Research plan projects
24 in Section 3.3. address development of risk-based
25 approaches for licensing digital safety systems. The

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

(202) 234-4433

www.nealrgross.com

1 results of this research may support existing risk-
2 informed licensing processes. But anytime you can
3 move from qualitative to quantitative on your
4 acceptance criteria you're taking a big step, in my
5 opinion, toward improving your process. For me,
6 qualitative acceptance criteria are, like I said,
7 'this system is swell.' That's a qualitative
8 assessment. 'This is a great system,' that's another
9 qualitative assessment. So I'd like to get us more
10 toward a 95/95 type acceptance criteria, 95 percent
11 confidence that it's 95 percent good.

12 MR. KEMPER: But I guess the key here is
13 that our plan certainly has a risk component to it.
14 And so we will look at fuel cycle facilities and see
15 what we can do for them when that time comes.

16 CHAIRMAN APOSTOLAKIS: And we will pay
17 attention to it.

18 MR. KEMPER: Absolutely.

19 MR. WATERMAN: NRR PRA boys had a general
20 comment, or one person had a general comment. "The
21 terms 'software reliability' and 'software quality'
22 are used somewhat interchangeably." And the Research
23 plan was revised to ensure there is a clear
24 distinction between the use of the term "reliability"
25 and the use of the term "quality." As I recall, we

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 have a project that used metrics, and what they're
2 saying is they would use the metrics to predict
3 reliability. And I think maybe you can use the
4 metrics to predict quality, but I don't know about
5 reliability. I don't know that quality and
6 reliability are always directly related. I mean, you
7 can have a quality system that doesn't do nearly what
8 you want it to do, but it still works every time.

9 In summary, as I presented earlier, we had
10 34 comments from NRR, NMSS, and NSIR. Those were the
11 formal comments. Thirty-one of the comments were
12 incorporated into the Research plan. RES revised the
13 Research plan to reflect the need for additional
14 information in several areas on the basis of
15 communications with the supported offices that I
16 really would like to see continue. And the Research
17 plan will continue to be updated in response to
18 communications with the supported offices as new needs
19 are identified and as research projects are completed.
20 And that's the end of the presentation, Dr.
21 Apostolakis.

22 CHAIRMAN APOSTOLAKIS: Thank you.

23 MR. WATERMAN: So we're working
24 aggressively to incorporate the comments. Sometimes
25 I've been known to lose my temper over being

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

(202) 234-4433

www.nealgross.com

1 frustrated, I can't get all the comments I want into
2 the Research plan into the Research plan. But we're
3 working on that issue. And I want the plan to be a
4 good plan, no doubt about it. It also has to be
5 flexible and adaptable. You know, who knows what the
6 next issue coming up is, you know? If we were that
7 smart, we wouldn't have any issues right now, would
8 we? So it has to be flexible enough to accommodate
9 that.

10 CHAIRMAN APOSTOLAKIS: Okay. Thank you
11 very much. I see we have some extra time, so maybe we
12 should invite other people to comment. Mr. Barrett
13 first. Do you have anything to say on this, or do you
14 want to add anything?

15 MR. BARRETT: No, I don't care to add
16 anything at this point. Thank you, George.

17 CHAIRMAN APOSTOLAKIS: Thank you. Mr.
18 Calvo?

19 MR. CALVO: Do you want me to do it from
20 here or come to the table?

21 CHAIRMAN APOSTOLAKIS: It's up to you.

22 MR. CALVO: I'd like to come to the table
23 because I think I need the overhead.

24 CHAIRMAN APOSTOLAKIS: That's fine.

25 MR. CALVO: Okay.

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

1 CHAIRMAN APOSTOLAKIS: Thank you,
2 gentlemen. Appreciate it.

3 MR. CALVO: If you have no objection, I'd
4 like Mr. Marinos and Mr. Loeser to join me at the
5 table, if that's okay.

6 CHAIRMAN APOSTOLAKIS: Fine. How long is
7 your presentation?

8 MR. CALVO: As long as you want it.

9 CHAIRMAN APOSTOLAKIS: No.

10 (Laughter)

11 CHAIRMAN APOSTOLAKIS: Well, actually,
12 yes.

13 MR. CALVO: I'll tell you one thing. I'll
14 send you the slides, of course the slides for the
15 presentation, also for the backdrop slides. I went
16 through the presentation. I cut out about five or six
17 slides. So it's very short.

18 CHAIRMAN APOSTOLAKIS: Five or six is
19 fine.

20 MR. CALVO: So actually, I will be
21 addressing what we do. I'll be responding to some of
22 the comments that Research has.

23 CHAIRMAN APOSTOLAKIS: So clearly identify
24 yourself for the record.

25 MR. CALVO: Sure. My name is Jose Calvo.

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

(202) 234-4433

www.nealrgross.com

1 I'm the branch chief of Electrical Instrumentation and
2 Control Branch in the Office of Nuclear Reactor
3 Regulation.

4 CHAIRMAN APOSTOLAKIS: And the other two
5 gentlemen?

6 MR. MARINOS: My name is Evangelos
7 Marinos. I was the section chief in the Electrical
8 Instrumentation and Control Systems Branch. I was the
9 section chief of the Instrumentation Section until May
10 16, when I was reassigned to a new position.

11 CHAIRMAN APOSTOLAKIS: Thank you.

12 MR. LOESER: My name is Paul Loeser. I'm
13 a technical reviewer within the Instrumentation and
14 Controls System, and at the moment, the remaining
15 digital reviewer.

16 CHAIRMAN APOSTOLAKIS: Thank you very
17 much. Okay, let's go on. Do we have copies of these
18 slides?

19 MR. CALVO: Yes, you should have.

20 MR. SNODDERLY: George, what we'll do is
21 these slides that are presented, we'll pass out to the
22 members and to anyone.

23 CHAIRMAN APOSTOLAKIS: Well, we don't have
24 --

25 MR. CALVO: You should have copies of

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 these slides because it was part of the package of the
2 slides.

3 CHAIRMAN APOSTOLAKIS: Speak into the
4 microphone, Mike.

5 MR. SNODDERLY: I said what I'd like is
6 for you to present that material which you'd like to
7 present, and then that would be publicly available.
8 Right.

9 MR. CALVO: Okay. I guess what I'd like
10 to do is what we do, what the NRR does. We've been
11 doing that for several years. The staff reviews the
12 process, not the product. And our process is
13 contained in the standard review plan. They tell us
14 how he's implementing the requirements -- not the
15 requirement, the guidance of the criteria set forth in
16 the standard review plan. So we leave it up to them.
17 We don't tell them how to do it, we review what is
18 there. And after we review the process, the lifecycle
19 process, how we are putting a system together. We go
20 back in for audits. We take a piece of the software,
21 we go through it, and we determine how that thing is
22 consistent with what they tell us. That's what we do.
23 Now -- go ahead.

24 CHAIRMAN APOSTOLAKIS: You are telling us
25 what you do. Is there an implication here that this

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 is good enough?

2 MR. CALVO: No.

3 CHAIRMAN APOSTOLAKIS: Okay. Let's go on
4 then.

5 MR. CALVO: I'm saying this is what we do
6 --

7 CHAIRMAN APOSTOLAKIS: No, that's fine, as
8 long as we understand what you mean.

9 MR. CALVO: And now I'm going to tell you
10 -- the next one will tell you what we have done. This
11 is the systems that we have done. A Westinghouse. A
12 more recent system was the Siemens, we have reviewed
13 their platform. The Westinghouse also, ASIC. This is
14 a functional modular implementation of a computer-
15 based system. We issued a Common Q for Westinghouse
16 on the combustion system, and that was Combustion, now
17 Westinghouse has combusted together, and recently we
18 have reviewed Triconex. We have reviewed the
19 platform. We have reviewed the operating systems.

20 It's very interesting to note that the
21 Siemens, the Westinghouse, and the -- wait, no, the
22 Westinghouse and the Common Q, the operating system is
23 not being developed in this country. It's developed
24 by the Germans and the Belgians. Some kind of way the
25 high level preparers are getting involved in the

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

(202) 234-4433

www.nealrgross.com

1 operating systems, it was done in this country. So
2 sometimes we had to go to Germans. We asked the
3 Germans to come over here so we can ask some questions
4 relevant to the operating system. So we have reviewed
5 that the Triconex is the one that is actually located
6 in Los Angeles, California, and they do that on their
7 own. They have their own capability to do all these
8 things. All the others, they don't have it. We
9 invite them over, we ask them questions, but they're
10 really platforms. Platforms tell you the operating
11 systems, and we look for things like we don't like
12 interruptions. We like for you to continue in a
13 closed loop, which is normally about 50 milliseconds.
14 It's a very simple system, the Reactor Protection
15 System and the Engineered Safety Feature System. All
16 you do, you go around for 50 milliseconds. And when
17 you don't want to go, you hang around there. Don't go
18 anywhere and come back, because you may not know where
19 you left it, and then you get into problems. So it's
20 a very simple system, very simple. The computers they
21 use are the very lowest speed computer, because the
22 lower the speed of the computer, the higher the
23 reliability. So we're not talking about these 1
24 gigahertz. We're talking about 30 megahertz. 30
25 megahertz. They're very slow, and they're very

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 reliable. And you don't want to go up with it,
2 because then it factors into the variability.

3 So this is the one that we have done.
4 This is the one we plan in the future. HF Controls
5 topical report. This is what is happening there. One
6 thing I would like to bring out. I think the one that
7 you're very much interested on getting involved is the
8 Oconee. The Oconee challenged somewhat underlying
9 principles and precepts of how you implement
10 instrumentation and control systems, whether analog or
11 digital. It's a very important one. The RPS, see
12 we're thinking about the four echelons of defense-in-
13 depth. We've got control systems, we've got
14 protection systems, we've got engineered safety
15 feature systems, and we've got display
16 instrumentation. You've got the echelons that give
17 you that kind of protection. What we want to be sure
18 is that if one fails, you've still got the other three
19 who are watching over that failure and can help you.
20 In the Oconee, the combined are two echelons, but they
21 combine protection and mitigation. And now we are
22 concerned about that. Maybe we're going too far with
23 that.

24 Now, I guess the question was asked today
25 that -- by the way, Mike Waterman did a superb job.

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

(202) 234-4433

www.nealrgross.com

1 A very positive presentation. I think I like the idea
2 that maybe we're getting together now instead of
3 moving apart. But I guess the question was asked,
4 they almost asked you who is going to do the review.
5 So some kind of way they figure out how they can get
6 around it. They don't have to ask that question
7 anymore because we've only got one left, you see. So,
8 one question that we don't have to answer, all right?

9 Okay, that's fine. So the other one I'd
10 like to show you is our perception of what we feel.

11 CHAIRMAN APOSTOLAKIS: Now, the Oconee
12 license amendment request I bet is not risk-informed.

13 MR. MARINOS: No, it is not.

14 MR. CALVO: What?

15 MR. MARINOS: It is not risk-informed.

16 CHAIRMAN APOSTOLAKIS: It is not risk-
17 informed, because we don't have any way of calculating
18 --

19 MR. MARINOS: We're using the conventional
20 approach that the Standard Review Plan guides us with
21 to do the review as we have done for the other reviews
22 that Mr. Calvo alluded to.

23 CHAIRMAN APOSTOLAKIS: Right.

24 MR. MARINOS: And this is a process that
25 was developed with the assistance of the ACRS some

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

(202) 234-4433

www.nealrgross.com

1 years back in a number of scientific institutions that
2 helped us develop the approach that we have, which as
3 Mr. Calvo indicated is a process-oriented approach for
4 review.

5 CHAIRMAN APOSTOLAKIS: When was this
6 developed?

7 MR. MARINOS: This was -- the final
8 version of the standard review plan was issued in
9 1997. It started in 1993, if I'm correct, and in '97
10 it was published as a final approach for review. It
11 was shared with a number of countries, in fact, the
12 developed countries, England, France, Canada. And
13 they gave us their advice, their guidance, and we
14 developed that process.

15 CHAIRMAN APOSTOLAKIS: The reason why --
16 well, one major reason why it's not risk-informed is
17 because we don't know how to do it.

18 MR. MARINOS: That's correct.

19 MR. CALVO: That's correct. Maybe one day
20 in the future it will be defined. We're not there
21 yet. We've got to --

22 CHAIRMAN APOSTOLAKIS: No, we will be
23 there someday in the future if we don't keep saying we
24 can't do it, let's not do anything about it.

25 MR. MARINOS: Additionally --

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: I understand what
2 your issues are. I mean, you have to make a decision
3 within a reasonable amount of time, right?

4 MR. MARINOS: This standard review plan
5 has not been fully tested, obviously, in this country
6 as Mike alluded to, Mike Waterman. Duke Power
7 Company's Oconee plant will be one of the best tests
8 for us. However, the senior level scientists under
9 their electrical instrumentation branch, which is a
10 digital, he was assigned, in fact it was recommended
11 by ACRS that he monitor the implementation of digital
12 systems using the standard review plan at any other
13 place where this is being done. And in fact, in
14 Taiwan and in South Korea, they have implemented
15 digital systems in the full scale, and our senior
16 level scientist has monitored that, and the results
17 are very positive in terms of guidance for doing the
18 right thing. So this is what we base the --

19 CHAIRMAN APOSTOLAKIS: Yes. I'd like to
20 know a little more about the Oconee proposal. And we
21 can get the documents, I suppose, and have a look at
22 them.

23 MR. MARINOS: The reviewer is Paul Loeser
24 presently, so he can give you more details about the
25 Oconee review.

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: No, I'd like to get
2 some documents first to read, and maybe in the future.
3 But it's okay, there's nothing proprietary there or
4 anything. I mean, you know, if there is we can look
5 at it. So yes please, coordinate with Mr. Thornsbury.

6 MR. CALVO: The Oconee uses the Siemens.

7 CHAIRMAN APOSTOLAKIS: Yes. No, you said
8 Framatome. Didn't you say Framatome?

9 MR. LOESER: Siemens sold that portion,
10 the instrumentation section, to Framatome. When we
11 started the review it was the Siemens TSX, now it's
12 the Framatome TSX.

13 CHAIRMAN APOSTOLAKIS: Okay. But you had
14 to go to Europe?

15 MR. MARINOS: Yes. Mike Waterman and
16 myself and another employee went to Siemens to monitor
17 there.

18 CHAIRMAN APOSTOLAKIS: The things one has
19 to do. Okay. All right.

20 MR. CALVO: The board will view how we see
21 the standard review plan. As you see, we have
22 reviewed a lot. We have a challenge in the future.
23 And what we're trying to do is trying to align
24 ourselves with the Office of Research. We don't have
25 enough researchers, and they don't have enough

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 researchers. And I don't know why we can't kiss and
2 make up so we can all work together, with the goal of
3 making the NRC look good at the end. I think we're
4 almost there, okay? We have not kissed yet, but we're
5 almost there.

6 CHAIRMAN APOSTOLAKIS: You have kissed,
7 but you have not made up? Is that it?

8 (Laughter)

9 MR. CALVO: That's the toughest part.

10 CHAIRMAN APOSTOLAKIS: Well, your first
11 bullet actually I think is great. I really would like
12 to see that in every project. And that message will
13 be sent loud and clear today and tomorrow. In each
14 project, we want to know -- well, in different words,
15 what are we doing now, what is the agency doing now,
16 why there is a need for improvement, right? The
17 problem to be solved, and how you're going to do it,
18 how you're going to solve it. I think this is really
19 the essence of the Research plan.

20 MR. MARINOS: We have gone through that,
21 and Mike alluded to a TAG, the task action group,
22 whatever.

23 MR. LOESER: Technical advisory group.

24 MR. MARINOS: Technical advisory group.
25 And we did attempt this. In a previous attempt to

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

(202) 234-4433

www.nealrgross.com

1 obtain concurrence from the NRR staff on the plan from
2 2000 to 2004. And we did periodically meet to discuss
3 the various projects that they're proposing, and we
4 didn't reach any conclusions of need on our part that
5 they could convince us that it was there. So this is
6 being proposed again, and I imagine maybe will be more
7 successful.

8 CHAIRMAN APOSTOLAKIS: But what I'm saying
9 is that I also subscribe to this kind of thinking, and
10 we will -- and I'm sure the ACRS, judging from the way
11 they reacted to the human performance research plan a
12 few years ago, they think the same way.

13 MR. CALVO: If I may add, it's very
14 important to know this, because we already review --
15 we only license a platform. We're going to be
16 implementing about a hundred new plants in this
17 country. If we're doing something wrong, we've got to
18 know what it is before we can turn the wheels back.
19 So that's important.

20 CHAIRMAN APOSTOLAKIS: I didn't get the
21 impression from Mr. Waterman that the Research staff
22 doesn't want to do this. I mean, this is a legitimate
23 request. I mean, that's fine.

24 MEMBER BONACA: Yes. I see it more as a
25 clarification. And really, for example, for the SRP

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

(202) 234-4433

www.nealrgross.com

1 he provided an answer to that and said that they're
2 developing procedures, and how to use criteria of the
3 SRP in a consistent way.

4 MR. CALVO: Which is a good -- it's a good
5 comment. And the reason for it, the standard review
6 plan, whether you like it or don't like it, that's our
7 bible, that's our criteria. They're mixing guidance
8 and criteria in there. But we must move ahead with
9 some instability in the process. If we're going to
10 change it, why it needs to be changed, because we have
11 a lot of trouble trying to convince the industry that
12 you've got to change it for these reasons. It's going
13 to cost you a lot of money and delays, and we'd like
14 to know -- and that's the alignment that I'd like to
15 have with Research in that area.

16 MEMBER BONACA: I didn't hear the word
17 "change" in the issue of the SRP. I heard the issue
18 developing a procedure to provide a consistent
19 interpretation. So that could be useful to you, it
20 seems to me.

21 MR. CALVO: That's fine. Which is a
22 healthy review process, which is fine. I've got one
23 more slide. The way we see what quality of research
24 that we need from the standpoint of NRR. I'd like to
25 give you a perspective of how we see the progress of

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 research. And this is the --

2 CHAIRMAN APOSTOLAKIS: Have you seen the
3 movie "Dr. No"?

4 MR. CALVO: Yes, I did. James Bond. I
5 don't know who won at the end, but -- Anyway, this is
6 documented in all these non-concurrence memos that we
7 have issued. It shows you the -- two or three of
8 them, which I believe has something that we feel that
9 has some value. But what is important here is not the
10 memos. What is important here is the fact that yes,
11 we've had meetings with Research, we have worked with
12 them, and I estimate that when you do things at a
13 working level and you start talking to each other,
14 things get resolved. So we're saying here we've had
15 a lot of meetings, and the project was discussed, but
16 final version of the project has not been seen, and
17 therefore may still not meet EEIB expectations. So we
18 look like we're moving in the right kind of direction.

19 Now, there was a comment made that also,
20 you say that informal comments were provided by the
21 Research. So informal comments, it forces the staff
22 to talk to each other, to align with each other. I'd
23 like to propose that we had almost 18 projects that we
24 have not discussed. Why don't we make them informal
25 comments so we can talk about it, and the value of

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

(202) 234-4433

www.nealrgross.com

1 those comments are incorporated into the program when
2 they incorporate comments into the program. We're
3 trying to be treated like the public. When the public
4 provides you comments, we go through all the comments,
5 and we resolve all the comments. We provide an answer
6 to the public.

7 CHAIRMAN APOSTOLAKIS: But let me
8 challenge you there a little bit, Mr. Calvo. I mean
9 you are saying, for example, digital system -- 3.3.2,
10 Digital System Failure Assessment Methods. And you
11 say it's not desirable. Why isn't it desirable? How
12 do you know it's not desirable?

13 MR. LOESER: The question we have here is
14 what are we going to do with it. If we know --

15 CHAIRMAN APOSTOLAKIS: I didn't hear you.

16 MR. LOESER: What are we going to do with
17 it from a regulatory basis? If we know that a
18 particular digital system fails twice as often as
19 different one, we can't tell the licensee not to use
20 the one that fails more often. We can require them to
21 take that into account. We can't --

22 CHAIRMAN APOSTOLAKIS: Is that what
23 "failure assessment methods" means?

24 MR. LOESER: You said 3.3 --

25 CHAIRMAN APOSTOLAKIS: 2.

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

1 MR. LOESER: Oh, failure -- sorry, failure
2 assessment. That has to do with setting up tools for
3 assessing these methods. Once again, I wrote a couple
4 of pages on the use of tools. I have some problems
5 with the concept. If we make the use of a tool
6 mandatory, then we are changing our regulatory method.
7 If we make it advisory, what happens if the tool comes
8 up with one result, and our conventional method of
9 review comes up with another? Tools by their very
10 nature become obsolete at the same rate as the types
11 of things they are judging. If I have a tool to come
12 up with the failure rate of a particular type of
13 microprocessor, that tool is going to become obsolete
14 as the microprocessor.

15 The biggest problem I had with all of
16 these, however, is the way --

17 CHAIRMAN APOSTOLAKIS: Wait a minute, now.
18 You're coming back again to reliability concepts, and
19 this doesn't say that. This says methods of
20 identifying system faults. So you're saying that
21 methods for identifying system faults is not desirable
22 by your branch.

23 MR. LOESER: No.

24 CHAIRMAN APOSTOLAKIS: I am not --

25 MR. LOESER: I didn't say that. What I'm

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

(202) 234-4433

www.nealrgross.com

1 saying is the project, the way it was written with the
2 intended results, or the intended products, and with
3 the type of justification they have listed is not what
4 we would have wanted. It was not discussed with us.
5 We haven't had an opportunity to change it. In some
6 of these instances where we said something was not
7 required, not desirable, we have discussed this with
8 Research. They have either been more specific on what
9 they're really looking for. The one that comes to
10 mind is the one on EMI testing. The project
11 originally indicated they were going to throw open the
12 entire issue of EMI testing, again which has been a
13 number of times. It turns out what they wanted was
14 there's one particular test that they think has a
15 faulty premise. They have reason to believe this, and
16 that's what they want to investigate. Once they
17 stated it like that we agreed that this was a
18 reasonable thing to do.

19 MR. CALVO: Keep in mind one thing. We
20 never saw this research plan. We never saw it. We
21 were not consulted to find out whether we align with
22 each other. So when it's put on the table for us to
23 review it, we had all those comments. This issue,
24 they have discussed it with us, I think we can find a
25 common ground. That's the big problem that we have.

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: So what is -- I
2 mean, the interactions that are happening now that Mr.
3 Waterman talked about should have taken place before.

4 MR. CALVO: That's correct.

5 CHAIRMAN APOSTOLAKIS: That's a reasonable
6 thing to say.

7 MR. CALVO: Agreed.

8 MR. LOESER: And I think if this
9 particular project is modified, states what actually
10 is going to happen, if we have some interaction I have
11 no doubt we can come to some sort of agreement as to
12 what should be done, why it should be done, and more
13 importantly what the results are expected. When they
14 state point blank that a reg guide, or a NUREG, on how
15 this should be done, we question whether this is
16 necessarily the right thing to do.

17 CHAIRMAN APOSTOLAKIS: There are two
18 issues here, it seems to me. One is the view we have
19 on the screen right now. And if I take the words
20 literally, I don't understand why you fail to see how
21 this would be useful. Okay? Methods for identifying
22 system faults it seems to me would be useful to inform
23 licensing systems. On the other hand, what you're
24 saying is that the way the thing was written was not
25 explicit as to what problem we're addressing, why that

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 is a problem, and how they expect to solve the problem
2 in a way that would be useful to you.

3 MR. LOESER: Yes.

4 CHAIRMAN APOSTOLAKIS: And that has a lot
5 of merit in it.

6 MR. LOESER: And I think we said that in
7 each of our non-concurrences, where we stated that we
8 think the solution to this is to get together with
9 Research, discuss each one of these research plans,
10 specify in a bit more detail exactly what they're
11 after, what the products are. I think they should not
12 make the assumption that it will necessarily,
13 particularly when it comes to software metrics, or
14 software PRA type issues. They should say that we
15 will study this, present the reports, and then
16 determine whether or not this should be turned into a
17 NUREG.

18 MR. MARINOS: I'd like to make a last
19 clarification with this language that is used there,
20 system fault. We're not talking any actual physical
21 system fault that they will identify. We're talking
22 about ability to identify errors in the software that
23 conventionally would not be identified by testing, or
24 V&V, or this way. So certain tools are being proposed
25 to be developed so that you can identify hidden errors

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 in the software, not system faults in the way that we
2 interpret the actual physical system fault. We all
3 need to know those if we can find them, but here is
4 something that we're struggling. Research has tried
5 to convince us that there is ways that we can find
6 means by which we can identify those things, and then
7 evaluate them. And as Paul alluded to, these tools
8 that may be developed for a particular application, it
9 will be actually for the same product if the software
10 changes. Certainly it will be not available, and that
11 will be usable for another product. So this is why
12 we're relying on a process in developing those
13 software, and of course, to complement this for
14 security, we apply the defense-in-depth and diversity
15 requirements, manual actions or automatic actions, to
16 cover any uncertainty associated with software.

17 CHAIRMAN APOSTOLAKIS: No. I mean, you're
18 absolutely correct, I mean there is -- we don't know
19 what else to do, and we are doing the best we can. I
20 mean, that's essentially that it is, diversity
21 redundant. But let's not forget, though, that this is
22 how the whole regulatory structure of the industry
23 started 50 years ago, 40 years ago. And then with the
24 advent of risk assessments, we found holes, we found
25 improvements, and so on. And also, in all honesty to

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 this day, the system is still intact. I mean, we are
2 risk-informing it, but not at a very high pace. Well,
3 is it possible then that your traditional
4 deterministic approach might have holes as well, and
5 that if we try to do quantitatively, or develop
6 methods for identifying faults, and go beyond that and
7 do risk assessments, we may find holes. I mean,
8 nobody's perfect, right? And the thing that I think -
9 - don't you think you overreacted?

10 MR. CALVO: No, I'm not. I'll tell you
11 what. I'm not.

12 CHAIRMAN APOSTOLAKIS: Look. It says not
13 desirable.

14 MR. CALVO: Wait a minute. Wait a minute.
15 Like I said before, we're moving ahead. We have
16 reviewed and accepted many systems. And now, as we
17 are responsible and accountable for the implementation
18 of computer systems at nuclear power plants, I'm
19 worried. I'm truly worried. Because there's nobody
20 going behind me and helping me out to tell me you're
21 moving in the right direction. I need that kind of
22 support.

23 CHAIRMAN APOSTOLAKIS: Are you starting to
24 get it now, do you think?

25 MR. CALVO: Well, I hope with your help

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

(202) 234-4433

www.nealrgross.com

1 and this continued communication maybe we're going to
2 get it. But I'm truly worried that we are moving
3 ahead, and all we've got to do is get one system that
4 fails because of the common mode failure. That's the
5 end of the application of computer systems in nuclear
6 power plants. We're going to put them on hold for a
7 long time. And I need their help, but they've got to
8 be focused on helping us out, to validate what we're
9 doing, is it correct. You're right, we've got
10 deterministic. I'm not quite sure if that's correct.
11 I don't know the standard review plan gaps in there.
12 We need them to focus and work with us, not to develop
13 some new techniques and tools to do what? They all
14 have been reviewed. There's nothing else to be
15 reviewed at this time, only advanced reactors. That's
16 something that you can put aside. They have limited
17 resources like we do, and we need that help, we need
18 alignment in here. It's very important.

19 CHAIRMAN APOSTOLAKIS: Well, it seems to
20 me, Mr. Calvo, that your disagreement with the
21 Research staff is more on the process that they're
22 following to develop this research plan rather than
23 the substance. You would like to see it more focused,
24 which is legitimate, but you were really upset because
25 you were not consulted before they put together the

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

(202) 234-4433

www.nealrgross.com

1 first draft. But if one reads your comments, gets a
2 very different impression, that nothing is of any
3 value to you, and that is a little difficult to
4 swallow.

5 MR. LOESER: First of all, that one column
6 that said "desired by NRR" --

7 CHAIRMAN APOSTOLAKIS: EEIB.

8 MR. LOESER: It probably should have been
9 re-termed as -- that we have a user need for it.

10 CHAIRMAN APOSTOLAKIS: Make it more
11 technical.

12 MR. CALVO: Now, wait a minute, you're
13 absolutely correct. This was a calling card. We need
14 a calling card to put it on the table and tell
15 Research, please, align with us and let's work
16 together. That was the calling card. That was it.
17 For an independent panel, you are looking at this, and
18 decide, yes, it looks that way. But that was a
19 calling card, let's start talking. And that was the
20 whole purpose of it. Instead of start talking, it got
21 worse, okay? And now we look like we are talking
22 now.

23 CHAIRMAN APOSTOLAKIS: You are talking.

24 MR. CALVO: Yes.

25 MEMBER BONACA: Another I think really

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

1 actually a discussion between NRR and the Research on
2 these issues by itself is going to improve the
3 agency's capability, because there's going to be
4 communication --

5 MR. CALVO: I agree.

6 MEMBER BONACA: -- and focus, and better
7 understanding of what's needed and what's not needed.
8 So I think --

9 MR. MARINOS: However, the process that
10 we've had in communicating mutual needs is the user
11 need, as Paul alluded to. So we had not expressed a
12 user need because we were comfortable at least right
13 now with the process we have in place through the
14 standard review plan to do reviews. So when we were
15 faced with this research plan, our concurrence, at
16 least for the Electrical Instrumentation Control
17 Branch would have been tantamount to a user need. And
18 we said we have no user need, we don't need this
19 research at this time. What we're doing is sufficient
20 for us to convey to industry a coherent licensing
21 approach. So that was the reason why we didn't concur
22 as a branch on this program, because we had not
23 identified a user need, and that is the only mechanism
24 by which we would concur on a plan. So in an
25 anticipatory research way, we wouldn't object, as you

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 are not objecting. You know, whatever they think they
2 want to do. We don't want to second-guess them, but
3 we certainly didn't want to be second-guessed either.

4 MEMBER BONACA: But in some cases, for
5 example, you know, there has been today we are looking
6 at PRA or risk evaluation as a fundamental support for
7 fire analysis. And yet, there has been a lot of
8 resistance in the past to developing risk-informed
9 approaches to that.

10 MR. CALVO: That's fine.

11 MEMBER BONACA: Now, all I'm trying to say
12 is that oftentimes, you know, you're looking at
13 Research for more long-term, longer-term than you need
14 instantly now. I think, you know, at that point
15 communication is going to clear that issue. And you
16 may agree that something can be done.

17 MR. CALVO: No, I don't disagree with you.
18 I worry about that we move it ahead with a lot of
19 reviews in here, with platform that we can review it,
20 and I need help. I truly need help. This research
21 program is looking from the researcher's standpoint,
22 not from the agency's standpoint. And I just want to
23 start getting together. The latest users needs that
24 you had, which I think you had a copy of it, was in
25 2003. That established priorities, what you're going

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 to do first to help NRR to take care of its customers
2 which are the licensees in this case. And I'm
3 concerned. I'm truly concerned.

4 MEMBER BONACA: I must say, I'm pleased to
5 see this move to yes, and not discussed --

6 MR. CALVO: I agree.

7 MEMBER BONACA: Because when I saw that
8 the first time, reflecting on this, I thought that the
9 "no" meant no need, desired no need, which is don't
10 see any use for it. Now, this being converted into
11 yes, with some changes, is beneficial.

12 MR. CALVO: Right. The "no" as presented
13 indicated that we had trouble with it. When somebody
14 hears you fresh, this is the program plan at Research,
15 tell me what you think about it. So it was no
16 communication. We just could not communicate even at
17 that time, okay? We could not communicate. So we
18 come out with the comments. And that was it.

19 CHAIRMAN APOSTOLAKIS: Okay. Now we have
20 only a few minutes. Have you used all your view
21 graphs or is there one more?

22 MR. CALVO: Almost done. I've got one
23 more.

24 CHAIRMAN APOSTOLAKIS: Okay, one more.

25 MR. CALVO: I'd like to make some

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

1 suggestions for you to consider.

2 CHAIRMAN APOSTOLAKIS: Okay.

3 MR. CALVO: How we can go ahead with this.

4 This is the latest users needs that we had, we
5 prepared, we sent to Research. We need to update the
6 old regulatory guides and go through because that has
7 momentum. We'd like to bring them up to date, which
8 I think Research is doing fine. And I think we can
9 establish some priority which we want to see first.
10 We don't want to review everything for the sake of
11 reviewing it. We want to have certain things in there
12 that we feel are important to our review process.

13 In state-of-the-art, monitor the cutting
14 edge of what is done in other industries and academia.
15 I think it's a good thing for Research. Keep abreast
16 of what is going on out there, and maybe we can find
17 out if something will have some implications on what
18 we have done up to now.

19 The other one, new ways to regulate. At
20 the moment these are primarily software-related.

21 CHAIRMAN APOSTOLAKIS: Let me understand
22 this now, the second bullet, the state-of-the-art
23 stuff. You would expect the Office of Research to
24 produce some sort of a NUREG report, or some document
25 that will summarize what is going on?

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

(202) 234-4433

www.nealrgross.com

1 MR. MARINOS: Yes.

2 CHAIRMAN APOSTOLAKIS: And brief you on
3 that?

4 MR. MARINOS: They have done so. And in
5 fact one statement that was made in Mike's
6 presentation that you commented on about not mature
7 technology yet. It was actually right out of the
8 NUREG that they produced and sent it to us for review
9 about software reliability. And there was a statement
10 there that the technology is not mature yet so we're
11 going to back off a little bit and wait. So that's
12 where the statement came from.

13 CHAIRMAN APOSTOLAKIS: So you appreciate
14 this comment?

15 MR. MARINOS: Yes, we appreciate that.

16 MR. LOESER: This is I think Research
17 Project 372.

18 CHAIRMAN APOSTOLAKIS: Who wrote that
19 report, do you remember?

20 MR. MARINOS: Oak Ridge. I think it was
21 Oak Ridge National Laboratory.

22 MR. LOESER: Actually, I thought it was
23 University of Maryland.

24 MR. CALVO: I know we are running out of
25 time. Let me go back, if you don't mind.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: Yes, go ahead.

2 MR. CALVO: New ways to regulate. We went
3 to the software. It requires that when a method is
4 discussed, we want to know the applicability of the
5 method, what is the guidance. It's very important to
6 distinguish what is guidance, what is criteria that
7 should be used. And I think in our case, the method
8 that we use is the standard review plan. Okay? Maybe
9 somebody can help with this, pick up some gaps and
10 holes in there, and maybe can identify those tools so
11 we can do that.

12 The other point is how do we know that the
13 method is properly applied, and that the licensee
14 knows what he is doing? The acceptance criteria is
15 needed. Okay, we're getting all this -- do you know
16 how many it takes to review one of these systems? The
17 platform? Something over one thousand hours. One
18 thousand hours. And the criteria is about that high.
19 And the guidance is about that high. That is a big
20 help. We can focus on the important things. Help me.
21 I need that help, okay? Right now we review
22 everything, okay?

23 CHAIRMAN APOSTOLAKIS: Yes, but again,
24 excuse me. There is a project somewhere here that
25 says prioritize the thing using risk importance. Do

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

(202) 234-4433

www.nealrgross.com

1 you say that's irrelevant?

2 MR. CALVO: No. Again, go back again, how
3 that project was presented to us. All right?

4 CHAIRMAN APOSTOLAKIS: Okay, okay.

5 MR. CALVO: And then we go back again.

6 CHAIRMAN APOSTOLAKIS: We have settled
7 that.

8 MR. CALVO: The "no" is not no, no, no.
9 It's not ever no. It's tell me -- explain to me why,
10 okay?

11 CHAIRMAN APOSTOLAKIS: Yes, okay. Fine,
12 fine.

13 MR. CALVO: The other one is justification
14 for the rejection of the license submittal if the
15 quality is not present. What is missing, and what is
16 important. We need that kind of help. Otherwise
17 we're going to spend a tremendous amount of time
18 trying to figure out that ourselves.

19 And I think the most important part, the
20 most important part, for Research and NRR working
21 level staff must work together to ensure that the
22 application of the digital technology in nuclear power
23 plants continues to be safe. And that is extremely
24 important, okay?

25 Now, what I would like for ACRS to

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

(202) 234-4433

www.nealrgross.com

1 consider, I recommend that the ACRS consider that all
2 the internal staff comments on the research plan
3 should be considered. All the comments. It's like
4 the public comments. When you go for the
5 communications to the public, you don't say 'I got 50
6 comments from NEI,' all the others I don't care about.
7 All the comments should be -- that would be the
8 courteous thing to do. Review all the comments. You
9 don't have to apply all the comments, but you learn
10 something by the interchange. That's one thing I want
11 the ACRS to think about that.

12 Then also, after review of the public
13 comment, you recommend the disposition of the comments
14 to be presented to the person who brought up the
15 comments and to the ACRS. That's what you do when
16 you've got the public comment. You come to the ACRS,
17 and you discuss it, the public comment, and how do you
18 resolve it. We want nothing else than that. We're
19 not a second-class citizen. We're just like the
20 public, American public, and we want to be treated
21 like that. The only way we can be treated as public
22 is to comment, and give you all those comments again?
23 I think it's wrong, okay? And what I'm saying, we
24 have not requested anything else that you have not
25 readily provided to the public. And one thing I

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 recommended for you is to get involved with the Oconee
2 application to replace the analog system. It's a very
3 interesting application who challenges a lot of our
4 principles and precepts. And brief the analog system,
5 and why do you do things. In the analog existing and
6 the digital system, they cannot be -- that's very
7 important.

8 CHAIRMAN APOSTOLAKIS: So you want us to
9 get involved in that?

10 MR. CALVO: Yes.

11 MEMBER BONACA: I would like very much --
12 I think it should be before the main committee.

13 CHAIRMAN APOSTOLAKIS: Me too. Me too.
14 I was telling Eric here --

15 MR. CALVO: And another thing. We need
16 your help on that one.

17 CHAIRMAN APOSTOLAKIS: Very good.

18 MR. CALVO: Because it's highly
19 philosophical, broader, and we need that because it
20 brings the whole aspect into that.

21 CHAIRMAN APOSTOLAKIS: Wonderful. So we
22 can actually -- I mean, we can have the stuff.

23 MR. CALVO: Yes.

24 CHAIRMAN APOSTOLAKIS: Just tell us when
25 will be an appropriate time to brief us.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. CALVO: So we can get Research to help
2 us in this.

3 CHAIRMAN APOSTOLAKIS: Yes.

4 MR. CALVO: I think we both jointly can
5 come in here and present.

6 CHAIRMAN APOSTOLAKIS: I really get the
7 impression, I mean just to close this. You are really
8 the decision-makers, right? You decide that something
9 is acceptable to this agency or not. And you really
10 want to know, if somebody says I'm going to help you,
11 where he's going to help you, how he's going to help
12 you, which point, you know. And this is a
13 characteristic of decision-makers. I mean, you really
14 don't want to see doing research for its own sake, and
15 all that. So I see what the difference in approaches
16 is.

17 MR. LOESER: I think research for its own
18 sake is very good. But then it has to be presented as
19 such, not as this is the solution to all your problems
20 in five years.

21 CHAIRMAN APOSTOLAKIS: Anyway, no I think
22 we understand, and the Research I'm sure understands.

23 MR. CALVO: I think you hit it right on
24 the target, and that's what we need. It's very
25 difficult for me to get a product from Research, and

1 then go back and look at the industry in the eyes and
2 say 'Hey fellows, I'm going to have to backfill you
3 all this because of this.' I've got to give them the
4 resource. If I don't have the resource, I'm going to
5 be in trouble. Look, I want this very much.

6 MR. MARINOS: One last comment that you
7 made about the regulatory uncertainty, and it was
8 changed to regulatory instability. I think that the
9 premise of the original statement was correct. I
10 believe that this plan will create, and I've had
11 already reaction from industry, it does create a
12 regulatory uncertainty, because it places a cloud over
13 the process we use and we have used to do major
14 reviews. Those platforms that we've used are major
15 things. And they're being implemented now to a plan
16 which is equally challenging, but not as challenging
17 as reviewing the platform. So how do you do this for
18 the entire industry, for the entire world under this
19 process, and yet we have this plan with 500 pages of
20 tools by which they will second-guess the work that we
21 do. That's where this regulatory uncertainty lies and
22 it is, in my view.

23 CHAIRMAN APOSTOLAKIS: Okay.

24 MR. CALVO: Anyway, that completes my
25 talk. Thank you for listening.

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: Thank you very much
2 gentlemen. Any comments from the staff?

3 MR. BARRETT: Yes. This is Richard
4 Barrett, Office of Research. I'd just like to say a
5 few things to clarify. First of all, we have a number
6 of processes for gaining user office commitments to
7 support our research program. And the TAG process is
8 certainly one of them. The process we've used of
9 developing this plan and submitting it for office
10 concurrence is also a legitimate process. We don't
11 always just sit and wait for a user need to come from
12 the user office. This is an area where I think the
13 Office of Research has justifiably taken the
14 initiative to produce something that can be of use to
15 the agency in the future. And I say that having
16 recently come from NRR.

17 Also, I think it's not fair to
18 characterize this as research for research's sake. I
19 think what the Office of Research has done is put on
20 the table a broad-ranging proposal. And we are open
21 to technical comments. We're open to process
22 comments. And we're anxious to work in a TAG
23 environment with our user offices in the future. The
24 Office of Research has a record of dealing openly with
25 its users, and we will continue to act in that way.

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: Okay.

2 MR. GRIMES: My name is Chris Grimes, and
3 I'm the deputy director of the Division of Engineering
4 in NRR. I want to clarify the point that Mr. Calvo
5 described this as a non-concurrence, and that's true.
6 The Office of NRR chose not to adopt all of the
7 comments submitted by EEIB on the user need. While we
8 do have an established protocol for the communication
9 between the two offices, individual branches, even
10 individual sections, tend to exercise the technical
11 advisory groups to a greater or lesser extent. They
12 have more or less effective communication between the
13 two offices.

14 There has been an effort underway between
15 the leadership teams and the two offices now for at
16 least one year, maybe two, to try and have a more
17 consistent treatment about user needs, and the
18 reliance on technical advisory groups to coordinate
19 the goods and services. And as you pointed out
20 before, it's not sufficient to say that they are
21 related to a strategic goal of safety, security,
22 effectiveness, and efficiency or openness. The goods
23 and services have to be related to how they
24 contribute. In what way are they expanding knowledge
25 so that we have a better understanding of safety, or

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

(202) 234-4433

www.nealrgross.com

1 that we have a more efficient review process? I share
2 Mr. Waterman's view that there ought to be a focus on
3 process improvements and contributions. And to that
4 extent, we felt that the majority of comments that
5 were going to be proposed were not constructive, and
6 that they would suggest the research plan should be --
7 the baby will be thrown out with the bathwater. So we
8 only adopted those that we thought were constructive.

9 We do favor -- there is a consistent use
10 of technical advisory groups on a regular basis. We
11 will not wait from 2003 till 2005 to do the next
12 comment or round of communications on the progress on
13 the user needs, or any of the research plans. Our
14 mutual offices will expect that a monitoring will be
15 done at least on a quarterly basis, if not a monthly
16 basis, to ensure effective communication.

17 MR. CALVO: If I may, a rebuttal, just a
18 little bit. A rebuttal a little bit. Those comments
19 that were selected to be given to Research that were
20 NRR, they were never discussed with us. We don't know
21 --

22 CHAIRMAN APOSTOLAKIS: Yes, this is
23 internal to the office.

24 MR. CALVO: I know the communication
25 problem is both vertical and horizontal. So we're

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

(202) 234-4433

www.nealrgross.com

1 having that problem, not only between offices. It's
2 within the office.

3 CHAIRMAN APOSTOLAKIS: Okay. Any other
4 comments from the staff or members of the public on
5 what we've heard? Well, thank you all. Thank you
6 very much. And we'll recess until 10:40.

7 (Whereupon, the foregoing matter went off
8 the record at 10:23 a.m. and went back on the record
9 at 10:41 a.m.).

10 CHAIRMAN APOSTOLAKIS: Okay, we'll
11 continue now with the revision of the regulatory
12 guide, right?

13 MR. KEMPER: Yes, yes. If I could just --

14 CHAIRMAN APOSTOLAKIS: And Mr. Kemper,
15 before George takes over. Go ahead.

16 MR. KEMPER: Thank you. I'd just like to
17 make a few comments here. We're really here, George,
18 at your invitation. This is a work in progress, and
19 we're almost done with this reg guide, draft reg
20 guide. But it hasn't quite gelled yet. So what we
21 would like to do is to review this with the working
22 group and get your comments. At this meeting, that's
23 fine, or later on if you choose to write something and
24 send it to us informally that'd be good too.

25 But basically the new reg guide endorses

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

(202) 234-4433

www.nealrgross.com

1 a process which is a revision of the IEEE 497-2002
2 that's a new approach to identifying post-accident
3 monitoring instrumentation. It uses a performance-
4 based versus deterministic point of view. As you all
5 know I'm sure, the current revision of Reg Guide 1.97
6 is very prescriptive. It's got the tables in the back
7 of it that we put together many years ago, which
8 George will go into details on some of that briefly.
9 Post-TMI, and it's been a well established document
10 that's been used for years. So, but with the advent
11 of advanced reactors coming onboard, you know
12 basically this document, Rev. 3 is designed for light
13 water reactors. These new advanced reactor designs
14 are other than light water reactors, in some cases.
15 So we need -- so the industry felt as though a little
16 broader guidance was needed.

17 And so we have attempted to endorse that
18 with this standard. We considered several options and
19 approaches to it because there's some things that are
20 a little unusual about it which George will talk about
21 in detail. What we'd like to do is just to capitalize
22 on this opportunity to share this with you and get
23 your reaction to it. Just it would make us feel I
24 guess a little more comfortable. The next process is
25 to send it out for industry comments. So NRR has

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 reviewed it and commented on it. OGC has also
2 reviewed it and commented on it, but as I say, we
3 haven't sent it out yet, so it's not quite gelled yet.

4 CHAIRMAN APOSTOLAKIS: You mean for public
5 comments?

6 MR. KEMPER: For public comments, yes.
7 Okay?

8 CHAIRMAN APOSTOLAKIS: Yes, great.

9 MR. KEMPER: So with that, George? Go
10 ahead and get started.

11 MR. TARTAL: My name is George Tartal. I
12 work for the Instrumentation and Control Section of
13 the Office of Research. I've been with NRC for about
14 a year, and before coming to NRC I had 13 years of
15 experience in design engineering in the private
16 sector.

17 CHAIRMAN APOSTOLAKIS: And you still want
18 to stay with the NRC after a year?

19 (Laughter)

20 MR. TARTAL: I'm sorry.

21 CHAIRMAN APOSTOLAKIS: That's okay. It
22 was a good decision joining the agency after? We are
23 allowed to joke. Makes long sessions easier to take.

24 MR. TARTAL: Can you hear me better now?
25 So as Bill mentioned, the reason we're presenting this

1 guide is because we're seeking the committee's verbal
2 interaction on the approach taken in the content of
3 the draft guide. First we'll provide a brief
4 background on the history of accident monitoring, then
5 discuss the current revision, Rev. 3 of Reg Guide
6 1.97. Then we'll provide a brief overview of IEEE
7 Standard 497-2002, which is a revised standard for the
8 selection, performance, design, qualification,
9 display, and quality assurance criteria for accident
10 monitoring. Then we'll describe the draft guide
11 presented for discussion today, Draft Guide DG-1128,
12 focusing on the regulatory positions and the issues
13 the staff addressed in trying to endorse the standard
14 in the guide. I'll describe the approaches the staff
15 considered for the draft guide, followed by a
16 conclusion and a request for any additional comments
17 or questions on the approach and content of the guide.

18 10 C.F.R. 50, Appendix A, Criteria 13, 19,
19 and 64 require instrumentation be provided to monitor
20 variables in systems under accident conditions. Reg
21 Guide 1.97 was issued as the effective guide in August
22 of 1977, and provided general design and qualification
23 criteria for accident-monitoring instrumentation. The
24 accident TMI II happened in 1979. Lessons learned
25 from TMI II and post-TMI action plan, NUREG-0737,

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 later codified in 10 C.F.R. 50.34(f) resulted in
2 Revision 2 to the Reg Guide 1.97 in December of 1980.
3 Revision 2 was to be implemented via NUREG 0737. A
4 later revision, Revision 3 then reorganized the design
5 and qualification criteria into tabular format, and
6 revised some radiation-monitoring variables. It was
7 issued 22 years ago in May of 1983 and is still the
8 current source of accident-monitoring criteria for
9 nuclear power plants.

10 Rev. 3 endorses ANS Standard 4.5-1980,
11 which has since been withdrawn as now an inactive
12 standard. And I'd like to briefly review the variable
13 types and categories in the current guide since we're
14 going to talk about them in a later slide.

15 CHAIRMAN APOSTOLAKIS: So the last
16 revision was in 1983?

17 MR. TARTAL: Yes, that's the current
18 revision.

19 CHAIRMAN APOSTOLAKIS: That's an
20 interesting situation, that we're endorsing a standard
21 that is now inactive. What does that say?

22 MR. TARTAL: That was -- that's the
23 current guide right now. We're not talking about the
24 draft guide. The current guidance is Rev. 3. The
25 draft guide is going to become Rev. 4.

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

1 CHAIRMAN APOSTOLAKIS: Yes. I understand
2 that.

3 MR. TARTAL: So that the current guidance
4 is 22 years old.

5 CHAIRMAN APOSTOLAKIS: No, but I'm saying
6 in 1980 I guess, no in 1983 we endorsed an ANSI
7 standard that has been withdrawn.

8 MR. KEMPER: That's correct.

9 MR. TARTAL: It's since been withdrawn,
10 yes.

11 CHAIRMAN APOSTOLAKIS: Why? Was it wrong,
12 or why was it withdrawn?

13 MR. TARTAL: It was withdrawn because Rev.
14 3 of the reg guide became the sole source for
15 accident-monitoring criteria. It really wasn't
16 needed. Rev. 3 was so prescriptive.

17 CHAIRMAN APOSTOLAKIS: Oh.

18 MR. KEMPER: It became the de facto
19 industry standard.

20 CHAIRMAN APOSTOLAKIS: Okay.

21 MR. TARTAL: Accident-monitoring variables
22 prescribed in Tables 2 and 3 of the guide are
23 organized by variable type. Type A are for planned
24 manual actions with no automatic control. They're
25 plant-specific and an example would be reactor coolant

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 level for monitoring core cooling. Type B are for
2 assessing plant critical safety functions. An example
3 is RCS pressure for monitoring RCS integrity. Type C
4 for indicating potential or actual breach of fission
5 product barriers. An example is primary coolant
6 radioactivity for monitoring fuel cladding integrity.
7 Type D for indicating safety system performance and
8 status. An example is high pressure injection flow.
9 Type E are for monitoring radiation levels, releases,
10 and environs, with an example being plant vent
11 radiation for monitoring airborne releases.

12 The design qualification criteria
13 applicable to each variable are determined by an
14 assigned category. Category 1 is for indicating the
15 accomplishment of a safety function, and analogous to
16 safety-related instruments. Category 2 is for
17 indicating safety system status, and analogous to
18 augmented quality-related instruments. Category 3 for
19 backup and diagnostic variables, and analogous to non-
20 safety related instruments. So with this prescriptive
21 list of variables to monitor, and comprehensive set of
22 design and qualification criteria to be met, Rev. 3
23 has become the de facto standard for accident-
24 monitoring criteria in the industry.

25 With digital instrumentation being more

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

(202) 234-4433

www.nealrgross.com

1 frequently employed in nuclear power applications, and
2 with the new and advanced plant designs being
3 considered for future licensing, a more flexible
4 approach to accident-monitoring was desired by the
5 industry. IEEE Standard 497-2002 was created to
6 consolidate the criteria from inactive Standards ANS
7 4.5 and IEEE Standard 497-1981, as well as from Reg
8 Guide 1.97 Rev. 3, and to update the criteria to the
9 current state of technology. It provides a
10 technology-neutral approach intended for advanced
11 design plants. It takes a performance-based non-
12 prescriptive approach to the selection of accident-
13 monitoring variables. The prescriptive tables of BWR
14 and PWR variables have been now replaced by variable
15 selection based on design basis accident mitigation
16 functions. This is the most significant change from
17 Rev. 3. The selected variable type then determines
18 the applicable performance, design, qualification,
19 display, and quality assurance criteria. The standard
20 reference is other recent industry standards in the
21 criteria, and also provides criteria for the use of
22 digital instrumentation. And the next slide provides
23 a brief overview of this criteria.

24 The definitions for variable types A
25 through E are similar to the definitions in Rev. 3 of

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

(202) 234-4433

www.nealrgross.com

1 the guide. Some typical source documents are also
2 referenced for each variable type, like EOPs, EPGs,
3 AOPs, etcetera. Performance criteria in the standard
4 include range, accuracy, response time, duration, and
5 reliability. Design criteria include single and
6 common cause failure, independence, separation,
7 isolation, power supply, calibration, and portable
8 instrumentation. Qualification criteria include
9 environmental and seismic qualification for fixed and
10 portable instruments. Display criteria include
11 display characteristics, identification, display
12 types, and recording. Finally, quality assurance
13 criteria are given. The significant differences here
14 in the criteria from that of Rev. 3 are new criteria
15 for selection, additional criteria for single- and
16 common-cause failure, guidance for use of portable
17 instruments, and examples of monitoring channel
18 displays.

19 This Draft Guide DG-1128 is the proposed
20 Rev. 4 of Reg Guide 1.97. It was prepared as a
21 response to a user need request from NRR. RES and NRR
22 have worked together to come up with an approach that
23 can be effectively implemented and regulated for new
24 and current plants. The draft guide endorses IEEE
25 Standard 497-2002 with exceptions and clarifications.

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

(202) 234-4433

www.nealrgross.com

1 It's intended for new nuclear power plants with
2 conversion to this new method by current operating
3 plants on a comprehensive and strictly voluntary
4 basis. And we'll talk about that in a minute. Next
5 we'll discuss the five regulatory positions against
6 the IEEE standard.

7 The first regulatory position addresses
8 the question 'How might current operating plants using
9 Rev. 2 or 3 of the Reg Guide 1.97, how might they
10 apply the criteria in IEEE 497?' The standard states
11 it's intended for new plants, but, quote, "The
12 guidance provided in this standard may prove useful
13 for operating nuclear power stations desiring to
14 perform design modifications or design basis
15 modifications." The staff thinks that current plants
16 may be interested to see if and how they can use the
17 new guidance. The problem is the standard doesn't
18 tell you how the current plants might use it. It
19 tells them they can use some of the guidance. But
20 what if current plants wanted to use all the guidance
21 and convert to the new method? By "convert" what we
22 mean here is moving from the current licensing
23 commitments in Rev. 2 or 3 of Reg Guide 1.97 and
24 revising their accident-monitoring program to the
25 criteria contained in Rev. 4. The standard, since

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 it's intended for new plants, does not provide any
2 guidance in translating from variable types and
3 categories as they have in Rev. 3 to only requiring
4 variable types in the IEEE standard. Since the
5 categories do not directly correlate to variable
6 types, the staff compared the variable types in
7 associated categories, and concluded that generally
8 Types A, B, and C are Category 1, Type D is Category
9 2, and Type E is Category 3. But there are some
10 exceptions to this translation. The example shown
11 here is PWR Subcooling Margin Monitor. It's a Type B
12 Category 2 variable. If they were to convert this
13 variable, would it become a Type B, or a Type D, or
14 something else? The variable selection process would
15 have to make this determination on a case-by-case
16 basis. Furthermore, even if the variable type doesn't
17 change, the individual criteria for that particular
18 variable type may be different, and the converted
19 variable would need to meet all the applicable
20 criteria in the standard for that variable type. For
21 current plants to convert some of the individual
22 variables may require physical modifications as well
23 as licensing basis changes. The new criteria may be
24 more or less stringent than the current criteria,
25 depending on the new selected variable type and the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 existing variable's assigned category. As a result,
2 we cannot intend this guide for current plants, but
3 current plants may convert on a voluntary basis. The
4 staff also feels that partial conversions of one
5 variable or system could result in the potential for
6 some variable or system interactions to be left un-
7 analyzed and un-monitored, and hence conversion should
8 be comprehensive of the entire accident-monitoring
9 program. As a result, the draft guide states it's
10 intended for new plants, and conversion for current
11 plants may be done on a comprehensive and strictly
12 voluntary basis by the licensee.

13 MEMBER BONACA: Yes. I mean, as I review
14 this part, I still get confused about how you go from
15 one to the other.

16 MR. TARTAL: It is confusing. It's not
17 straightforward.

18 MR. KEMPER: Yes. And to add more to the
19 confusion, you know, this is a new process. It really
20 hasn't been worked out yet, right? So there's no
21 plants out there with Rev. 4?

22 MEMBER BONACA: The most confusing thing
23 was, I mean, so many of the changes in 1983 were tied
24 to the issues that came out of TMI.

25 MR. TARTAL: Yes.

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

(202) 234-4433

www.nealrgross.com

1 MEMBER BONACA: And you know, I was trying
2 to trace back on how you would deal still with those
3 issues in an explicit fashion based on this new
4 guidance, and our regulatory position, you can trace
5 it easily. This doesn't seem to be specific
6 requirement pointing into that direction, while the
7 old reg guide clearly had pointers there. You could
8 see why they did certain things because of the
9 experience of TMI. So it's a little confusing. Do
10 you expect that the people with current plants would
11 go this new approach?

12 MR. KEMPER: Yes. I've received a couple
13 of calls so far from the BWR owners group
14 representatives. And from indications I've gotten
15 through those calls that they're waiting for this to
16 be issued so they can evaluate, I guess, what they
17 want to do, if anything, to the current generation
18 plants.

19 The other point here too is by having a
20 situation where plants are straddled, if you will,
21 part of their post monitoring PAMI instrumentation is
22 in Rev. 3, complies with Rev. 3, and part of it goes
23 to Rev. 4. It'd be very difficult I guess from an
24 inspector's standpoint to go out and actually audit,
25 you know, what the licensing criteria is. And

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

(202) 234-4433

www.nealrgross.com

1 secondly, NRR would really have quite a burden placed
2 on them for these submittals as they come in, you
3 know, one by one, or two instruments here, one
4 instrument there, trying to comply with this new
5 standard and leave the rest of them where they are.
6 So that --

7 MEMBER BONACA: That's another issue that
8 I was thinking of, you know. Again, this piecemeal
9 application, if it happens, takes existing plants away
10 from some level of standardization that we have been
11 able to implement in these plants to whatever degree
12 we could. And that standardization I believe is
13 responsible for improvements in safety performance,
14 just because there is a lot of news of lessons learned
15 from sister plants. And this could be radically
16 different. I mean, you could see departures that
17 would take somebody pretty much away from the
18 experience. Anyway, it's just an observation.

19 MR. TARTAL: So the second regulatory
20 position the staff addressed was the IEEE Standard's
21 requirement for maintaining channel calibration during
22 an accident. The standard requires maintaining
23 instrument calibration by means of re-calibration,
24 proper calibration interval specification, selecting
25 equipment that does not require calibration, or by

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

(202) 234-4433

www.nealgross.com

1 cross-calibration with other channels having known
2 relationship to that variable. The staff believes
3 that although conceptually a good idea, plants should
4 not be required to maintain calibration during the
5 accident. Instead, the draft guide states that the
6 plants should design accident-monitoring channels to
7 the extent possible with the ability to maintain
8 calibration during an accident.

9 The third regulatory position addresses
10 IEEE Standard's future work section on severe
11 accidents, and how it relates to selection criteria.
12 The standard does, however, include the requirement
13 for Type C variables to have extended ranges, which
14 was a post-TMI action item now in 10 C.F.R. 50.34(f).
15 The agency's severe accident policy does not require
16 mitigation of severe accidents, and hence there are no
17 requirements to monitor severe accidents. However,
18 the draft guide incorporates the language from NUREG-
19 0660, which is the post-TMI action plan, into the
20 criteria to clarify the requirement for extended
21 ranges for Type C variables, but does not further
22 address severe accidents.

23 The fourth regulatory position addresses
24 the IEEE Standard's exclusion of contingency actions
25 from the variable selection process. Contingency

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

(202) 234-4433

www.nealrgross.com

1 actions are most commonly associated with those
2 additional actions and EOPs used when primary success
3 paths have not been successful. The IEEE standard
4 assumes that all contingency actions are to mitigate
5 action conditions that are beyond the licensing basis
6 of the plant. But the staff doesn't want to
7 unnecessarily exclude contingency actions from the
8 potential list of variables to monitor if some of
9 those actions could be a potential accident-monitoring
10 variable in accordance with the given criteria.
11 Therefore, the staff feels that this restriction
12 toward contingency actions should not be endorsed.
13 Instead, the licensee should consider all EOP actions
14 for design basis events during the variable selection
15 process, allow the selection criteria to determine if
16 the variables used for the contingency action can be
17 excluded.

18 The fifth regulatory position is a
19 carryover from Rev. 3 of Reg Guide 1.97, and addresses
20 the number of points of measurement for a variable.
21 The IEEE standard does not address a number of points
22 of measurement for a variable like Rev. 3 did. The
23 regulatory position states that the number of points
24 of measurement for each variable should be sufficient
25 to adequately indicate the variable value. In other

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

(202) 234-4433

www.nealrgross.com

1 words, for example, if you were to measure containment
2 temperature due to the size of containment space, you
3 wouldn't want to use a single point measurement and
4 say that's representative of everywhere inside
5 containment. You'd want several measurements at
6 various locations.

7 Next I'll briefly describe the four
8 approaches the staff considered to solving this need
9 for a more flexible source of accident-monitoring
10 criteria. One approach was to take no action. Reg
11 Guide 1.97 would remain at Rev. 3 for current and new
12 plants, and IEEE 497 would not be endorsed. That
13 solution may be adequate for the fleet of current
14 operating plants, but the prescriptive variable list
15 and outdated criteria of Rev. 3 wouldn't be of much
16 use for a licensee of an advanced design plant. So
17 the staff did not choose this approach.

18 The second approach the staff considered
19 was to revise Reg Guide 1.97 to incorporate all
20 previously approved deviations which were generic to
21 that particular design, as well as other
22 clarifications and role changes as a means of updating
23 the guide for current plants, and at the same time
24 endorse IEEE 497 for both current and new plants.
25 First, all the changes that I mentioned a second ago

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

(202) 234-4433

www.nealrgross.com

1 have already been approved, so it would be unnecessary
2 to go through the process of re-approving them in this
3 guide. Second, providing separate guidance for
4 current and new plants within the same reg guide could
5 result in a confusing and ambiguous guide. Therefore,
6 the staff did not choose this approach.

7 The third approach the staff considered
8 was to have two reg guides addressing accident-
9 monitoring. A new reg guide, 1.xxx endorsing IEEE 497
10 would provide accident-monitoring criteria for new
11 plants, and Reg Guide 1.97 Rev. 3 would remain the reg
12 guide for accident-monitoring for current plants. The
13 first problem is the nuclear industry knows Reg Guide
14 1.97 is the sole source for accident-monitoring
15 criteria. The staff feels that issuing a second reg
16 guide also providing accident-monitoring criteria
17 would be confusing to licensees and regulators.
18 Second and more importantly, there are a number of
19 regulatory documents which refer to Reg Guide 1.97 for
20 accident-monitoring criteria, like 10 C.F.R. 50.49 and
21 Reg Guide 1.89. And the staff would need to revise
22 all the regulatory documents that refer to the Reg
23 Guide 1.97 to also refer to this new Reg Guide 1.xxx.
24 So the staff didn't choose that approach either.

25 The fourth approach the staff considered

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

(202) 234-4433

www.nealrgross.com

1 was to revise Reg Guide 1.97 to endorse IEEE 497 for
2 new plants as the standard says it's intended.
3 Current plants would continue to use the guidance in
4 Rev. 2 or Rev. 3 of Reg Guide 1.97, or voluntarily and
5 comprehensively convert to the criteria in Rev. 4.
6 The benefits of this solution are that it endorses the
7 updated consensus standard for new plants, which
8 Approach 1 didn't do; it would create clear and
9 unambiguous guidance for new and current plants, which
10 Approach 2 didn't do; and retain the industry-familiar
11 name of Reg Guide 1.97 for new and current plants,
12 which Approach 3 didn't do. As a result, this is the
13 approach that the staff chose. Furthermore, NRR and
14 OGC have reviewed the draft guide, and have no
15 technical or legal objections to the content approach
16 in the draft guide.

17 In conclusion, Draft Guide DG-1128, the
18 proposed Revision 4 to Reg Guide 1.97 endorses the
19 current industry standard IEEE Standard 497-2002 with
20 exceptions and clarifications. It's consistent with
21 and provides a method for meeting the NRC's
22 requirements. Standard Review Plan Chapter 7 will
23 require updating for the new revision of the guide.
24 The revision is intended for new nuclear power plants,
25 and any current plant wishing to convert to the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 criteria contained within may do so on a comprehensive
2 and voluntary basis. There are no backfit issues
3 associated with this revision. And finally, we ask
4 the subcommittee if there are any additional comments
5 or questions that you have before we proceed with
6 issuing the draft guide for public comment.

7 MEMBER WHITE: Excuse me, could you
8 clarify what you mean by "no backfit issues"?

9 MR. TARTAL: Since the draft guide is
10 intended for new plants, it doesn't affect the current
11 plants. Backfit issues are associated with current
12 operating plants.

13 MR. KEMPER: We've tried to emphasize
14 voluntary use for current generation plants as the
15 only way that we would -- the way we are endorsing the
16 standard. To be very clear about that.

17 CHAIRMAN APOSTOLAKIS: Any comments? No?

18 MEMBER BONACA: I just have a question.
19 I mean, you know, I can see how the licensee could
20 take this new approach, okay, through some way that
21 wasn't clear to me how it was easy it's going to be.
22 He would then choose certain issues of the protection
23 system or ESF and so on and so forth features. Do you
24 envision that there was a transition of that type by
25 many at some point the NRC would feel compelled to go

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

(202) 234-4433

www.nealrgross.com

1 back to a more prescriptive approach for individual
2 types to plant? I'm talking about the type of plant,
3 like you know for example for PWRs, they finally
4 decided that everyone had to have this specific
5 measurement. Everybody had to have the same.

6 MR. TARTAL: Those tables were initially
7 put into the reg guide because the industry didn't
8 understand how to implement the previous revision of
9 the reg guide.

10 MEMBER BONACA: Okay.

11 MR. TARTAL: It gave general design and
12 qualification criteria, and at that point accident-
13 monitoring was still in its infancy. People didn't
14 understand how to use the general criteria. So to
15 make it more clear, the NRC came out with Rev. 2 which
16 had the prescriptive list of variables.

17 MR. KEMPER: And I think that history has
18 shown -- Barry you can speak up here if you'd like --
19 that as time has gone on, there's been many exceptions
20 requested and granted to the prescriptive list in Reg
21 Guide 1.97.

22 MR. TARTAL: Deviations.

23 MR. KEMPER: Yes, deviations by various
24 NSS-type or plant-specific issues and so forth. So
25 this new performance-based criteria hopefully will

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 eliminate that. Each plant will do their own analysis
2 unique unto itself, and then of course NRR will have
3 the task of reviewing and approving that.

4 MEMBER BONACA: And I agree that the
5 understanding of plant behavior has changed
6 significantly, so that will be acceptable. Thank you.

7 MR. TARTAL: Okay. Other questions?

8 CHAIRMAN APOSTOLAKIS: Okay. Thank you
9 very much.

10 MR. KEMPER: Thank you.

11 CHAIRMAN APOSTOLAKIS: Sam, maybe you can
12 help us here. Can we start the next -- the afternoon
13 session a little earlier?

14 MR. DURAISWAMY: No.

15 (Laughter)

16 MEMBER WHITE: Does that mean you need
17 more dialogue?

18 CHAIRMAN APOSTOLAKIS: Okay. We'll recess
19 then until 12:30.

20 (Whereupon, the foregoing matter went off
21 the record at 11:08 a.m. and went back on the record
22 at 12:30 p.m.).

23 CHAIRMAN APOSTOLAKIS: We're back in
24 session. The next item on the agenda is a short
25 presentation by Mr. Kemper on software quality

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 assurance. Correct?

2 MR. KEMPER: That's correct.

3 CHAIRMAN APOSTOLAKIS: Okay.

4 MR. KEMPER: Thank you. Well again, I'm
5 Bill Kemper, the section chief for the Instrumentation
6 and Control Engineering Section of Research. And
7 since we've got some new members here, I'll just give
8 you a quick background of myself. I've been with the
9 agency for just a couple of years. I'm a relative
10 newcomer. I spent 29 years in the nuclear industry
11 before that, worked at three different utilities, and
12 three different power plants, and spent a lot of time,
13 done a lot of things in my career, but a lot of it was
14 in operations and instrumentation and control
15 engineering. So it's a pleasure for me to be here
16 working with this agency on the regulatory side of the
17 business.

18 So at any rate, I only have 15 minutes to
19 speak, so I will try to get through this on time. I
20 just wanted to provide a brief discussion, kind of an
21 overview of what we're trying to accomplish here in
22 this area of software quality assurance. The diagram
23 you see before you is out of the research plan. This
24 covers the activities that are currently scoped out
25 for Section 3.2 of the research plan. Right now we

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 have three initiatives that we're focusing on in this
2 area. You'll receive detailed presentations following
3 mine on each one of these areas. So at any rate,
4 there's more time for more questions as they come up
5 in each one of these areas.

6 And listening to the presentations this
7 morning, actually I kind of -- I'd like to build on
8 some of the statements that were made earlier about
9 the research programs. What we tried to do is put
10 this presentation together such that we can explain
11 what the agency is doing now, what the areas for
12 improvements might be, and then what we intend to do
13 about it, it boils down to, okay? So.

14 CHAIRMAN APOSTOLAKIS: This will be a good
15 template for all the presentations.

16 MR. KEMPER: So to provide some -- I'm
17 sorry.

18 CHAIRMAN APOSTOLAKIS: Oh go ahead.

19 MR. KEMPER: Yes, to provide some
20 background on the current process for evaluating
21 software quality of licensee applications, the NRC SRP
22 Chapter 7, Standard Review Plan, Revision 4 which was
23 issued in June of 1997 provides the regulatory
24 framework for the review and approval of digital
25 safety systems. As part of its review of digital

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 safety systems, NRC evaluates safety-related software
2 quality by reviewing the developmental process, for
3 example verification and validation testing,
4 configuration management programs, and software
5 development products, such as software requirement
6 specs, software design documentation, test plans,
7 requirement traceability matrices, those sort of
8 things. In other words, the agency reviews the
9 software developmental processes and products produced
10 by the vendors and the licensees themselves. Now, I
11 think we're all in agreement, the SRP is adequate to
12 provide guidance, in other words, what to review, to
13 the staff in performing safety reviews that pertain to
14 digital safety systems.

15 The review and approval of digital systems
16 currently depends on qualitative evaluations of
17 digital system features and development processes.
18 Software quality assurance evaluations are performed
19 manually, without the aid of assessment tools or other
20 means of obtaining quantitative measures of software
21 quality. And also, the SRP Chapter 7 Branch Technical
22 Position 14 identifies digital system development
23 attributes that should be reviewed, but does not
24 really provide detailed guidance on the process for
25 confirming that the software conforms to the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 acceptance criteria.

2 CHAIRMAN APOSTOLAKIS: So this slide then
3 is what we're doing now, and what we need to do.

4 MR. KEMPER: This is the delta, if you
5 will.

6 CHAIRMAN APOSTOLAKIS: Good.

7 MR. KEMPER: This is, as we see it, the
8 area for improvements that we're trying to set the
9 foundation for that. So as I've stated, the SRP is a
10 very thorough document, very thorough compilation of
11 what requirements must be satisfied. What we're
12 attempting to conduct research on is to provide the
13 reviewer with information about how the criteria
14 should be satisfied, and also how much is good enough,
15 quite honestly. As Mike Waterman said earlier in his
16 presentation, a lot of the reviews is a function of
17 what the reviewer has within himself or herself in
18 terms of meeting these criteria.

19 CHAIRMAN APOSTOLAKIS: Now, when you say
20 in the second bullet software quality assurance
21 evaluations are performed manually, you envision in
22 the future the reviewer to have computer help?

23 MR. KEMPER: That's true. I'm going to
24 get into that very shortly here. In the next slide or
25 two. So NRC reviews the results of software

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 development processes and safety assessments, but the
2 reviews do not include a means for independent
3 assessments of software quality assurance. Now, by
4 "independent" I mean what we're trying to provide is
5 a method for reviewing software that does not just
6 rely on licensee- or vendor-produced products. We
7 hope to provide tools that will provide another
8 dimension to the agency's capabilities to review
9 software. For example, when the licensee submits a
10 new fuel design for review, the agency not only
11 reviews the code and documentation that the licensee
12 used for the new fuel design, but the NRC has its own
13 codes that it can run independently to verify what the
14 licensee has concluded. And you can make the same
15 statement in the PRA business. The agency has its own
16 PRAs to use to validate licensee activities pertaining
17 to risk. We don't have tools like that in the I&C
18 business, so that's what we're proposing to do is try
19 to create some of those tools for independent
20 assessments.

21 So given the complexity and sophistication
22 of current digital safety systems, the goal of this
23 research program is to provide independent assessment
24 methods and objective acceptance criteria that can
25 supplement and augment the existing guidance in

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 Chapter 7 of the SRP. These words, you've heard these
2 several times. We're going to continue to make this
3 statement as we go through our projects.

4 So this information can be provided as
5 formal review procedures for verifying consistency
6 with the SRP guidelines, which could also improve
7 effectiveness and consistency of software quality
8 assurance evaluations and reviews.

9 MR. ARNDT: Let me jump in here for a
10 second. The point here is that if we have these extra
11 tools, or additional methodologies, or additional
12 information, we don't have to use them in every case.
13 But where we want additional information, or where it
14 would be useful, or there's a particular issue, the
15 idea is to have these available so that we can do
16 additional work if we feel that's justified.

17 MR. KEMPER: Okay. Also, the current
18 state-of-the-art in software system safety assessment
19 includes a number of methods and tools for
20 quantitatively assessing the quality of software. For
21 example, there are software system analysis techniques
22 such as Petri-net analysis, Markov analysis, dynamic
23 flow modeling, being used in software modeling
24 techniques right now. Tools such as software metrics,
25 formal verification methods, and testing techniques,

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 such as data flow testing, fault injection, and
2 mutation testing, are being used for software design
3 analysis techniques to ensure that the software system
4 works in a particular way.

5 So what we're trying to accomplish is to
6 review what software quality assurance methods and
7 tools are out there being used in other sectors of the
8 process control industry. And we will then, if
9 possible, adapt these tools for deployment on software
10 systems within the nuclear industry.

11 CHAIRMAN APOSTOLAKIS: I wouldn't use the
12 word "quantitatively" on your first line. There are
13 a number of -- like, I don't think formal verification
14 methods are quantitative. I mean, they're logic.

15 MR. ARNDT: They're logic systems to
16 verify that --

17 CHAIRMAN APOSTOLAKIS: Quantitative means
18 you produce numbers. So I mean, you can still make
19 your point by deleting the word "quantitative".

20 MR. ARNDT: We can do that.

21 MR. KEMPER: I guess the point here though
22 is it's a process. It's a consistent process.

23 CHAIRMAN APOSTOLAKIS: I understand.

24 MR. KEMPER: It's an algorithm, right? In
25 other words, it's a methodology that's --

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: These are methods
2 that --

3 MR. KEMPER: -- that's not the function of
4 the individual, the human being.

5 CHAIRMAN APOSTOLAKIS: Structured methods.

6 MR. KEMPER: Structured, exactly, very
7 good.

8 MEMBER GUARRO: Structural, formal.

9 MR. KEMPER: Exactly.

10 CHAIRMAN APOSTOLAKIS: All of them are
11 formal. Right? Even the third bullet there. Because
12 you insert the word "formal". Software metrics, I
13 don't know what you mean by that.

14 MR. KEMPER: We're going to explain that
15 to you in just a minute.

16 CHAIRMAN APOSTOLAKIS: Good.

17 MR. KEMPER: Okay. So therefore, research
18 in this area will focus on assessing possible analysis
19 methods that are currently used in design and analysis
20 of safety-critical software systems to use in the
21 regulatory process. We intend to focus on methods
22 that have likely short-term application without the
23 need to do extensive development and apply these to
24 nuclear industry applications. For example, fault
25 injection testing has been used by a number of

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 industries, including some nuclear platform suppliers.
2 Formal methods have been used in several industries to
3 support safety-critical applications. Software
4 metrics are currently being used for software quality
5 control and continuous improvement activities in
6 organizations that have programs that are capability
7 maturity model level 4 and 5 respectively. In fact,
8 all military vendors right now are required to have a
9 CMM level 3 program in order to even bid on a
10 contract. So we're just trying to build on these
11 tools and technologies that are out there. And also,
12 any nuclear supplier and vendor should be at least a
13 CMM 3 level because they have a well-defined program
14 per 10 C.F.R. 50 Appendix B, and so they should be
15 ready and capable to implement metrics.

16 And in summary, this research area
17 currently focuses on three initiatives to develop
18 independent methods of assessing software quality
19 and/or reliability: the use of software metrics to
20 evaluate quality, the use of fault injection
21 techniques to evaluate digital system dependability,
22 and to provide technical guidance and review
23 procedures for evaluating self-testing features in
24 digital systems. Now, self-testing features is not
25 really an independent testing method in and of itself.

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 This is really a review criteria issue. So what we
2 want to do is investigate the self-testing methods and
3 technologies that are being used right now in the
4 industry, and try to get a better idea of what are the
5 best testing schemes that we're aware of, and how much
6 reliability is gained from the various self-testing
7 schemes, considering the failure probability presented
8 to the software system due to the added complexity
9 associated with the self-testing software itself. In
10 other words, how much benefit is gained for the extra
11 complexity. Right now we don't have any information
12 to build on in that arena.

13 CHAIRMAN APOSTOLAKIS: So why did you
14 decide not to pursue formal verification methods?
15 That's the only one you're leaving out isn't it?

16 MR. ARNDT: Well, we're choosing to look
17 at particular aspects of particular projects. We
18 looked at formal methods through our cooperative
19 agreement with Halden because that's part of their
20 research program. The results to date didn't appear
21 to be as promising as other methodologies. We
22 continue to keep track of formal methods through our
23 cooperative agreement through Halden. To my
24 knowledge, I'm more than happy to be informed, there
25 was a lot of work in this area in the '80s and '90s,

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

(202) 234-4433

www.nealgross.com

1 some successes, then it kind of fell out of favor for
2 awhile. It's starting to become more popular now that
3 some of the tools are much more sophisticated. So as
4 with anything else in the research program plan, as we
5 have the resources, we're going to look at whether or
6 not any particular methodologies may be useful. If
7 they do appear to be useful, then it will get rolled
8 into the next upgrade a year from now, or two years
9 from now, whenever.

10 CHAIRMAN APOSTOLAKIS: Is the work that
11 you're doing with Halden mentioned in the plan? I
12 can't remember.

13 MR. KEMPER: Yes, I think it is mentioned
14 in the plan.

15 MR. ARNDT: It's part of, I think, the
16 cooperative international agreements, which is in
17 Section 3? Probably 3.7.

18 MR. KEMPER: Although there's no specific
19 projects that are the outcome of that directly in and
20 of themselves. We use that right now as supporting
21 information for background and to integrate into other
22 existing projects. But I think Steve's making a good
23 point here. The idea of this research plan is it's a
24 flexible document. So if we have good reason to
25 believe that formal methods is an area that we should

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 pursue, then we will certainly do that.

2 CHAIRMAN APOSTOLAKIS: Well, I mean it
3 depends on what you call formal methods. Because of
4 course, most people would think of the logic --

5 MR. ARNDT: Proof calculuses and things
6 like that.

7 CHAIRMAN APOSTOLAKIS: Find errors and so
8 on. Or confirm that things are self-consistent. But
9 I recall that the Canadians adapted these methods.
10 They didn't quite use formal methods to prove
11 correctness, but they borrowed heavily, you know,
12 developing tables and all that.

13 MR. ARNDT: Yes. They use it as a design
14 criteria, basically.

15 CHAIRMAN APOSTOLAKIS: Yes. I mean, are
16 you familiar with what they have done?

17 MR. ARNDT: Yes.

18 CHAIRMAN APOSTOLAKIS: Is there anything
19 useful there?

20 MR. ARNDT: I've read some of the work.
21 Also, the Brits did some work in that area on Sizewell
22 as more of a design methodology as opposed to a formal
23 correctness proof.

24 CHAIRMAN APOSTOLAKIS: Okay. All right.
25 You done?

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. KEMPER: Okay. Almost. So at any
2 rate, to conclude, these research projects will
3 provide objective acceptance criteria and review
4 procedures that augment and supplement existing SRP
5 guidance for approving or denying digital safety
6 system license applications. And that's the hardest
7 part. When we deny something, we need to have a solid
8 foundation to build on. So that really concludes my
9 short overview of this area. If there's --

10 CHAIRMAN APOSTOLAKIS: So what is the
11 distinction between quality assurance and the risk
12 part of it?

13 MR. ARNDT: The big issue is quality
14 assurance is the effort to assure or get a level of
15 confidence that the software is performing safety
16 functions appropriately.

17 CHAIRMAN APOSTOLAKIS: Without
18 quantitative estimates.

19 MR. ARNDT: Without necessarily having
20 quantitative estimates. That doesn't mean you can't
21 have quantitative estimates, it's just not the primary
22 objective of quality assurance.

23 CHAIRMAN APOSTOLAKIS: Well, let's say
24 that you find yourself sometime in the future, you
25 really trust the risk methods. Then all this would go

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 away, wouldn't it?

2 MR. ARNDT: No.

3 CHAIRMAN APOSTOLAKIS: If I trust a
4 method, and the method tells me I have a 10^{-5} or -6
5 variability, I have a high level of confidence that
6 this is pretty good.

7 MR. KEMPER: Well, but the quality I think
8 is an underlying principle that has to be preserved
9 for those risk performance measures to be valid.
10 Okay? The failure probably is predicated on certain
11 underlying notions.

12 CHAIRMAN APOSTOLAKIS: If it were not
13 preserved, would I get a number as low as 10^{-5} ?

14 MR. ARNDT: Presumably not --

15 CHAIRMAN APOSTOLAKIS: No.

16 MR. ARNDT: But the point is we're not a
17 risk-based organization, nor are we likely to be.

18 CHAIRMAN APOSTOLAKIS: I put you in a
19 hypothetical situation.

20 MR. ARNDT: Okay.

21 CHAIRMAN APOSTOLAKIS: So this it seems to
22 me is important because we cannot do the other thing.
23 We cannot really estimate risks with any kind of
24 confidence.

25 MR. ARNDT: Well, you get into the same

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 basic state that we have in any part of the business.
2 I mean, we have Appendix B, and we don't -- we can
3 grade quality, if you will, by risk, but you don't get
4 rid of quality assurance.

5 CHAIRMAN APOSTOLAKIS: No, you don't.

6 MR. ARNDT: Because you need to have that
7 understanding that the process is working, that there
8 was appropriate --

9 CHAIRMAN APOSTOLAKIS: Because a lot of
10 these things cannot be modeled in the PRA.

11 MR. ARNDT: That's right. And even if
12 they can be, you're never going to have 100 percent
13 confidence. So there's several different ways you
14 attack the problem. The purpose of this program is
15 simply to use the software engineering methods that
16 are out there to try and make software quality
17 assurance evaluations better.

18 CHAIRMAN APOSTOLAKIS: But the fault
19 injection technique, for example, it has, you know,
20 you inject the faults and see what happens and so on.
21 And then they go on to do some numerical calculations.
22 You don't mean that the whole package here, I mean,
23 part of it may be useful, part of it may not.

24 MR. ARNDT: Yes. The real issue in these
25 programs -- and I don't want to talk through all the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 programs because we have presentations for that -- is
2 to gain a better understanding of both the process and
3 the product itself, understand how the system works or
4 doesn't.

5 CHAIRMAN APOSTOLAKIS: Okay. So you have
6 presentations on each one of these?

7 MR. ARNDT: Yes.

8 CHAIRMAN APOSTOLAKIS: Okay, great. Let's
9 go on then.

10 MR. KEMPER: Okay. As a matter of fact,
11 the next presentation is by Norbert Carte, and Steve
12 Arndt also will participate in this, and also this is
13 Ming Li from the University of Maryland.

14 MR. CARTE: Hello. My name is Norbert
15 Carte. I am also in the I&C section, Engineering
16 section of the Engineering Research Applications
17 Branch. I've been with the NRC since early February,
18 and prior to that I spent 13-plus years performing
19 verification and validation of various digital systems
20 in the nuclear industry. I'll be presenting today
21 with Ming Li, one of the researchers from the
22 University of Maryland. And I'll allow him to
23 introduce himself.

24 DR. LI: My name is Ming Li. I'm a
25 research associate at the Center for Reliability

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

(202) 234-4433

www.nealrgross.com

1 Engineering at the University of Maryland in College
2 Park. I've been a key researcher for this project
3 since 1998. I hold a Bachelor's degree in Electrical
4 Engineering, and the Master's in Systems Engineering,
5 and the Ph.D. in Reliability Engineering. My research
6 interests include software engineering, reliability
7 engineering, software measurement, software testing,
8 and the PRA. Thank you.

9 CHAIRMAN APOSTOLAKIS: So I take it you
10 will talk about the metrics?

11 DR. LI: Right.

12 MR. CARTE: Ming will be talking about two
13 metrics in detail, and I'll be giving an overview of
14 the program itself. So we'll start off with a
15 discussion of the issues facing the NRC, some of which
16 you've heard previously, as well as the basis of the
17 current engineering project, and then discuss two
18 metrics in detail, and follow on with a brief
19 discussion of future work and conclusions.

20 The basic issue facing the NRC is
21 regarding the increasing size and complexity of
22 submittals. And this will result in an increased
23 workload, and with the limited staff that could
24 present some problems. Software is currently being
25 used in more systems as well as an increase in the use

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 of self-checking software and other techniques result
2 in more complex systems. Also, with the use of
3 commercial off-the-shelf equipment we have more
4 powerful development environments, and that means that
5 software programming is becoming more complex, or
6 abstract, as well as many of the details are becoming
7 hidden. Software engineering methods are also
8 becoming more powerful and usable, and therefore can
9 be used to address these issues.

10 CHAIRMAN APOSTOLAKIS: Now, are these
11 comments true for existing reactors? I mean, are we
12 really using complex software? Not for future
13 reactors. I am talking about, you know, control and
14 all that, feedback. I mean, what is the level of the
15 sophistication of the software that are being used in
16 safety-related functions these days?

17 MR. CARTE: Well, the question is not
18 necessarily just what is currently being used,
19 although I believe there are some 30 systems that have
20 been approved. There are, in general, three SERs,
21 Triconex, Westinghouse, and Teleperm TXS which propose
22 using development environments and systems, and the
23 potential application is for plant-wide
24 modernizations. And the obsolescence issue will
25 result, possibly, in many plants wanting to do

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 complete plant-wide modernizations. And there are
2 some -- but currently what we see are system-level
3 modernizations.

4 CHAIRMAN APOSTOLAKIS: Are there any
5 plants right now that are using digital software in
6 safety-related functions?

7 MR. CARTE: Safety-related. I think
8 Vogtle has a diesel sequencer that uses a Westinghouse
9 ABB Advant system.

10 MR. KEMPER: Sure, the CE System 80 Plus
11 design. It's got a compression calculator. Let's
12 see. What is it, the Eagle?

13 CHAIRMAN APOSTOLAKIS: What is that
14 system?

15 MR. KEMPER: Eagle 21.

16 MR. WATERMAN: Eagle 21 is a reactor
17 protection system.

18 MR. KEMPER: Yes. There are numerous
19 spotted applications out there, but it's not on a
20 generic-wide basis.

21 CHAIRMAN APOSTOLAKIS: So the reactor
22 protection system is basically monitoring and then
23 SCRAMming?

24 MR. KEMPER: Right, it's a trip system.
25 Exactly. But like the core protection calculator is -

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1

-

2

CHAIRMAN APOSTOLAKIS: But aren't these relatively simple systems?

4

5

6

7

8

9

MR. KEMPER: Well, the basic function of tripping, you know, comparing a set point to a parameter and then tripping your relay is, but like the core protection calculator, it's got a fair amount of sophistication involved with calculating that variable trip set point.

10

11

MR. WATERMAN: And those have always been digital in several plants.

12

13

14

15

16

17

18

19

20

21

22

23

MR. KEMPER: The point here though I think that Norbert's trying to make, and excuse me for breaking in on you here Norbert, is that increasing complexity and size of submittals. There's nothing to prevent licensees from making submittals for plant-wide upgrades. In fact, when I was at Calvert, that's one of the last projects that we concluded was a plant-wide digital upgrade project for, you know, cost us \$60 million over the next 10 years. So this is what's going on out there in the industry, and that's what we're being subjected to. Those submittals could come at any time.

24

25

CHAIRMAN APOSTOLAKIS: Is the Oconee license amendment request that was mentioned this

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 morning the first serious step towards using digital
2 I&C in safety systems?

3 MR. ARNDT: Well, I don't know if you'd
4 call it the first serious step, but it is a very large
5 step that will include RPS and SFAS and other systems.

6 MR. KEMPER: I believe that's true though.
7 That's a good way to quantify it. I mean, others, I
8 think Callaway approached this once, and then they
9 withdrew after some interaction with the staff.

10 CHAIRMAN APOSTOLAKIS: Because the
11 regulatory stuff more seems to feel that this is
12 really --

13 MR. KEMPER: Yes, I think it is.

14 MR. CARTE: Well, it also represents a
15 change. The fact that you're integrating two systems
16 into one system. You're integrating the RPS and the
17 SFAS. And digital systems allow for that sort of
18 thing.

19 CHAIRMAN APOSTOLAKIS: Yes. Yes, I agree.
20 I'm trying to get a picture. Anyway, keep going.

21 MR. CARTE: Okay. So as has been gone in
22 a little more detail this morning, the current review
23 process is basically a software development review
24 process as well as some sample threat audits that are
25 selected by the reviewer. Standard review plan is a

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 generic plan, and it requires an application-specific
2 review plan. The reason I point that out is there are
3 different programming paradigms, such as structured
4 programming, for instance something programmed in C,
5 object-oriented programming in C++, and programmable
6 logic controllers. Each represent a different
7 paradigm, will have different vulnerabilities or
8 weaknesses and different strengths. And therefore it
9 might be better to have specific review criteria for
10 different paradigms, as well as potentially measures.

11 The reg guides that currently endorse
12 generic IEEE standards, in other words they're not
13 programming paradigm-specific, as well as the current
14 standard review plan does not address the use of
15 measures.

16 CHAIRMAN APOSTOLAKIS: I noticed both in
17 the previous presentation and this one, you guys are
18 very careful to point out, you know, this is where we
19 are, this is where we're going. I didn't get that
20 impression from the plan that I reviewed. Is the new
21 version going to be as explicit? I understand you are
22 revising it now, right?

23 MR. KEMPER: Yes, we are. And --

24 CHAIRMAN APOSTOLAKIS: Because this is
25 really the way it ought to be. This particular issue,

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

1 this is what's happening now, these are the issues,
2 and this is how we're going to help. I sense there is
3 a disconnect there.

4 MR. KEMPER: Well, we --

5 CHAIRMAN APOSTOLAKIS: But I reviewed the
6 earlier version I must say, so I know that you are
7 revising it now. But it would be nice to spend a few
8 extra hours, Bill, to make sure that it's very clearly
9 stated in each section where we are and where we're
10 going. I think that's the main idea behind a good
11 plan.

12 MR. KEMPER: I think that's absolutely
13 right. We attempted to do that in the initial draft.
14 We provided a background for each one of them which
15 really addressed the issues, here's the problem
16 statement, if you will, and then the task that we
17 intended to accomplish. So certainly it's obvious we
18 need to embellish that. We'll do that.

19 CHAIRMAN APOSTOLAKIS: That's all. Yes.
20 Okay, let's move on. Boy, you're really slow, aren't
21 you? You've been here only since February you say?

22 MR. CARTE: Yes.

23 CHAIRMAN APOSTOLAKIS: Well, we joke every
24 now and then.

25 MR. CARTE: Yes. So the current research

1 goals. The objective of this research is to perform
2 a large-scale validation of measures identified
3 previously through previous research to quantitatively
4 assess the quality of software.

5 CHAIRMAN APOSTOLAKIS: You know, this now
6 raises the expectations. You say quantitatively. I'm
7 looking for numbers.

8 MR. CARTE: Yes.

9 CHAIRMAN APOSTOLAKIS: Do you want to
10 delete that word now, or?

11 MR. CARTE: No.

12 CHAIRMAN APOSTOLAKIS: Shall we keep
13 looking for numbers?

14 MR. CARTE: Well, numbers in themselves
15 aren't bad.

16 CHAIRMAN APOSTOLAKIS: Well, that's what
17 quantitative means.

18 MR. CARTE: Yes. The question is how you
19 use those numbers.

20 CHAIRMAN APOSTOLAKIS: No, no, no. I
21 would like to know whether you produce them first.

22 MR. CARTE: That is the intent, yes.

23 CHAIRMAN APOSTOLAKIS: So this is all
24 quantitative?

25 MR. CARTE: Yes.

1 CHAIRMAN APOSTOLAKIS: All right. Let's
2 see. Okay.

3 MR. CARTE: That is, we envision the
4 incorporation of measures to produce standardized
5 quantifiable evaluations. Now, the question of what
6 you do with those numbers relates to the acceptance
7 criteria. How do you establish an acceptance criteria
8 once you have a repeatable number generation system.
9 And there are different ways of establishing
10 acceptance criteria. Some are theoretical, and others
11 include benchmarking it, or some combination of
12 theoretical and benchmarking.

13 The purpose of this research is to be
14 flexible as well, to look at measures that could be
15 used by the licensee, the NRC, or both. And also, we
16 want to address how you compare or combine different
17 assessments. So when you look at a software design
18 description, or a software requirements
19 specifications, and have a quality determination, how
20 do you compare those? Are you comparing apples and
21 oranges? Or how do you compare the thoroughness or
22 completeness of testing to the quality of the software
23 requirement specification? One method of performing
24 such a comparison is a Bayesian method, which
25 basically relies on a probably or confidence, and then

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 using the Bayesian techniques to combine them. The
2 other way would be to normalize the quality assessment
3 in terms of some common measure or metric, such as
4 defect density or reliability. The other goals of
5 this research are to address the issues previously
6 raised.

7 CHAIRMAN APOSTOLAKIS: You are not going
8 to develop any methods that are usable by the
9 licensees and not the NRC? I mean, you better
10 rephrase that. You say they're licensee, NRC, and/or
11 both.

12 MR. CARTE: Yes.

13 CHAIRMAN APOSTOLAKIS: Well, no. You're
14 developing tools for the NRC, right? You are a member
15 of this agency.

16 MR. CARTE: Yes.

17 CHAIRMAN APOSTOLAKIS: If the licensee
18 wants to use them, fine. I can assure you that we'll
19 --

20 MR. KEMPER: That's what we meant to say,
21 actually.

22 CHAIRMAN APOSTOLAKIS: I know. I know.
23 So change the words.

24 MR. CARTE: Okay. The use of metrics for
25 quantifying software quality has a large basis in

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 literature. To give you an example, I've listed three
2 IEEE standards regarding the use of measures and
3 metrics. In particular I wanted to point out in 1061,
4 one of the statements which says, "The use of software
5 metrics does not eliminate the need for human judgment
6 in software evaluations." So it is not the intent to
7 replace human judgment, it's to provide more
8 resolution, more information to the individual
9 performing that judgment.

10 From that general literature and industry
11 search, Lawrence Livermore Laboratory identified a
12 pool of 78 measures. From that pool, the University
13 of Maryland selected 30 measures, and categorized
14 those measures in terms of the lifecycle phase to
15 which they were applicable, as well as the semantic
16 category, such as size and complexity. This was done
17 in part to ensure all areas were covered, all
18 lifecycles, and all semantic families.

19 They then elicited expert opinion in order
20 to rank those measures and families. They also
21 elicited peer review to evaluate the research
22 performed. They also performed a preliminary
23 evaluation which was published in the NUREG/CRITERIA
24 that's identified, as well as wrote some publications
25 in peer reviewed journals.

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 MEMBER WHITE: Excuse me. The peer
2 reviewed journals, are those journals in which the
3 software community normally publishes? So they're not
4 just our industry journals, is that correct?

5 DR. LI: Yes.

6 MEMBER WHITE: Thank you.

7 CHAIRMAN APOSTOLAKIS: Like which one?

8 DR. LI: IEEE Transactions on Software
9 Engineering.

10 CHAIRMAN APOSTOLAKIS: So you're going to
11 tell us what it is, right? Soon.

12 MR. CARTE: Yes.

13 CHAIRMAN APOSTOLAKIS: Okay.

14 MR. CARTE: So the large-scale validation
15 project being performed by the University of Maryland
16 selected a sample of the measures. It is not
17 validating all 30 measures. It selected that sample
18 from the different classes of measures, some highly
19 ranked measures, some medium, some low ranked
20 measures, as well as different semantic -- from
21 different semantic families. One example of a
22 semantic family is the functional size, such as
23 feature point, function point, or full function point,
24 and complexity, such as cyclomatic complexity. And
25 these measures were applied to all phases of the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 software development lifecycle in a nuclear reactor
2 protection system.

3 So the issues raised previously. In the
4 NUREG itself, the issues raised identified during the
5 peer review was that it was -- the preliminary
6 validation was performed on a relatively software
7 application. The application was not a nuclear safety
8 system, which means that they looked at a low
9 reliability system, as opposed to an ultra high
10 reliability system. The benchmarking of the data did
11 not use real operational profile, and it looked only
12 at one phase of the software development lifecycle.
13 And these issues are addressed in the current research
14 project.

15 The ACRS addressed some of these issues,
16 as well as some others. One is the ease of obtaining
17 the metric. The current research will provide an
18 evaluation of the ease of use for the metrics that
19 they validated. A comment was software-centric versus
20 a system-centric approach. We are more conscious or
21 aware of the need to consider the entire system, and
22 are looking at it from that perspective, although we
23 are primarily looking at systematic failures that have
24 a software origin.

25 Another issue raised was that the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 uncertainty in the preliminary research was greater
2 than the required reliability of the ultra high
3 reliability systems. That is an issue we're conscious
4 of, and we're looking at the research to address that,
5 but some things to think about. With a low
6 reliability system we had lower reliability numbers
7 and higher -- and larger uncertainties than we would
8 desire for an ultra high reliability system. The
9 other issue is that this is not necessarily a new
10 issue. If we have qualitative evaluations, there is
11 always an uncertainty associated with a qualitative
12 evaluation. The problem is we haven't specified what
13 reliability is required, or we haven't talked about
14 the uncertainty associated with that qualitative
15 evaluation. So it's not necessarily a new issue,
16 we're just trying to resolve that issue, and it
17 becomes more visible when we start talking
18 quantitatively. And I just want to point out that
19 measures do not eliminate the need for human judgment.

20 The other ACRS comment was regarding the
21 validity/robustness of the measures. So we are
22 applying the measures to a different type of system,
23 a different function, so we're looking at an RPS
24 rather than a door entry system. We're looking at
25 different programming languages, such as C & Assembler

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 versus C++. So with that I'll turn the discussion
2 over to Ming.

3 DR. LI: Our current technical goal is to
4 try to quantify software quality through software
5 engineering measurement.

6 CHAIRMAN APOSTOLAKIS: You need a
7 microphone if you're going to stand up.

8 DR. LI: I'll sit here, sorry.

9 CHAIRMAN APOSTOLAKIS: Yes, you keep
10 talking and we will try to find him. Yes, you can use
11 the cursor.

12 DR. LI: The philosophy behind this
13 research is summarized as the answer to a question
14 what determines software quality. In general,
15 software quality is determined by the software
16 product, the characteristics, in particular the defect
17 remaining in the software, and how the software may be
18 used. The way software is used is summarized using
19 the concept of operational profile. Software product
20 characteristics can be further determined by the
21 product characteristics, for instance, what type of
22 application is it, how big is the functional sizes.
23 And the process characteristics, for instance, how
24 good the developer's skills are, how tight the budget
25 is, what development tools and methods are used,

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

(202) 234-4433

www.nealrgross.com

1 etcetera. All these characteristics can be explicitly
2 or implicitly described using software engineering
3 measurements. Therefore, an obvious inference is
4 software engineering measurements determine software
5 quality.

6 CHAIRMAN APOSTOLAKIS: You seem to be
7 focusing on numbers here.

8 DR. LI: Right, I'm going to talk about
9 numbers shortly.

10 CHAIRMAN APOSTOLAKIS: But I don't care
11 about the number of defects. If I have one that is
12 fatal, that really bothers me. So it's not really the
13 number. I mean, it's important to know the number,
14 but --

15 DR. LI: Right, right --

16 CHAIRMAN APOSTOLAKIS: When do you focus
17 on the significance of the defect?

18 DR. LI: Right, I'll talk about it
19 shortly.

20 CHAIRMAN APOSTOLAKIS: You'll talk about
21 it. Okay.

22 DR. LI: So the following steps are taken
23 to pursue this technical goal. First, to estimate the
24 number of defects remaining in the software, and
25 second, to quantify the likelihood that these defects

1 result in system failures.

2 I'll talk about the procedure, the steps,
3 using two examples. The first example is defect
4 density. Defect density, defined as a ratio of unique
5 defects found by inspections to the size of the
6 product. The defects are classified into different
7 criticality levels. And the inspections are
8 requirement inspections, design inspections, and code
9 inspection.

10 CHAIRMAN APOSTOLAKIS: How do you measure
11 the size of the product?

12 DR. LI: The size can be either the source
13 code size or the document size. The source code size
14 can be the line of code, or it can be the function
15 point. And the document size can be the number of
16 pages, or it can be the number of paragraphs, or
17 number of lines.

18 The effect of that, the requirement
19 inspection, design inspection, and code inspection
20 allow us to predict software quality at an early
21 stage. Defect density has been widely accepted in the
22 industry and academia. For instance, IEEE Standard
23 982.2 includes this measure. And the defect density
24 is the de facto standard to measure software quality.
25 A significant amount of research has been done using

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 this measure as a quality indicator.

2 MEMBER WHITE: I have a question about the
3 size of the product. How do you handle the number of
4 relationships that data have to other data, or that
5 some line of software would have to data. In other
6 words, I guess that's a complexity, actually, issue.

7 DR. LI: No, it's size, not complexity.
8 They're different.

9 MEMBER WHITE: All right. So -- but you
10 do take that into account then?

11 DR. LI: Right, right.

12 MEMBER WHITE: Okay, thank you.

13 CHAIRMAN APOSTOLAKIS: Well, I still don't
14 understand. You say it's a de facto standard measure
15 of quality. What is? You're doing a review of
16 requirements and the code and all that, you identify
17 the defects, and then you take that number, you divide
18 by the size of the product?

19 DR. LI: Right, these are --

20 CHAIRMAN APOSTOLAKIS: What does that tell
21 me now?

22 DR. LI: Well, that tells, you know, that
23 -- it's the density. It tells how many defects
24 potentially --

25 CHAIRMAN APOSTOLAKIS: I have found.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 That's all it tells me.

2 DR. LI: Right, that have found. Right.

3 CHAIRMAN APOSTOLAKIS: So why is that a
4 measure of quality?

5 DR. LI: Well, because the more you have
6 the lower quality of your product. This measure
7 historically --

8 CHAIRMAN APOSTOLAKIS: But again, wait a
9 minute now. Are you applying this to a product that
10 somebody tells you is ready to be used, or to a
11 product that is in the process of being produced?

12 DR. LI: Sorry, I didn't get it
13 completely.

14 CHAIRMAN APOSTOLAKIS: If it's part of the
15 process, then you do find defects, because that's the
16 whole idea. So are you doing it after the fact? In
17 other words, now somebody has produced a product and
18 says put it in your plant, and you go there, and you
19 do a review, and you find a few errors.

20 DR. LI: Well --

21 CHAIRMAN APOSTOLAKIS: Is that what you
22 mean?

23 DR. LI: Right. You can do both. In our
24 institution, in our research right now we are doing,
25 you know, the latter situation. We have a real

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

(202) 234-4433

www.nealrgross.com

1 application from nuclear power plants. We have the
2 entire document. And we are doing the inspection,
3 from requirements to the code.

4 CHAIRMAN APOSTOLAKIS: Okay. So you find
5 a particular number.

6 DR. LI: Right.

7 CHAIRMAN APOSTOLAKIS: And it certainly
8 gives you an idea of how good it is, yes, I can't
9 disagree with that. Sure.

10 DR. LI: Next we will quantify --

11 CHAIRMAN APOSTOLAKIS: You already have
12 quantified.

13 DR. LI: -- the likelihood of these
14 defects to the system failure.

15 CHAIRMAN APOSTOLAKIS: So far you have
16 found the number of defects, and you divided by the
17 size, and that's a number.

18 DR. LI: Right, that's a number.

19 CHAIRMAN APOSTOLAKIS: That's fine.

20 DR. LI: This is a standard. In other
21 words, this is a measure found in the industry.

22 CHAIRMAN APOSTOLAKIS: Okay, let's go on
23 and see now what you do with that number.

24 MEMBER GUARRO: One question.

25 DR. LI: Yes.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MEMBER GUARRO: What is your definitional
2 defect in this context?

3 DR. LI: Well, we adopted IEEE definition,
4 which is a deviation from the requirements. So all
5 the terminology is here.

6 CHAIRMAN APOSTOLAKIS: So everything is
7 compared to the requirements. If the requirements
8 themselves are not self-consistent, what would that
9 be?

10 DR. LI: Sorry?

11 CHAIRMAN APOSTOLAKIS: The requirements
12 themselves are not a self-consistent set. Would that
13 be a defect?

14 DR. LI: Right.

15 CHAIRMAN APOSTOLAKIS: Or you would never
16 find it?

17 DR. LI: Well, we have specific measures
18 to this --

19 CHAIRMAN APOSTOLAKIS: But that's not a
20 deviation from the requirements. That's faulty
21 requirements.

22 DR. LI: If there are any inconsistencies
23 in the requirements, we have a specific measure to do
24 that.

25 CHAIRMAN APOSTOLAKIS: But not this one.

1 DR. LI: Not this one.

2 CHAIRMAN APOSTOLAKIS: Okay. Okay.

3 DR. LI: We have certain measures.

4 MEMBER GUARRO: Okay, but also in -- just
5 to pursue for a moment the issue here. Do you
6 differentiate requirements in levels of criticality?

7 DR. LI: Yes.

8 MEMBER GUARRO: So you will classify
9 defects also according to --

10 DR. LI: To the criticality level.

11 MEMBER GUARRO: -- the criticality level?

12 DR. LI: Yes.

13 MEMBER GUARRO: Okay.

14 MEMBER KRESS: And then what would you do
15 with that classification? Would you put a weighting
16 factor on the quantifier?

17 DR. LI: We have a specific technique so
18 we can propagate this different criticality defect to
19 the --

20 MEMBER KRESS: To the --

21 DR. LI: To the probability of failure.
22 Because we can't review them differently. I will talk
23 about shortly, you know, that special technique.

24 So given the value of defect density, then
25 we can calculate the number of defects in the software

1 using this simple --

2 CHAIRMAN APOSTOLAKIS: Wait a minute, now.
3 That's how you started. What do you mean you can
4 calculate? You found them.

5 DR. LI: Right, right. We found the
6 number of defects.

7 CHAIRMAN APOSTOLAKIS: Yes.

8 DR. LI: This assumes that if you have a
9 defect density number provided by someone else, how
10 you get to the number of the defects.

11 CHAIRMAN APOSTOLAKIS: This is a big step
12 here. So you're saying 'I found the DD in a
13 particular program, and now somebody gives me another
14 program.'

15 DR. LI: No, no, no. That's --

16 CHAIRMAN APOSTOLAKIS: I don't understand
17 the situation.

18 DR. LI: There's two different situations
19 here.

20 CHAIRMAN APOSTOLAKIS: Yes.

21 DR. LI: This relationship I just put here
22 to highlight the relationship between the number of
23 defects and defect density.

24 CHAIRMAN APOSTOLAKIS: Oh. So that's the
25 definition of DD.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 DR. LI: Right, right.

2 CHAIRMAN APOSTOLAKIS: All right.

3 DR. LI: So they found the standard, but
4 the inspection may not find all the defects. The
5 number of such latent defects can be estimated
6 statistically using the capture/recapture techniques.
7 Capture/recapture techniques were first applied in a
8 study of the fish and wildlife populations. The
9 simplest capture/recapture technique is a so-called
10 two sample model. The first sample provided to
11 individuals captured a mark that returned to the
12 population, and the second sample provided the
13 individuals recaptured. Using the number of
14 individuals captured in both samples, and if the
15 numbers captured is adjusted by one sample, one can
16 estimate the number of not captured individuals, and
17 then the entire population of the wildlife.

18 Recently, this technique has been applied
19 in the software engineering field to estimate the
20 number of defects not found by the inspection. In
21 these applications, the number of defects is the
22 analogy to the animal population size.

23 CHAIRMAN APOSTOLAKIS: Wait a minute. You
24 are saying that you can estimate the population size
25 from a small sample?

1 DR. LI: Right.

2 CHAIRMAN APOSTOLAKIS: Wow.

3 DR. LI: This technique has been --

4 CHAIRMAN APOSTOLAKIS: Don't you have to
5 make some additional assumptions? I mean.

6 DR. LI: Right.

7 CHAIRMAN APOSTOLAKIS: So let's say I want
8 to know how many coyotes there are in a particular
9 place. What do I do? Capture a few and then
10 extrapolate, or what?

11 DR. LI: Well, this is an entire
12 discipline. And this technique has been validated for
13 over 30 years in biology.

14 CHAIRMAN APOSTOLAKIS: Yes -- no. This is
15 not an argument you can use here. You have to tell us
16 why. You're asking me to believe somebody else. I
17 have difficulty doing that. I don't understand how
18 you can find five defects, and then you are able to
19 tell me how many more there are. There's something
20 missing there.

21 MR. CARTE: There's a couple of ways that
22 this technique can be applied. One way, if you look
23 at the animal population, you would choose a capture
24 area that is representative of the total area. So in
25 a software system, you would choose a set of modules

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

(202) 234-4433

www.nealrgross.com

1 that are representative of all the modules in the
2 system in terms of size, complexity, in terms of the
3 different programmers or programming groups. So if
4 you had a representative sample of modules that you
5 applied this technique to, then you could estimate for
6 the whole population.

7 CHAIRMAN APOSTOLAKIS: So there are
8 additional assumptions, then. As you say, you go to
9 an area that is more or less representative, and then
10 you assume the density of animals is the same as in
11 the bigger area.

12 MR. CARTE: Yes, that would be --

13 CHAIRMAN APOSTOLAKIS: Then I can
14 understand how you can find that, but the question is
15 whether these assumptions are valid.

16 MR. CARTE: Yes. That's one way that the
17 measure can be applied. The other way that this
18 measure could be applied, and that's why I mentioned
19 licensee earlier, is if a licensee were to apply such
20 a measure, they already have systems in place in terms
21 of their QA procedures that completely review the
22 entire system. They have multiple reviews in place.
23 So if you used a capture/recapture model with removal,
24 in other words once the defect is identified it's
25 removed, and the multiple reviews, you can use these

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

(202) 234-4433

www.nealgross.com

1 techniques to estimate the number of defects
2 remaining, and the type of defects, because you can
3 categorize the type of defects found. So it can be
4 applied in a complete system review by a licensee. I
5 do not think that the NRC would be interested in
6 having multiple reviewers do a complete review of the
7 entire system of documentation. For that particular
8 application, it is less likely to be done by the NRC,
9 but reviewing a sample is more likely to be done. So
10 in that sense it can be used.

11 CHAIRMAN APOSTOLAKIS: And that number of
12 remaining defects can never become zero, can it?
13 Because of the way you have structured the method?
14 Which means now you have to tell NRR that if that
15 number falls below a certain number it's acceptable.

16 MEMBER KRESS: It seems to me like this
17 assumes you know the curve for the capture/recapture
18 value versus the number of defects.

19 MR. CARTE: Well, the capture/recapture
20 model, there's three methods of using defect density.
21 There are in general three methods of using defect
22 density to characterize remaining populations. One is
23 capture/recapture, the other would be a neural network
24 approach, and another would be the family of curve-
25 fitting methods that you describe. But basically if

1 you have sufficient data, the equations behind
2 capture/recapture are supposed to characterize the
3 likelihood of capture of different types of defects
4 because you have multiple reviewers and multiple
5 capture rates. And so you can get estimates.

6 MEMBER KRESS: I can buy this. You do it
7 several times and you get the start of a curve and
8 extrapolate this curve.

9 MR. CARTE: Right. You have to have --

10 MEMBER KRESS: I don't see where a neural
11 network comes into play.

12 MR. CARTE: Right. The idea with a neural
13 network is that maybe these systems are non-linear,
14 and neural networks do better at matching those.

15 MEMBER KRESS: See, it's just a way to
16 correlate the data if it's non-linear.

17 MR. CARTE: Right.

18 CHAIRMAN APOSTOLAKIS: But are you going
19 to tell us what to do with that number?

20 DR. LI: Yes. Next. Given the number of
21 defects remaining in software, we utilize the so-
22 called fault propagation technique to study the
23 likelihood of these defects caught to the -- sorry,
24 that the failure probability caught by this number of
25 defects. And as the software engineering study has

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

(202) 234-4433

www.nealrgross.com

1 shown, a defect will manifest itself as a failure if
2 and only if the three following conditions are
3 satisfied. First, this defect needs to be executed.
4 Second, this defect needs to create a space anomaly.
5 And the third, this state normally needs to propagate
6 to the output of the software.

7 These three conditions are summarized in
8 the PEI models proposed by Jeff Voas. And this is
9 published in the 1990s in IEEE Transactions on
10 Software Engineering. In these models, E represented
11 the probability that a particular section of program
12 is executed. I represented the probability that the
13 execution of the execution of the problematic location
14 affects the data state. And the P, the probability
15 that an infection of the data state affects system
16 output. Given the availability of P, I, and E, the
17 software quality indicator, or the probability of
18 failure per demand can be given using this equation.

19 Next, we utilize finite state machine
20 techniques to quantify this model. Finite state
21 machine models system behavior. This example models
22 PIN entering function for a sample security gate
23 system, which requires the entrant to enter the PIN.
24 This model starts from the entry state, and at the end
25 of the way the exit state. A rectangle represents a

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 state. An arc represents a tradition. A link from
2 entry to exit constitutes a task. The probability of
3 each transition are embedded in the finite state
4 machines. So the probability of each task can be
5 calculated as a product of the probability of each
6 transition within that task.

7 CHAIRMAN APOSTOLAKIS: Can you give us an
8 example?

9 DR. LI: Yes. For instance here, you have
10 the -- from the start, you need to enter the PIN. The
11 PIN, you have two conditions. One is a good PIN, and
12 the other one is a bad PIN. So the probability of the
13 good PIN can be 0.8, and the probability of the bad
14 PIN can be 0.2.

15 CHAIRMAN APOSTOLAKIS: Why?

16 DR. LI: This data is from the user
17 profile, from the log file. We obtain this data from
18 the field data, from this profile from the field data.

19 CHAIRMAN APOSTOLAKIS: And?

20 DR. LI: Then we map the defects to this
21 model. And this dashed line shows the defects located
22 here. Then we know the task that travels this
23 transition will lead to a failure. So the integral of
24 the probability of the task that travels this
25 transition will provide us the estimation of the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 probability of failure caused by this defect. We
2 repeat this procedure for all defects. Then we have
3 the overall probability of failure per demand.

4 CHAIRMAN APOSTOLAKIS: And for all defects
5 you will have this information of 0.8 versus 0.2?

6 DR. LI: Right, right.

7 CHAIRMAN APOSTOLAKIS: I can't see how.
8 I mean, this was a very concrete example. You know,
9 you can go there and type in their PIN, and they make
10 a mistake. And you know that, and you can find it.
11 But what if you have something esoteric, somewhere
12 there buried. I mean I don't know how --

13 DR. LI: Well, let's talk about the actual
14 --

15 CHAIRMAN APOSTOLAKIS: You know the
16 probability of each path. Wow. That's a pretty
17 strong statement, isn't it? Because that assumes that
18 all these probabilities are external, aren't they?

19 DR. LI: Well, currently --

20 CHAIRMAN APOSTOLAKIS: That would be which
21 probability that you showed us earlier, P?

22 DR. LI: That's P.

23 CHAIRMAN APOSTOLAKIS: Okay.

24 DR. LI: Oh, sorry.

25 CHAIRMAN APOSTOLAKIS: That's P?

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 DR. LI: No, that's E. Execution.

2 CHAIRMAN APOSTOLAKIS: Okay.

3 DR. LI: And with the way we build this
4 finite state machine, we can guarantee that E and I
5 are equal to 1.

6 CHAIRMAN APOSTOLAKIS: So if I have now a
7 reactor protection system, it's monitoring a fairly
8 large number of parameters, you will be -- wouldn't E
9 be the probability of any possible combination of
10 values of these?

11 DR. LI: That's correct.

12 CHAIRMAN APOSTOLAKIS: And you will know
13 what the probability of these combinations is?

14 DR. LI: Yes. Currently --

15 CHAIRMAN APOSTOLAKIS: How on earth would
16 you know?

17 DR. LI: Currently we have the data from
18 the actual nuclear power plant.

19 CHAIRMAN APOSTOLAKIS: How would you know?

20 DR. LI: They maintain a comprehensive log
21 data, data file.

22 CHAIRMAN APOSTOLAKIS: No, but I'm talking
23 about accidents here. I'm not talking about normal
24 operations.

25 DR. LI: Yes, that's what I'm talking

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 about.

2 CHAIRMAN APOSTOLAKIS: How many accidents
3 have we had? So that we'll be able to say the
4 probability of this combination of variable values is
5 that. I don't see how we can know that. I mean, you
6 can have weird situations where you have to SCRAM.
7 And you're saying, no, I will know the probability
8 that I will have this weird combination. Maybe you
9 do, but I have to be convinced a little more.

10 MEMBER GUARRO: Well, this brings back a
11 point that was, I think in a previous chart there was
12 as an indicator of quality was mean time to failure.
13 Mean time to failure is something you can measure in
14 a system that you operate normally. You can observe
15 and recover from failures. But when you're talking
16 about severe accidents, mean time to failure is
17 something that doesn't mean much as an indicator of
18 performance, because you don't see mean time to
19 failure as measurable, right? So this is an important
20 point to keep in mind when translating statistics
21 taken from a routine type of application,
22 extrapolating to a rare accident scenario type of
23 application.

24 CHAIRMAN APOSTOLAKIS: Yes. And how would
25 this apply to the examples, who did it this morning,

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

(202) 234-4433

www.nealrgross.com

1 I think it was Mike Waterman. The Turkey Point and
2 Davis-Besse, real incidents. Would you take -- not
3 right now -- would you take your model and go to that
4 piece of operating experience and tell us how you
5 would have predicted that? How would you have
6 assigned a probability to this problem with the
7 sequencers? I think it's awfully hard. I mean, it's
8 one thing to talk about people typing in personal
9 identification numbers, and quite another dealing with
10 a nuclear reactor.

11 MR. ARNDT: There's two issues here, both
12 of which are important, but have different aspects.
13 One is, as rightly pointed out, your operational
14 profile of how these finite state machines work, and
15 where they go, and things like that, it's difficult to
16 get a complete characterization because, as you get to
17 lower and lower probability events it's harder and
18 harder to predict those. The other issue is
19 predicting by some kind of analysis methodology this
20 one or anything else, interactions that exist,
21 failures or whatever, that you just haven't thought
22 about. By characterizing in a more formalized way the
23 analysis of particular kinds of things. In this case,
24 if you write the detailed state space evaluation of
25 the system, you then have something to hang onto, and

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 you can look at them in a formalized way. So without
2 actually doing the analysis, I would say likely we
3 would have caught things like the Turkey Point
4 analysis, because we just didn't look at it, because
5 we didn't have a formalized, organized way to look at
6 it. Both of those are very valid points, but they're
7 different issues.

8 CHAIRMAN APOSTOLAKIS: Yes. But this is
9 not being advertised as being a methodology that helps
10 you look at the structure of the software. It's
11 advertised as a methodology that produces a
12 probability. And it would be critiqued as such. I
13 mean, I fully appreciate that, you know, I mean the
14 standard -- if you do a full tree analysis, you really
15 understand your system independently of how good your
16 numbers at the end are.

17 MR. ARNDT: Yes. And what Bill and I
18 tried to point out in the earlier presentation is that
19 the programs under the software quality assurance
20 program have multiple roles. The primary role is to
21 better understand the system, and secondarily have
22 more quantitative assistant approaches to do that.

23 CHAIRMAN APOSTOLAKIS: And a number of
24 methodologies out there deal with the internal
25 workings of a system.

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

(202) 234-4433

www.nealrgross.com

1 MR. ARNDT: Right.

2 CHAIRMAN APOSTOLAKIS: I have no problem
3 presenting them as such. I do appreciate that you're
4 learning a lot about the system by attempting to do
5 this, and other things. Maybe that should be a
6 project. But when you start saying that I will
7 calculate the probability by taking this integral, and
8 I will need E, P, and whatever else it is, I just
9 don't know that you can do it, Mr. Li. I really want
10 to believe you, but I cannot. So try to convince me.
11 I'm really on your side. I just can't accept this.
12 I think it's too optimistic. I have to be frank with
13 you.

14 DR. LI: I think the best way to convince
15 is to wait for us to finish our real application.

16 CHAIRMAN APOSTOLAKIS: Then it's no fun if
17 I wait.

18 MR. KEMPER: That's what I was going to
19 suggest. This is Bill Kemper again. Perhaps if you'd
20 like --

21 CHAIRMAN APOSTOLAKIS: Okay.

22 MR. KEMPER: -- we can certainly dove into
23 this when we get close to the endpoint and provide
24 whatever exposure you need, George, to the process.

25 CHAIRMAN APOSTOLAKIS: No, I'm not saying

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 that you should stop. I'm just giving you my problems
2 as you go.

3 DR. LI: Yes, I understand that.

4 CHAIRMAN APOSTOLAKIS: But you also have
5 to understand that giving an example with somebody
6 typing in a PIN is not a very convincing argument.
7 You're talking to Advisory Committee Reactor
8 Safeguards. I mean, we don't care what people do when
9 they type their PINs.

10 DR. LI: There's another entire discipline
11 to study how to obtain --

12 CHAIRMAN APOSTOLAKIS: You have to
13 immediately think in terms of safety.

14 MR. ARNDT: Right.

15 DR. LI: Correct.

16 MR. ARNDT: And that was one of the
17 critiques that we got on the preliminary evaluation
18 was that it needs to be a system designed to be
19 implemented in a nuclear environment, which is why
20 we're using a different nuclear system --

21 CHAIRMAN APOSTOLAKIS: Okay.

22 MR. ARNDT: -- for the secondary
23 evaluation. Go ahead.

24 DR. LI: My next example is statement test
25 coverage. Statement test coverage, defined as a

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 portion of software statements executed against a set
2 of test cases. This measure is also --

3 CHAIRMAN APOSTOLAKIS: So excuse me, now
4 you are trying to figure out what P is, is that
5 correct?

6 MR. ARNDT: This is a different measure.

7 DR. LI: That's another measure. Sorry.

8 CHAIRMAN APOSTOLAKIS: Oh.

9 DR. LI: It's on Page 14.

10 CHAIRMAN APOSTOLAKIS: I know. But did
11 you tell us how we would get the other probabilities?
12 Like P and I?

13 DR. LI: Oh. Well, just as I discussed,
14 P and I are equal to 1. You know, the way to develop
15 this finite state machine model can guarantee that P
16 and I are equal to 1. If P and I are not equal to 1,
17 which means there are conditions keep the defect from
18 being infected and propagated. So in the finite state
19 machine model, you should be able to decompose and to
20 identify, the describe these conditions. Just like
21 additional branches. So the advantage of this finite
22 state machine model technique is that you reduce the
23 PIE model to the E model.

24 My next example is test coverage, the
25 statement test coverage. The statement test coverage

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

(202) 234-4433

www.nealrgross.com

1 is defined as the software statements executed against
2 a set of test cases. This measure has also been
3 widely accepted in the industry and academia. The
4 IEEE standard also includes this measure. And this
5 measure is commonly used in the software industry to
6 control testing process. In particular, Malaiya
7 studied the relationship between the defect density
8 and the number -- sorry, test coverage and the number
9 of defects. And this slide summarizes such
10 quantitative relationship. This is empirical
11 relationship. C_1 is a statement test coverage. And
12 C_0 is the intermediate result which represented the
13 portion of the defects found by the testing. And A_0 ,
14 offer 0 to offer 1 are coefficients. And the N_0 is
15 the number of defects found in testing. So N is the
16 number of defects remaining.

17 CHAIRMAN APOSTOLAKIS: C_0 is what, defect
18 calculation?

19 DR. LI: Defect coverage, which is the
20 portion of defects found by testing. N_0 is the number
21 of defects found by testing.

22 CHAIRMAN APOSTOLAKIS: No. Coverage means
23 the portion of statements executed.

24 DR. LI: That's C_1 . It's called test
25 coverage, statement coverage. C_0 is defect coverage.

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

1 This is the intermediate result.

2 CHAIRMAN APOSTOLAKIS: What is the
3 justification of this logarithmic exponential
4 equation?

5 DR. LI: Well, this work --

6 CHAIRMAN APOSTOLAKIS: Is it a vehicle or
7 what?

8 DR. LI: This is an empirical -- well, I
9 will say coefficient relationship. This one published
10 in the International Symposium on Software Engineering
11 Conference. And we validated this relationship using
12 two applications which are summarized in NUREG-6848.

13 CHAIRMAN APOSTOLAKIS: Validated.

14 DR. LI: And again, we utilize finite
15 state machine techniques to quantify --

16 CHAIRMAN APOSTOLAKIS: You know, our
17 handouts don't have the equation. Why? We have
18 blanks.

19 MR. CARTE: That's an editorial problem on
20 my part. They're there, they're just printed in the
21 color white.

22 (Laughter)

23 CHAIRMAN APOSTOLAKIS: White characters on
24 white background. There was a play that won the
25 Pulitzer Prize. It was about a painting that was

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 white stripes and white background.

2 I also, I'm uncomfortable when you say
3 it's used widely by the industry. I mean, our staff
4 went and talked to the industry in the '90s, and the
5 message was don't go near those methods. Not just
6 these, any methods. So now you're saying they're used
7 widely? Maybe that's a slight exaggeration on your
8 part? I mean, does Boeing use things like that? Does
9 Airbus use them? I doubt it. And you know, there was
10 a paper in a conference, yes sure, as you know there
11 are many papers in many conferences.

12 DR. LI: You mean the measure itself --

13 CHAIRMAN APOSTOLAKIS: Yes.

14 DR. LI: -- it's relationship.

15 CHAIRMAN APOSTOLAKIS: Yes. I mean, do
16 you know of any serious industry that's really using
17 it and makes decisions using that?

18 MR. ARNDT: George, part of the issue is
19 a lot of the metrics are used, but exactly what
20 they're used for is really the more appropriate
21 question. Using metrics to improve the development
22 process was the original intent, to, all right, are we
23 getting enough coverage, are we finding enough faults,
24 should we ship a product based on X. Part of the --
25 the whole purpose of this research is can you use

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 metrics that are used in the design process in the
2 assessment process.

3 CHAIRMAN APOSTOLAKIS: I think you're
4 going to have a major problem with this estimation of
5 the number of defects remaining in that you will have
6 to eventually tell us what's acceptable. And I don't
7 know how NRR can approve something knowing that there
8 is a number of defects remaining. On the other hand,
9 you might say we are licensing reactors, so we know
10 there's a probability of a major accident. I don't
11 know, guys. The thing obviously leaves me very
12 uncomfortable. But again, I'm willing to be
13 convinced.

14 MR. ARNDT: One of the other issues is we
15 don't have to use this as a strict quantifiable,
16 go/no-go decision. If we, at the end of the research,
17 at the end of the current project we're looking at,
18 which is trying to validate the methodologies for a
19 larger system, the result may be quantitative go/no-go
20 decisions are not possible. However, the use of the
21 various families of metrics, ones that look at
22 complexity versus ones that look at other things will
23 give us an indication of where in the system there may
24 be bigger problems. The system may be exhibiting too
25 much complexity, it's driving the number up relative

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 to the other metrics, therefore you should spend more
2 time looking at complexity issues. So the point here
3 is we're trying to figure out how much of this can we
4 use in a regulatory environment. I mean, if the
5 project succeeds wildly beyond our dreams, then we
6 could maybe get to the point of quantification for a
7 go/no-go, but that doesn't necessarily mean that's how
8 we're going to use it.

9 CHAIRMAN APOSTOLAKIS: The other
10 philosophical objection I have is that it focuses so
11 much on the number of defects. If you come from the,
12 you know, safety perspective, the number is probably
13 relevant, but really it's the quality. It's the kinds
14 of defects that I have. That scares me much more than
15 just the number. And this seems to be focusing
16 exclusively on numbers.

17 And you know, coming back to Dr. Guarro's
18 question, how do you define the defect? You said the
19 violation of the requirements. Well, that's pretty
20 general. But --

21 MEMBER GUARRO: That could be something
22 when the screen comes the color yellow instead of
23 blue.

24 CHAIRMAN APOSTOLAKIS: Yes. And I have a
25 thousand of those. I don't care.

1 MEMBER GUARRO: It should be blue, and
2 then you define it.

3 CHAIRMAN APOSTOLAKIS: Like you know, the
4 type of the equation is in white. That's a defect.
5 But I don't care. We can fix it. It's not a safety-
6 related defect. I'm interested in the safety-related
7 defect. And I don't see how this can find it. What
8 if you say, okay, you have coverage, right? And you
9 find -- in the previous one, defect density, right?
10 Tell me, what is a typical number of defects one
11 finds? Eleven? I don't know. A hundred? Seventy-
12 two?

13 MR. KEMPER: Slide 18, I think, is where.

14 CHAIRMAN APOSTOLAKIS: 18?

15 MR. KEMPER: In the next few slides we'll
16 give you some numbers, but the point I wanted to try
17 to make though is -- yes, Slide 18, we've got some
18 numbers ahead of you. We're going to talk to you
19 about. But the point I was trying to make here, these
20 metrics -- we've already said it before. It cannot
21 replace the human being, the human element.

22 CHAIRMAN APOSTOLAKIS: Yes.

23 MR. KEMPER: In other words, the idea is
24 these hopefully will be a pointer for experienced,
25 seasoned reviewers to help them assess where they

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 should focus their detailed review.

2 CHAIRMAN APOSTOLAKIS: But again, I don't
3 know. It seems we are going out of our way to find
4 something useful here. Because you say, I mean on
5 Slide 18 it says 210 were highly ranked measures, and
6 so on. What if one of these 210 is failure? Failure.
7 You have core meltdown, and the whole thing. I mean,
8 I wouldn't put it as 1 out of 210. I would say this
9 is really the real deal, I have to look at it, and
10 understand it, and eliminate it. And these methods
11 don't do that. They look at numbers.

12 DR. LI: Well, the fact is that we do look
13 at the criticality. We do look at the effect of
14 different defects.

15 CHAIRMAN APOSTOLAKIS: And then what do
16 you do with them, though? You don't seem to do much
17 about them.

18 DR. LI: Just like I mentioned in this
19 diagram, in order to map that defect to this model,
20 you have to understand semantically what does that
21 defect mean. What the defect --

22 CHAIRMAN APOSTOLAKIS: I know that. But
23 then you go on and calculate densities, you calculate
24 C_1 , C_0 , and so on. The severity enters in a very
25 crude way in your classification of criticality.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 DR. LI: Right, but defect density does
2 count the criticality. Test coverage is a different
3 measure. That's why we have different measures.

4 CHAIRMAN APOSTOLAKIS: Let me ask you
5 something else. Are these gentlemen, or ladies,
6 Pfleeger, Malaiya, are they working on high
7 consequence industries? Or are they working on PCs?
8 I mean, do they worry about severe consequences in
9 their software evaluation?

10 DR. LI: I will say they are software
11 engineering people.

12 CHAIRMAN APOSTOLAKIS: So they don't get -
13 -

14 (Laughter)

15 DR. LI: They work at Microsoft.

16 CHAIRMAN APOSTOLAKIS: Well, I mean, yes.
17 If your biggest worry is that Microsoft Word works
18 most of the time, it seems to me you have a certain
19 number of concerns. And if you don't want to have
20 radioactivity release, you have another number of
21 concerns. Very different approaches. Very different
22 mindsets.

23 MR. ARNDT: There's been work in all parts
24 of the software engineering community. And that's
25 actually one of the biggest challenges in some of

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 these areas, particularly the ones where the
2 quantification, or the analysis is based on empirical
3 curves, is to determine whether or not that particular
4 empirical curve is sufficiently based in safety-
5 related applications, or is it just a compilation of
6 everything. So that those particular issues are
7 things that we're trying to attack at the various
8 points.

9 CHAIRMAN APOSTOLAKIS: Let me understand
10 something else now here. This session is supposed to
11 go until 2:30. Is your presentation going to be until
12 2:30, or there's more?

13 MR. CARTE: I have two slides when he's
14 done.

15 CHAIRMAN APOSTOLAKIS: Okay, okay. So
16 we're doing fine. So can you go to 18?

17 DR. LI: 18?

18 CHAIRMAN APOSTOLAKIS: Well, or no here,
19 17.

20 DR. LI: 17. Okay, this slide summarizes
21 the current status. And we apply 12 measures to a
22 real nuclear application. It's an I&C application.
23 And the measurement in progress and their completion
24 date, summarized in this table. And the further
25 analysis required. By July 15 we need to build up the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 operational profile. By August 15, we need to build
2 the finite state machine. And by August 15, we need
3 to perform a reliability testing. And this -- the
4 final analysis needs to be done by September 30.

5 CHAIRMAN APOSTOLAKIS: Is that when the
6 contract ends?

7 MR. ARNDT: No, the contract goes till
8 November to get the report finished.

9 CHAIRMAN APOSTOLAKIS: Now, last time that
10 you guys were here from Maryland, you told us about
11 how you surveyed experts, and they told you, you know,
12 how, what is the conditional probability that this
13 measure gives you a good idea as to how good the
14 program is. Am I saying it correctly?

15 DR. LI: Well, basically the expert
16 opinion elicitation study provide an indicator about
17 which measure is better in terms of predicting
18 software quality. So that's one --

19 CHAIRMAN APOSTOLAKIS: That was in
20 addition to this.

21 DR. LI: Sorry?

22 CHAIRMAN APOSTOLAKIS: It was in addition.

23 DR. LI: Right.

24 MR. ARNDT: It was an input to this
25 program.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: If it's input then
2 I want to understand how. If -- again, you know, a
3 great way of answering my questions is to put yourself
4 in the shoes of the regulatory staff this morning.
5 They receive this application from Oconee. How would
6 you apply your method to help them make a decision?
7 If you give them a generic statement, like the defect
8 density according to the experts is a good indicator
9 36 percent of the time, I just don't know what they
10 can do with that. Because they are dealing with a
11 specific system. If you can give them more specific
12 information, then more power to you, great. This is
13 really the test, not that somebody presented a paper
14 in 1994. So they have this issue in their hands. How
15 could something like this be helpful to the decision-
16 maker?

17 MR. CARTE: There are a couple of ways
18 that this could be helpful to the decision-maker.
19 One, if the licensee implements a measurement program,
20 then the NRC could review the measurement program and
21 use that to increase their level of assurance that the
22 system provided is okay. One of the things that Steve
23 mentioned earlier is that this research stems from the
24 design engineering research. So basically, when you
25 look at the IEEE standards regarding measurement, they

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 all talk about establishing a measurement program.
2 And in some of the literature it talks about you have
3 to wait a few years before you really see the results
4 of the measurement program. And they are based on a
5 stable process. So given a stable design process, you
6 are able to characterize, or statistically make
7 characterizations about the product. So one
8 application is that if a licensee implements a
9 measurement program, and implements it correctly, that
10 can give us reassurance, and allow us the possibility
11 to look at a smaller sample of threat audits.

12 I mean, if we're doing a sample of threat
13 audits, those should be statistically characterizable
14 of the system in general. Can we look at a smaller
15 number of audits. Can we rely on the measurements
16 that they use. And that's part of -- to understand
17 how good these measurements are. If they give us --
18 we've both done measurements, but -- and then we look
19 at those measurements, we need to have some assurance,
20 or some confidence that measurement programs and the
21 types of measurements are actually useful in
22 predicting or indicating reliability or quality. It's
23 more difficult to implement a measure on a piece of
24 software that arrives. Defect density is a measure
25 that could be done, in a sense, but what that would

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 require is at least two reviewers to review a product.
2 And that sample product would be representative. And
3 then from that you could calculate how many latent
4 defects there are. You could also characterize the
5 type of defects there are. And you basically get
6 latent defects from defects found by one reviewer and
7 not the others. So that indicates that these defects
8 are not as easily encounterable.

9 And when you talk about quality, there are
10 many dimensions of software quality, and
11 maintainability is one of them. How cohesive are the
12 specifications, how modular are the specifications.
13 The same rules that you apply to source code review
14 can be applied to document review, in terms of
15 cohesiveness, clarity, modularity. So not all the
16 defects identified are -- will impact the proper
17 functioning of the system.

18 MR. ARNDT: The point is we're trying to
19 understand whether or not methods like this are
20 usable. And if you go out and try and use them in a
21 test case --

22 CHAIRMAN APOSTOLAKIS: I am trying too,
23 Steve.

24 MR. ARNDT: Okay.

25 CHAIRMAN APOSTOLAKIS: I really am trying

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

(202) 234-4433

www.nealrgross.com

1 myself. But I seem to be a little more skeptical than
2 you are.

3 MR. ARNDT: Fair enough.

4 CHAIRMAN APOSTOLAKIS: Which is fine.

5 MR. KEMPER: If I could offer one thought
6 too, just to kind of tag onto what Steven just said.
7 You know, we're -- this project is a three-phase
8 project as you're aware, and that we're really trying
9 to assess the viability of these metrics on a complex
10 system using nuclear power plants. Actual deployment
11 of this technology now into inspection criteria is a
12 yet-to-be-determined project. So we'll build onto the
13 results of this to actually figure out how to actually
14 implement this into the regulatory process.

15 CHAIRMAN APOSTOLAKIS: If --

16 MR. KEMPER: If it's useful, yes, exactly.

17 CHAIRMAN APOSTOLAKIS: Well, fine. You
18 know, I have no problem with that.

19 DR. LI: This slide summarizes our
20 preliminary results so far that we obtained. The
21 number of defects predicted from the completed
22 measures.

23 CHAIRMAN APOSTOLAKIS: Which program are
24 you applying this to now?

25 DR. LI: It's a real nuclear software. I

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

1 cannot disclose the name of the software based on the
2 agreement with the vendor.

3 CHAIRMAN APOSTOLAKIS: You found 210
4 highly ranked?

5 DR. LI: I just tried to highlight that
6 number, 210, from cyclomatic complexity. It's not the
7 number of defects remaining. It's the number of
8 defects before the testing. So ongoing research is
9 trying to explore how many defects are remaining.

10 CHAIRMAN APOSTOLAKIS: Okay.

11 DR. LI: And another point is that bugs
12 per line of code. This measure is obsolete. So the
13 value from that measure is not representative.

14 CHAIRMAN APOSTOLAKIS: Which one is
15 obsolete?

16 DR. LI: The bugs per line of code. Bugs
17 per LOC here.

18 CHAIRMAN APOSTOLAKIS: Oh.

19 DR. LI: And I also want to highlight that
20 although the measure cause effect graphing ranked by
21 the experts in low category, but the way we measure,
22 it significantly promotes the ranking of this measure.
23 So that's why we have a very low number of defects
24 predicted from this.

25 MEMBER WHITE: Excuse me. Can you tell me

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

(202) 234-4433

www.nealgross.com

1 why bugs per line of code is irrelevant, or
2 unimportant?

3 DR. LI: Well, this measure was invented
4 in the 1970s, and based on the data from assembly
5 language. So the line of code for the high-level
6 language like C, and from the low language like
7 Assembler, are significantly different. So that's why
8 this measure and this empirical relation between the
9 number of bugs and the line of code.

10 MEMBER WHITE: I understand that argument,
11 but the number 590 is still pretty large.

12 DR. LI: Right.

13 MEMBER WHITE: And so that would cause me,
14 you know, to -- it would cause me some anxiety. So
15 why would we still -- why would we consider that
16 irrelevant? I understand about lines of code, but 590
17 is a big number, right?

18 DR. LI: Right. Well, that's why the
19 experts rank this measure very low. So which
20 indicates that everybody should not take this measure.

21 MEMBER WHITE: You'll help me, won't you.

22 MR. ARNDT: What you've got to realize is
23 one of the purposes of doing a validation study is to
24 try and determine which measures may be useful, and
25 are predictive of what the reality is. So what the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 idea is is to look at some of the low ranked measures,
2 ones that we have less going in confidence that will
3 be useful, to, one, validate that that's true, and,
4 two, also decide that, yes, we don't hold a lot of
5 confidence in that particular measure even though it's
6 out there in the community. And that if a licensee at
7 some point in the future says, well, you guys are
8 interested in metrics, I'll throw this into my
9 application, we can say, well, that's nice, but based
10 on our research it's pretty useless. So the point is
11 that we want to look at a variety of measures to
12 understand not only how easy are they to use, what
13 information do they give you from an understanding of
14 the system, but also whether or not we would add any
15 value to them in a licensing review. So the idea is
16 to look at a number of different issues.

17 What Ming was pointing out is in some
18 cases it depends on how the metric is defined. In
19 this case, it's not well defined anymore based on --
20 because we don't program in Assembler very much
21 anymore. Other cases like cause effect graphing
22 depends on how well the procedure for developing that
23 metric is defined. As Ming mentioned earlier, as part
24 of this research we better defined that procedure, so
25 we now believe it is probably a higher ranked measure

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 because the consistency in developing that measure is
2 higher than it was when we first started looking at
3 it, and ranked it as a low ranked measure.

4 MEMBER WHITE: Okay. Under medium ranked
5 measurements you have, is that capability maturity
6 model?

7 DR. LI: Right.

8 MEMBER WHITE: And the 4.58 is between 4
9 and 5. But that's a medium ranked measure. And the
10 cyclomatic complexity is a high ranked measure? What
11 does the number 210 mean?

12 DR. LI: Well, just as I mentioned, this
13 is not the number of defects remaining. This is the
14 number of defects before testing. So after the
15 testing, the development process will fix most of the
16 defects here. So this is just a preliminary result.
17 And we are working on that, try to theoretically
18 figure out how many defects are remaining.

19 MEMBER WHITE: Okay.

20 MEMBER GUARRO: I'm having some trouble in
21 relating the concept of number of defects to these
22 measures, actually. For example, in cyclomatic
23 complexity, what 210.37 means. Some metric? Because
24 the label says number of defects, and I'm not sure --

25 CHAIRMAN APOSTOLAKIS: It says predicted.

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

(202) 234-4433

www.nealrgross.com

1 MEMBER GUARRO: Well, if I interpret that
2 correctly, in bugs per line of code I'm going to have
3 590 bugs per line of code?

4 CHAIRMAN APOSTOLAKIS: That's crazy.

5 MEMBER GUARRO: That doesn't seem to be
6 the meaning of what you have there.

7 MR. ARNDT: Well, let me do the simple
8 answer, and Ming can elaborate the more complicated.
9 What we're trying to do so we can make a comparison on
10 relative value is we're getting the actual number out
11 of whatever the particular metric is, and then we're
12 using published literature, or correlations, or
13 whatever for each different measure to try and
14 normalize each of the measures to a particular value,
15 like number of defects predicted, or some other
16 normalized value. That's what those numbers are.

17 MEMBER WHITE: Since we have a little
18 time, and since I'm an old country boy, maybe you
19 could help me a little bit more. If I'm from the NRR,
20 and you tell me that this safety-related application,
21 digital system does have a normalized value of
22 whatever it is, let's say it's 210. What does that
23 tell me? How do I use that information? What do I do
24 with it? Does that tell me it's good code, bad code,
25 I ought to be worried about it, I ought to throw it

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 out? I'm sorry if I'm dense, I just don't understand
2 yet.

3 DR. LI: This is not the final result.
4 The final result we will provide the probability of
5 failure per demand. By combining the operational
6 profile and the number of --

7 CHAIRMAN APOSTOLAKIS: Any demand? What
8 do you mean probability of failure per demand? This
9 is conditional probability. Depends on the demand.

10 DR. LI: The system we're studying is an
11 RPS system. So by "demand" we mean it's a per trip.

12 CHAIRMAN APOSTOLAKIS: Well, even so, I
13 mean any combination of variables will give me the
14 probability of failure? Okay, go ahead, then what?
15 Then you will provide that probability which will be
16 what? 0.02, something like that?

17 DR. LI: Well, we don't know the results
18 yet.

19 CHAIRMAN APOSTOLAKIS: But let's say it's
20 0.02. The question from Mr. White is what do you do
21 with that.

22 DR. LI: Well, from the software quality
23 perspective, that value tells us if you run it one
24 hundred times, you will experience two failures.

25 CHAIRMAN APOSTOLAKIS: Yes.

1 DR. LI: That's a statistical indicator.

2 MR. CARTE: We're talking about measures
3 and results that they produce, but we have not
4 established acceptance criteria. That's the point
5 where you establish whether the result produced is
6 acceptable or not.

7 CHAIRMAN APOSTOLAKIS: Well, the other
8 question is of course whether the probability should
9 be 0.02, or you should have some sort of an
10 uncertainty range associated with that.

11 DR. LI: Well, that's in our next step.

12 CHAIRMAN APOSTOLAKIS: I think you're a
13 brave man to claim that you will produce a probability
14 of failure based on these measures. I am very, very
15 skeptical. Anyway, let's keep going. 19 is your
16 future?

17 MR. CARTE: Yes. So the future work in
18 the large-scale validation will in part include the
19 development of -- first we have to determine which
20 methods are acceptable. And from that we can look at
21 what is the acceptance criteria. And there's a couple
22 of ways of developing acceptance criteria. And one is
23 to apply these measures -- which is called
24 benchmarking -- one is to apply the measure in
25 parallel with the current evaluation process, and

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 based on what we currently deem as acceptable, what
2 are the measures of that software. And that gives us
3 a relative estimate of the acceptance criteria that we
4 should look for. So in future when systems come in
5 and their measures are significantly below that, the
6 currently acceptable levels, that should cause some
7 concern.

8 The other aspect of acceptance criteria
9 relates to this calculation of failure per demand,
10 probability of failure per demand. And one reason to
11 pursue a method like that is that it gives you a
12 theoretical way of determining an acceptance criteria.
13 If you can characterize, at least statistically, what
14 you estimate the failure probability to be, then you
15 could apply PRAs and from that get an acceptance
16 criteria. If that works, that is less work than
17 benchmarking, because how long do you have to
18 benchmark a measure before you have confidence in that
19 measure? And so, yes it is a little bit cutting edge
20 to pursue that, but that's part of the motivation for
21 pursuing it.

22 CHAIRMAN APOSTOLAKIS: When you say future
23 work, you mean after Maryland finishes in November?
24 Or future in the next few months?

25 MR. CARTE: Well, both. The first step,

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

(202) 234-4433

www.nealrgross.com

1 because the research isn't done, the research final
2 report will include an evaluation about the
3 acceptability of those measures. And that will be
4 reviewed by us, and our NUREGs are circulated to NRR
5 for review. And so we'll evaluate that. If those
6 methods are deemed to be acceptable by the NRC, then
7 we will need to look at training and the use of those
8 metrics. If they're not acceptable, then that work is
9 in essence done. If we the NRC, and that includes
10 input from NRR, determine that this is still promising
11 and we wish to look at additional measures, we can
12 pursue that as subsequent research. And another area
13 of subsequent research is technology-specific
14 measures. For instance, right now there are three
15 SERs for PLC-based systems, and yet we're not looking
16 at PLC-specific measures. How does lines of code
17 apply to a function block design, for instance?

18 Basically we feel that software
19 engineering measures are sufficiently mature for
20 assessing software quality in safety-related nuclear
21 applications.

22 CHAIRMAN APOSTOLAKIS: I thought the
23 comments from both you and Steve so far pointed to the
24 conclusion that you're really not sure. But now
25 you're definitive. I thought you were still

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 exploring, and now you're saying no, they're
2 sufficiently matured.

3 MR. CARTE: They've matured for performing
4 assessment, yes. Whether we have an absolute
5 acceptance criteria, or how we use those numbers -- a
6 quantitative assessment gives you more granularity in
7 the performance of your review. Also, if you have
8 detailed measurement rules it gives you a more defined
9 process.

10 CHAIRMAN APOSTOLAKIS: I agree with all --
11 these are generic statements. In this particular
12 approach it seems to me you have to really scrutinize,
13 like in any approach, the fundamental assumptions.
14 And the problem with software is that, as someone said
15 this morning, there's usually specification errors,
16 design requirement errors, and so on. And 99.9 if not
17 100 percent of the matters we have here really do not
18 apply. We don't deal with those kinds of errors in
19 standard risk assessments. So we really have to go
20 back to the assumptions, every step of the way. You
21 know, they say this, I can say something about the
22 remaining faults. No. For me, that's a major claim.
23 It requires major arguments. I don't see them. So I
24 must say at this point I disagree with the first
25 bullet. That doesn't mean you shouldn't agree with

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 it. I mean, in the future sometime we have to resolve
2 this. I'm awfully skeptical about all this. I really
3 don't think it gives you anything. There you are.
4 But then again, I may be wrong. Right? We'll find my
5 P and my E integrate. So, the last bullet says what
6 now, Norbert?

7 MR. CARTE: Measures of software quality
8 are related to proper system operation. And this
9 large-scale validation project provides a promising
10 methodology for estimating the impact of software
11 quality on proper system operation.

12 CHAIRMAN APOSTOLAKIS: Okay. Is your
13 presentation over? Any questions? Comments?

14 MEMBER WHITE: I have a question. This
15 candidate system that you're evaluating in your
16 project, what was the requirement for reliability?
17 Was it like one failure in 10^{-6} , or 1 in 10^{-4} , 10^{-2} ?

18 DR. LI: These were not mentioned
19 explicitly in the requirements.

20 MEMBER WHITE: Okay. Well, the point is
21 what you're using in your project is a highly -- is
22 supposed to be a highly reliable system, right? But
23 you can't characterize exactly what that is right now.
24 But it's like -- it's better than 1 in 100? One in
25 1,000?

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. ARNDT: Although, to my understanding,
2 and I could be wrong, but to my understanding the
3 actual line criteria was not specified when it was
4 originally designed. If you go back to the standards
5 that it does reference in its design work, you can
6 infer based on some other standards 10^{-4} , 10^{-5}
7 ballpark.

8 MEMBER WHITE: Thank you.

9 MEMBER GUARRO: Can you go back to Slide
10 15 so we can write in the formulas?

11 CHAIRMAN APOSTOLAKIS: What? Oh I think
12 Eric is doing that. Sergio? He's going to do it.
13 Okay, any more comments or questions? There is a
14 question here.

15 MEMBER BONACA: I was missing the first
16 half an hour. I had a meeting here. But I just, on
17 reviewing this report here on preliminary validation
18 as a NUREG. I was intrigued by, again, you had the
19 Table 1 on Page 7 where you identify 40 or 30-odd
20 measures. And you pick up two high ranking class, two
21 medium, two low. You work with those. It draws out
22 the conclusion, and then you seem to be able to apply
23 those conclusions to the whole set.

24 MR. CARTE: We get some indication of the
25 validity of the ranking. In other words, for those

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

(202) 234-4433

www.nealrgross.com

1 measures that are low ranked, do they perform low
2 ranked for those that are medium ranks.

3 MEMBER BONACA: That was a specific
4 purpose.

5 MR. CARTE: Yes.

6 MEMBER BONACA: In fact you had some
7 changes in rank that resulted from the evaluation.

8 MR. CARTE: Yes.

9 MEMBER BONACA: Okay. Okay.

10 CHAIRMAN APOSTOLAKIS: Okay. Anything
11 else?

12 MR. WATERMAN: Mike Waterman, Research.
13 Just from an NRR perspective, can't get that out of my
14 blood, I guess. On Slide 18 where you showed the
15 preliminary results, and you've got number of defects
16 predicted. Have you considered building a system
17 where you actually knew how many defects were in the
18 system so that you could check out and see just how
19 well these particular metrics, for example, were
20 predicting defects when you already knew the answer?
21 I don't see a benchmark -- I don't know if there were
22 actually 4.58 defects remaining in the system, or if
23 there are 200 by looking at this chart. All I see is
24 the numbers, and you don't have anything to weigh
25 those numbers against, you know, what is really in the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 system. And I think that would be very helpful, you
2 know. Because right now none of those numbers mean
3 anything to me other than if I was using bugs per line
4 of code, and I was an NRR reviewer, I'd get pretty
5 excited pretty quick. And I'd know that I'd have to
6 extend an audit by several weeks just to chew into
7 that. So right now I'm, just from my experience as a
8 reviewer, those numbers there sort of disturb me
9 unless I know how many defects are there really
10 remaining. Then I could say, oh yes, cyclomatic
11 complexity, how ridiculous. And look, CMM does a
12 pretty good job. You know, I don't know that by
13 looking at that. So it would seem to me somewhere
14 down Research's road there would be a benchmark model
15 where you know all the answers. You apply these
16 things to that benchmark model, and see how well it
17 does in finding the right answer. I don't know if
18 that's in the research or not. That's Norbert's
19 research project.

20 DR. LI: Right, this is absolutely
21 correct. We will do a reliability testing later. And
22 based on that reliability testing, we will know how
23 many defects are really remaining in the system.

24 MR. WATERMAN: But it seems to me you'd
25 have to find every defect so that you could see how

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

(202) 234-4433

www.nealrgross.com

1 well you come out on predicting number of defects,
2 right?

3 DR. LI: Right.

4 MR. WATERMAN: And then I don't know how
5 reliability relates to defects if you have a defect
6 that doesn't affect reliability.

7 MR. ARNDT: Right. Well, that's the
8 difference between a failure and a defect.

9 MR. WATERMAN: Yes.

10 MR. ARNDT: If you look at the slide
11 before the one that's right up there, if you go up,
12 17. You look at the analysis and progress. Part of
13 the effort is to do some testing to get -- for the
14 system under consideration to get a failure on demand
15 estimate to validate the predictions that the metrics
16 will provide you.

17 MR. WATERMAN: Well, could we use --

18 MR. ARNDT: -- a rough evaluation of
19 whether or not the predictions are reasonable, and
20 which metrics are most closely tied to the test base
21 prediction.

22 MR. WATERMAN: Well, Roman Shaffer from my
23 section made a suggestion I thought was pretty
24 ingenuous, was to take our fault injection tool that
25 we've got, and apply it to your benchmark model, and

1 let the fault injection shake the daylights out of it,
2 if you will, and see how many bugs fall out, and then
3 use that as a benchmark against all of these things.

4 CHAIRMAN APOSTOLAKIS: Could be.

5 DR. LI: Yes, that's possible.

6 MR. ARNDT: There's a number of different
7 methodologies for trying to get a reasonable
8 prediction based on a different methodology to support
9 which metrics are the most accurate.

10 MR. WATERMAN: And I guess finally, as a
11 reviewer of a system, having a large number of metrics
12 would probably really assist me because they would
13 point me in directions that I needed to go when I
14 actually reviewed the product manually, instead of
15 just relying on just these numbers. I would hope that
16 the reviewers who were remaining in NRR would use
17 those numbers to tunnel down in to very certain
18 aspects of a particular product and see why that
19 particular aspect isn't coming out so great. So you
20 know, so I look at this research as kind of helpful in
21 that way. That's all.

22 CHAIRMAN APOSTOLAKIS: Thank you very
23 much, gentlemen.

24 MR. ARNDT: Thank you.

25 CHAIRMAN APOSTOLAKIS: And we'll recess

1 until 2:45.

2 (Whereupon, the foregoing matter went off
3 the record at 2:18 p.m. and went back on the record at
4 2:45 p.m.).

5 CHAIRMAN APOSTOLAKIS: Back in session.
6 Mr. Arndt?

7 MR. ARNDT: Yes, sir.

8 CHAIRMAN APOSTOLAKIS: The floor is yours.

9 MR. ARNDT: Okay. We're going to talk now
10 a little bit about the project that is identified
11 under Section 3.2.2 in the Research Program Plan.
12 This is the digital system dependability. Myself, who
13 you all know, and Mr. Shaffer will give this
14 presentation. I'll just do the brief introduction,
15 and then Roman will do the meat of the presentation.
16 I will of course be available for questions.

17 As we talked about this early afternoon,
18 this is part of the software quality assurance
19 program. And this part of the overall program is
20 designed to look at different testing aspects to
21 understand digital system dependability in a more
22 detailed fashion. Next slide, please.

23 As we talked about this morning, the
24 current state-of-the-art for these various digital
25 systems includes a very promising methodology referred

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

(202) 234-4433

www.nealrgross.com

1 to as fault injection testing that permits the system
2 to be reviewed at a fairly deep level. Once you
3 obtain the information, or a better understanding of
4 how the system works, that could then support modeling
5 methodologies in a number of different ways. And it
6 doesn't really matter which modeling methodology you
7 use to embed the information you learn about the
8 system. The idea here is to characterize the behavior
9 of the system using this particular methodology. In
10 this case, although fault injection has been
11 historically looked at in the software area, there's
12 also been work in the hardware area, in the total
13 digital system area for integrated hardware/software
14 interactions. People have done it in the simulation-
15 based arena as well. So there's a number of different
16 ways you can do this. We're going to look at it in a
17 particular way to try and develop a better
18 understanding of the system. So the idea here is to
19 develop an understanding of the various aspects of how
20 the system can fail, and information we can gain out
21 of these kinds of techniques.

22 Roman is going to give you some more
23 details of what the specific goals are for this
24 project. This project basically is an out-cropping of
25 information we gained under a cooperative agreement

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 with the University of Virginia and other research
2 programs. We now want to take that information that
3 we gained and use it to develop specific applications.

4 MR. SHAFFER: Thanks. Good afternoon. I
5 am Roman Shaffer, and I thank you for the opportunity
6 to present our research plans on digital system
7 dependability. I will be doing most of the talking,
8 but Steven, as he said, will be available to take
9 questions. Can you hear me? I'm going to talk about
10 the goals of this research, how we hope to support and
11 augment the current process; the motivation for
12 performing the work, what led us to do the digital
13 system dependability work in this way; some
14 fundamental concepts and applicability to the
15 regulatory assessment process. Probably the first few
16 slides will be basic for some of you, but I'll go
17 through them anyway to give you some background of why
18 we're doing this the way we're doing it. An overview
19 of the selected methodology, which is a process
20 involving fault injection experiments, a brief
21 discussion on specific projects that we have planned,
22 and I say here conclusion, but that should be a
23 summary.

24 The function of the Office of Research is
25 to provide technical assistance to the various user

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

(202) 234-4433

www.nealrgross.com

1 offices, such as NRR and NMSS to meet their respective
2 missions, whether licensing actions, rulemaking,
3 etcetera. We can do this in a number of ways, one of
4 which is to supplement their staff by doing licensing
5 reviews. Examples of this, we are performing some gas
6 centrifuge license application reviews. Another
7 example is we are reviewing the regulations and
8 providing them recommendations on certain decisions
9 they need to make. Another way RES supports the user
10 offices is through our research products.

11 For the dependability research in
12 particular, the overarching goal is to continue to
13 support acceptability decision-making regarding
14 digital safety systems. This means the effort will
15 supplement and augment the current process by defining
16 objective acceptance criteria from digital technology
17 from a system perspective -- and there'll be more on
18 this later -- and applying modeling tools and analysis
19 methods that will be generically applicable to the
20 systems that we're interested in. And this is
21 important as we move towards a performance-based
22 regulatory framework.

23 Given the complexity of digital systems,
24 we need to understand the behavior of these systems
25 under the influence of internal and external faults so

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

(202) 234-4433

www.nealgross.com

1 that we can analyze any consequent errors that might
2 produce system failures. So if we look at the
3 sequence that the system is operating, a fault occurs,
4 that affects the information flow within the system,
5 and after further processing, if there is an external
6 adverse impact on the system that is observable we
7 call that a failure. So it's failures, errors -- I'm
8 sorry, faults, errors, failures. When we understand
9 their behavior, we can characterize it and analyze
10 digital systems for performance such as timing
11 requirements, jitter, confirm that it does what it's
12 supposed to do upon demand. For reliability and
13 availability, for their failure modes, do we account
14 for all modes, and subsystem and system safety,
15 because interconnecting safe subsystems does not
16 guarantee a safe system.

17 Another aspect of this research is to
18 investigate if the data from this research, such as on
19 failure modes and likelihoods, will be applicable to
20 the probabilistic risk assessments. But this is tied
21 more to Steven's discussion tomorrow.

22 Next I will discuss our motivation for
23 undertaking this effort, such as why we need to
24 improve our understanding of newer technologies, and
25 also sources of faults. I'll also go over some simple

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 illustrations of these systems. Previous research by
2 experts in the software and hardware fields, as well
3 as examples of catastrophic digital system failures
4 indicate that software can have severe defects, even
5 after V&V. There's some work by Capers Jones who
6 correlated the number of critical and significant
7 errors to the number of lines of code. Some other
8 examples are the Ariane V rocket failure, the Therac-
9 25 deaths, the work by Koopman and Siewiorek
10 investigating various operating systems, and the most
11 recent example is the August 14 blackout. I believe
12 I read something that there was a defect deep in the
13 code that was involved with that.

14 There's also a greater reliance on
15 software to perform critical functions. As you see
16 what's being proposed to the NRC, this is quite
17 apparent. These systems are reliant on software in
18 safety-critical functions. There's also digital
19 hardware components, which can have design and random
20 defects. Some work by Avizienis and Huh studied a
21 COTS processor and found approximately 70 defects. I
22 think is a well known example, but I call upon it here
23 because it ties into the work, ties into our
24 motivation for performing this work.

25 Because the interaction of hardware and

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 software can lead to a new class of defects, we need
2 to understand how often such defects are triggered, or
3 how often these faults occur, and how critical they
4 are. Do they cause death, damage to the system, or
5 are they just an annoyance? And, given the complexity
6 of the systems, and the significant interfacing
7 external and within the system, what practical methods
8 are available to determine their risk, in our case to
9 nuclear safety? We want methods that are feasible to
10 perform, and that can be used in our regulatory
11 process. We don't want to take upon techniques or
12 methods that are not timely. We'll get more into this
13 later.

14 The figure represents a digital system
15 composed of hardware and software, and various sorts
16 of faults at different phases of the system's life.
17 The yellow stripe outer boundary represents those
18 development processes, design features, and operating
19 procedures meant to prevent faults and errors from
20 occurring. The red stripe boundary on the lower side
21 represents those design features to handle faults and
22 errors when they occur. In the development phase,
23 there are requirements and specification mistakes,
24 such as incomplete specifications. Also in this phase
25 are mistakes in implementing the specifications. In

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 the operational phase there are operator mistakes,
2 including those related to human-system interfaces,
3 human-machine interfaces, external disturbances, such
4 as from electromagnetic radiation, humidity,
5 temperature, etcetera, and component defects, random
6 failures. Internal to the system are also hardware
7 and software faults. Now, this doesn't mean we're
8 going to be treating hardware and software as separate
9 components. This is just an illustration of the
10 sources of faults.

11 This figure may offer a better
12 illustration of the fault error failure sequence
13 discussed in the earlier slide. Under certain
14 conditions, any of these mistakes, disturbances,
15 and/or component defects could defeat the protection
16 mechanisms in the development and operational phases
17 of the system's life to cause faults. For example, in
18 the hardware/software interactions. This could
19 potentially affect the information flow within the
20 system, which is called an error. If after further
21 operation there is an observable effect on the system,
22 then that is a failure. The system is said to have
23 failed, perhaps due to improper error handling, or
24 occurrence of another fault.

25 An important aspect of assuring safety of

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

(202) 234-4433

www.nealgross.com

1 digital safety systems is determining the criticality
2 and associated frequency of occurrence of faults in
3 the hardware/software interactions. In the digital
4 system dependability work, we will take a system point
5 of view. Because software must execute on hardware,
6 it is critical to understand the integrated
7 hardware/software system, and whether or not any
8 failures in that system lead to unsafe conditions.
9 This is not an easy task, however, as we all know.

10 The system functions for fault detection
11 and handling can be quite complex, and perhaps even
12 the majority of system software could be devoted to
13 fault and error handling. The methodology we have
14 selected for the digital system dependability research
15 can be used to exercise these functions. We can
16 therefore analyze various classes of faults for the
17 potential to cause unsafe conditions. The results of
18 the research, including the data generated, could
19 potentially be used to augment and supplement the
20 current regulatory process as far as acceptability
21 decision-making, and that is through the development
22 of an objective acceptance criteria.

23 An overview of this methodology is the
24 subject of later slides in the presentation.

25 CHAIRMAN APOSTOLAKIS: Go back please, to

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

1 your slide. What do you mean by "such software may
2 not be exercised sufficiently." The last sentence
3 there.

4 MR. SHAFFER: That means during their
5 testing they may not test all of the diagnostic
6 functions. They may concentrate on the safety-
7 critical functions and not necessarily make sure that
8 the fault diagnostics perform.

9 CHAIRMAN APOSTOLAKIS: And this is due to
10 what? The fact that these are complex?

11 MR. SHAFFER: Could be. Could be that
12 they're complex. Could be deadlines in the project
13 scope, any number of things.

14 CHAIRMAN APOSTOLAKIS: Yes, but why does
15 this apply to your last bullet only? That's what I'm
16 trying to understand. You say you have much of the
17 software is designed to handle fault detection, fault
18 location.

19 MR. SHAFFER: Well, that's only --

20 CHAIRMAN APOSTOLAKIS: That applies to
21 everything, right?

22 MR. SHAFFER: Yes, it does. This is just,
23 we're talking -- we're concentrating on the fault
24 detection, location, isolation, and recovery functions
25 because the safety systems that we've approved and

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 we'll see in the future will have these functions
2 built in. So not only will they concentrate on the
3 normal safety-related functions, we'll be looking at
4 the fault isolation.

5 CHAIRMAN APOSTOLAKIS: Also, if you will
6 go on before this.

7 MR. SHAFFER: Sure.

8 CHAIRMAN APOSTOLAKIS: You may have
9 implementation errors that you will never see until
10 you have the right external input, right?

11 MR. SHAFFER: That's correct.

12 CHAIRMAN APOSTOLAKIS: So these are not
13 just inputs. I mean, this is just a notional diagram,
14 I guess.

15 MR. SHAFFER: That's correct, I believe I
16 stated that.

17 CHAIRMAN APOSTOLAKIS: You may not --

18 MR. SHAFFER: That's right. It's just
19 illustrative. It's not supposed to get all possible -
20 - implementation mistakes are sources of errors.

21 CHAIRMAN APOSTOLAKIS: And now you see
22 again my favorite subject, failure rates, and the
23 rates, and all that. I don't think the stuff on the
24 left has anything to do with rates. The stuff on the
25 right does. The external disturbances, for example,

1 you might say have a rate of occurrence. And this is
2 the kind of thing that I keep coming back to, that
3 before we use Markov, or whoever, any other Russian
4 name, you have to ask yourself what does this
5 quantitator present? Does it model all the stuff
6 that's useful? Requirements and specification
7 mistakes cannot be modeled. External disturbances
8 probably can. So that's what I mean by going to the
9 assumptions, rather than taking the model -- component
10 defects, I don't know. May or may not. I don't know
11 exactly what you mean. Operator mistakes could be,
12 could be.

13 So this is really the essence of it,
14 precisely because what you have on the left there is
15 so important for software. You see, for hardware, we
16 don't really pay much attention to it. We have all
17 sorts of testing and all that. But for software, this
18 is the heart of the matter.

19 MR. ARNDT: We'll talk tomorrow in greater
20 detail about what kinds of modeling we've looked at as
21 possible ways of doing this. Although this project,
22 you need to use some kind of models to work with, but
23 the primary emphasis of this project is the
24 understanding of the system, not necessarily what you
25 do with that information in terms of what model you

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 use.

2 CHAIRMAN APOSTOLAKIS: No, but all I'm
3 saying is that this is a good picture --

4 MR. ARNDT: Right.

5 CHAIRMAN APOSTOLAKIS: -- to put in
6 context my earlier comments about Markov, and the
7 rates of occurrence, and all that.

8 MR. ARNDT: Okay.

9 CHAIRMAN APOSTOLAKIS: You have strong
10 motivation here, Roman. Several slides. You are a
11 motivated guy.

12 (Laughter)

13 CHAIRMAN APOSTOLAKIS: That's good,
14 though. That really -- that's nice to see that.

15 MR. SHAFFER: In a previous slide I
16 mentioned that digital system faults could be
17 triggered at system interfaces. This figure is a
18 simple representation of a digital system where we can
19 see various interfaces, both internal and external.
20 We have interfaces at the inputs and outputs from and
21 to the physical plant and humans, the human operators,
22 which again, these include the operating environment
23 and the HMI system.

24 CHAIRMAN APOSTOLAKIS: See, this is now
25 where my comment this morning becomes more relevant.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 When I asked what is the level of complexity of
2 software being used in nuclear facilities, or in
3 general our digital I&C. Do we really have
4 controllers in the safety systems? And if we don't,
5 why should I worry about this?

6 MR. SHAFFER: This is just an illustrative
7 example of the systems we want to test. I could just
8 as easily have put safety system. The safety systems
9 take an action.

10 CHAIRMAN APOSTOLAKIS: My point is all
11 this input, output, humans, and so on, the control
12 actuators, and all that, if I don't have any systems
13 like that safety systems in the nuclear plant right
14 now, and as given also what was said this morning
15 that, you know, resources are limited, why should I
16 worry about this at all?

17 MR. SHAFFER: Because we do have systems
18 like this.

19 CHAIRMAN APOSTOLAKIS: Safety systems?

20 MR. SHAFFER: Sure we do. You have the
21 maintenance technicians, you have the operators at the
22 control panels who are going to take action based on
23 what these certain indications are. You're going to
24 have actions --

25 CHAIRMAN APOSTOLAKIS: Digital?

1 MR. SHAFFER: Yes. We have safety systems
2 in newer technologies that have gone in under 50.59.
3 Teleperm, Common Q, and Tricon. I'm not sure Tricon's
4 is a safety system, but they're out there.

5 MR. WATERMAN: This is Mike Waterman.
6 Yes, several plants have put in digital load
7 sequencers as part of their emergency load sequencing.
8 I know of one plant, I believe it's the Oconee units
9 have a digital aux feedwater system. I think that's
10 a safety system also. And right now the systems are
11 kind of individual modular type systems that handle
12 one function or another, but yes, those digital
13 systems are out there, and the progressive licensees
14 are gearing up right now to start retrofitting.

15 CHAIRMAN APOSTOLAKIS: I raise this issue
16 because if you look at the general -- and maybe it
17 doesn't apply, but if you look at the general
18 literature out there, those guys, you know, they look
19 at major pieces of software, like the one that
20 controlled the Ariane rocket and so on, and they draw
21 some conclusions and so on. And I remember I visited
22 one of them, I was at one of the meetings of the
23 National Academy, the group that was preparing the
24 National Academy report. And it was very contentious.
25 And the main theme that one of the participants kept

1 coming back to was 'But this doesn't apply to nuclear
2 systems. We have very simple systems. We have very
3 simple systems. You can't take a lesson learned from
4 Ariane and say, well, this applies to the auxiliary
5 feedwater system.' That's what I'm trying to do. I
6 mean, are we taking into account the level of
7 complexity of our digital software in our plants right
8 now? We are not trying to solve, you know, the
9 EuroSpace problems, or NASA's problems for that
10 matter.

11 MR. KEMPER: But what we're trying to do
12 is prepare ourselves for what's coming. Okay? You're
13 right, what's installed in the plant right now is just
14 a smattering of what's going to be installed in terms
15 of digital technology in 10 years. So there's a bow
16 wave, in my humble opinion, there's a bow wave heading
17 towards the agency of digital upgrades that are bound
18 to happen because of the obsolescence of analog
19 systems. So this research will position us as a
20 regulator to do the research that we feel is needed to
21 estimate the dependability of these systems.

22 CHAIRMAN APOSTOLAKIS: This morning the
23 issue of prioritizing the various items you have in
24 your plan came up. Maybe if you decide to come up
25 with some prioritization scheme in the near future,

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 this could be one of the considerations. What to do
2 first, and what to do second. Because right now the
3 plan does not prioritize, but I'm pretty sure you will
4 have to do some prioritization at some point. And a
5 number of criteria, of course.

6 MR. KEMPER: But there are priorities and
7 a schedule timeframe, but as I say, that was developed
8 without full buy-in of our customers, our
9 stakeholders. And this is considered a pretty high
10 priority project.

11 CHAIRMAN APOSTOLAKIS: It is.

12 MR. KEMPER: Right.

13 CHAIRMAN APOSTOLAKIS: Interesting.

14 MR. SHAFFER: There's also interfaces as
15 the information flows through the embedded controller
16 -- in this case it could be a safety system -- which
17 is represented by the dotted line, the outer dashed
18 line. The process variables acquired by sensors is
19 conditioned by analog hardware, converted to digital
20 values, and then processed by calculation and/or
21 decision logic, which could be hardware and/or
22 software. The flow of information continues whereby
23 the digital values are converted to analog signals to
24 actuate a change in the process variable being
25 controlled. It is interesting to note that the

1 sensors and actuators themselves can and do have
2 embedded controllers, such as smart sensors and
3 digital valve actuators.

4 The functions shown inside the dotted line
5 can take various hardware forms, from single
6 integrated circuits called systems on a chip, which
7 could be field-programmable gate arrays, and/or
8 application-specific integrated circuits, to
9 individual cards containing processors communicating
10 over backlink, to widely dispersed sensors and
11 actuators communicating over field buses or through
12 the air via radio waves connected by network bridges,
13 routers, or gateways over an Ethernet connection to a
14 central controller. In our focus on safety systems,
15 we don't have any widely dispersed safety systems.
16 But again, this is an illustrative example of all the
17 interfaces within these digital systems.

18 When we consider the role of software and
19 its significant interaction with hardware, then the
20 challenge of finding practical methods of assessing
21 the safety and potential risk of these systems is
22 apparent. From the earlier slide on the fault failure
23 error sequence, it is possible again to get a better
24 feeling of how fault at various points to of the
25 system could potentially affect the information flow.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 Again, an error. If the information flow has an
2 observable effect external to the dashed line on the
3 figure outside the embedded controller, then that is
4 a failure. That failure then could have adverse
5 consequences for humans or the physical plant being
6 controlled.

7 I will now review some concepts and
8 challenges of the digital system dependability effort.
9 This figure is used to graphically illustrate the
10 hierarchical approach to digital system design,
11 including tolerance systems. Its purpose here is to
12 further illustrate the complexity of these systems,
13 and the level of effort required to analyze them. On
14 the left side are the various layers of design and
15 protection for the physical system and its components.
16 As we move up the layers, our fraction increases.
17 That means the lower layers represent physical
18 components, such as electronics, circuits, or PN
19 junctions, where first principles are applied. The
20 highest layer is where system architecture is
21 represented, such as modularity and so on, and is
22 derived from the system specifications. The right
23 side is the hierarchy of modeling methods and tools.
24 Accurate modeling at higher layers could require
25 iterating with models from the next lower level to

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 identify and estimate critical parameters. These
2 models can be very complex, from millions of
3 transistors at the circuit level to hundreds of states
4 at the architectural level. The figure on the left
5 side identifies possible sources of faults. Physical
6 faults could be introduced at the lowest layer, which
7 could then be inherited by subsequently higher levels
8 if coverage requirements are either not met or not
9 properly specified. Also note that new faults could
10 be introduced at each layer, which could also be
11 passed upwards. Those faults that defeat all layers
12 of protection are failures.

13 One significant challenge is to determine
14 the level of abstraction necessary to adequately model
15 the hardware/software system. Though we have tools
16 for each layer available to us, our intention is to go
17 to the lower layers only as a necessity, because of
18 the unique and proprietary knowledge and level of
19 effort required to analyze at those lower levels.

20 CHAIRMAN APOSTOLAKIS: How is this
21 motivation only for 3.2.2? Isn't this for everything
22 we do in this area? This nice picture?

23 MR. SHAFFER: It's just laying the
24 groundwork.

25 CHAIRMAN APOSTOLAKIS: It's not -- yes,

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

1 but for everything, not just for 3.2.2.

2 MR. SHAFFER: Yes, the point is that these
3 systems are complex, and this was a process actually
4 applied earlier in this work. Another illustrative
5 example of the difficulty of building safe systems and
6 analyzing them. That's all.

7 CHAIRMAN APOSTOLAKIS: Another point that
8 would be of interest here is what does the present
9 regulatory approach, how does it fit into this?

10 MR. SHAFFER: How does it fit into this?

11 CHAIRMAN APOSTOLAKIS: Yes.

12 MR. SHAFFER: In our current approach?

13 CHAIRMAN APOSTOLAKIS: Yes.

14 MR. SHAFFER: Well, as you've heard
15 earlier, we focus mostly on the software development
16 lifecycle, but then there's also --

17 CHAIRMAN APOSTOLAKIS: So what is that?
18 I mean, we're covering all these architectural level,
19 algorithmic level, functional level. I mean, we do
20 that?

21 MR. SHAFFER: No.

22 CHAIRMAN APOSTOLAKIS: No. Yes? Yes or
23 no? You said yes? You want to come to the
24 microphone? Identify yourself, please.

25 MR. CHIRAMAL: I'm Matt Chiramal from NRR,

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

1 and this is -- we look at every level of this. But
2 maybe talk to the BT that he's talking about, but we
3 look at all the levels, architecture, algorithmic,
4 functional, logic, circuit level. These are parts of
5 the review.

6 CHAIRMAN APOSTOLAKIS: On the left, you
7 mean? Every level on the left? Although the right is
8 really modeling.

9 MR. CHIRAMAL: On the right is when they
10 start designing it completely. At this point, the SER
11 is on the platforms.

12 CHAIRMAN APOSTOLAKIS: Okay, thanks.
13 Let's go on.

14 MR. SHAFFER: For safe operation, a
15 digital system must have the capability to detect a
16 large percentage of faults. When a fault is detected,
17 the system will perform appropriate action to prevent
18 transition to an unsafe state or condition. In the
19 dependability community, the parameter for measuring
20 how well a system prevents unsafe conditions after
21 detecting a fault is fault coverage, or simply
22 coverage.

23 Coverage is defined as a conditional
24 probability that the system correctly handles a fault,
25 given that a fault occurs. Note that there are --

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: That's not the same
2 way Mr. Li defined it earlier, is it?

3 MR. SHAFFER: These are different
4 projects, different methods, different areas of focus.

5 CHAIRMAN APOSTOLAKIS: Different
6 terminologies.

7 MR. SHAFFER: He's talking about test
8 coverage. We're talking about coverage from the fault
9 tolerant dependability community.

10 CHAIRMAN APOSTOLAKIS: But his test
11 coverage was not a condition of probability, was it?

12 MR. SHAFFER: You'll have to talk to him
13 about that. It's not my project.

14 CHAIRMAN APOSTOLAKIS: No, it's not.

15 MR. ARNDT: The effort he was talking
16 about was a software testing concept of how much of a
17 particular set of code was covered during a particular
18 kind of testing. This is a different concept which
19 just happens to use the same -- similar terminology.

20 CHAIRMAN APOSTOLAKIS: So C_p is the
21 conditional probability that a fault exists and we
22 don't detect it?

23 MR. SHAFFER: That's correct. Now, C_p is
24 the probability given that there's a fault that your
25 fault detection functions detect it. Given that there

1 is a fault, it's the probability that the fault
2 detection circuit will detect that fault. A failure
3 would be $1-C_D$, and that would be a coverage failure.

4 Note that there are different types of
5 coverage. For simplicity, the term "coverage" will be
6 used to reference a system's coverage requirements.
7 Coverage requirements are application-specific. A
8 failsafe system would require high fault detection
9 coverage in order to shut down to a safe state,
10 whereas a highly reliable system would require fault
11 recovery mechanisms to restore the system to a known
12 good state after detecting a fault. Note recovery
13 requires fault detection, fault location, fault
14 isolation, and fault recovery. Coverage is an
15 important concept, but it is a difficult parameter to
16 estimate.

17 CHAIRMAN APOSTOLAKIS: I don't understand
18 the probability C_I . Why is there a probability that
19 the fault would be isolated? Can you give me an
20 example?

21 MR. SHAFFER: Again, it has to do with the
22 function in the software code or the hardware.

23 CHAIRMAN APOSTOLAKIS: If I know where the
24 fault is, and say I know the redundancy of the system,
25 shouldn't I know with certainty whether this is

1 isolated or not? Why do I have a probability that it
2 will be isolated?

3 MR. SHAFFER: Because it may not perform
4 its function all the time. I mean, there's --

5 CHAIRMAN APOSTOLAKIS: I don't understand
6 why that would be the case.

7 MR. SHAFFER: Why it would be the case?
8 Because circuits fail, hardware fails. There's just
9 certain failures in a system where the fault isolation
10 circuit may not work.

11 MR. ARNDT: Take for example if you have
12 a fault tolerant system, either software fault
13 tolerant or hardware fault tolerant, that compares the
14 output of a sub-routine, or compares the output of a
15 processor. If for some reason the system has a fault
16 that affects both of those, then you're not isolating
17 the fault. There's some probability that --

18 CHAIRMAN APOSTOLAKIS: You are really
19 unlucky, in other words. Not only is there a fault --

20 MR. ARNDT: Well, that depends on our
21 architecture.

22 CHAIRMAN APOSTOLAKIS: -- what you have
23 built into the system to protect you against it also
24 fails.

25 MR. ARNDT: Right.

1 CHAIRMAN APOSTOLAKIS: And then fault
2 recovery would be the conditional probability that all
3 these terrible things have happened, but still I
4 recover somehow?

5 MR. SHAFFER: And your system handles the
6 fault correctly, in this case yes. That it recovers
7 correctly. If any of those fail, then it's considered
8 a coverage failure, and you end up in an unsafe
9 condition.

10 CHAIRMAN APOSTOLAKIS: I guess you're
11 going to give us some examples of this.

12 MR. SHAFFER: Okay. Watchdog timer
13 detects a fault, resets the system, it's a fault
14 recovery mechanism. For fault recovery you can go to
15 your checkpoints when you detect a fault. To recover
16 from that, you can either go back in time to a known
17 good state, or you could go forward to repair the
18 system and find -- starting out in an error state, you
19 eventually transition to a good state, a normal
20 operations state. Interrupt service routine. That
21 can be considered a forward recovery mechanism in
22 software.

23 CHAIRMAN APOSTOLAKIS: Anyway, keep going.

24 MR. SHAFFER: A number of researchers have
25 developed methods to assess the reliability of digital

1 systems, Jeff Voas, Jacob Abraham, Kang Shin, Ravi
2 Iyer, Koopman and Siewiorek, Barry Johnson, and Jay
3 Lala among others. Two current issues for the NRC
4 regarding digital safety-related systems are
5 understanding the behavior of digital safety systems,
6 and understanding the risk of digital safety systems.
7 This project is focused on the former, with the hope
8 to provide relevant data for the latter under a
9 different project, which Steven will discuss maybe
10 during this presentation, if you have questions, or
11 tomorrow.

12 The digital system dependability research
13 will undertake several case studies to attempt to
14 estimate the coverage of qualified digital systems.
15 These systems all have built-in diagnostics. Because
16 these systems were designed to different requirements,
17 not only will the research give us more insight into
18 the safety of the systems, but also the research will
19 allow us to apply the method to diverse platforms for
20 different reactor applications. The objective is to
21 determine if their built-in fault tolerant protection
22 mechanisms function as expected, or fail under certain
23 conditions, and if they do fail, what are the
24 consequences. We want to determine the criticality of
25 the failures.

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 Longer term we want to know if the
2 selected methodology provides credible results, for
3 example, under a peer review. That's an important
4 component of this research. We need to bring in
5 experts from diverse fields and have them review our
6 work. And is it practicable, that is the method has
7 measurable benefits to the current regulatory process
8 for the level of effort it requires.

9 The presentation will now turn to an
10 overview of the selected methodology shown in the
11 figure. More detailed information is available in
12 technical reports generated during a cooperative
13 agreement with the University of Virginia. There is
14 a report associated with each of those blocks. The
15 research will build upon the UVA effort by applying
16 the process to digital safety systems. These projects
17 will be discussed in more detail later. UVA
18 originally developed this method for designing safety-
19 critical systems as they have been involved in about
20 20 different system design projects. They've actually
21 built fault tolerant systems with this methodology.
22 NRC intends to apply the process to assessing several
23 safety-critical systems as case studies. The process
24 is based on an effective technique for characterizing
25 system behavior under faulty conditions called fault

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 injection. By injecting corrupted signals either onto
2 hardware pins or into software instruction sequences,
3 it is possible to determine how the system will react.
4 The fault injection experiments will be used to
5 estimate critical model parameters necessary for
6 solving the derived analytical model, which is the
7 first block there.

8 The process starts with determining
9 reliability and/or safety requirements, and confidence
10 levels, and deriving an analytical model, perhaps
11 using Markov models, Petri nets, or even fault trees.
12 Because this is a quantitative approach, system
13 information generated from certain qualitative
14 analyses, such as design reviews, hazards analyses,
15 etcetera, will be used when developing the analytical
16 model. The statistical models for estimating the
17 critical model parameters, in our case coverage, using
18 input from the fault injection experiments. The
19 statistical model determines the number of fault
20 injection experiments required to meet the confidence
21 intervals. The remainder of the process essentially
22 determines the types of faults to inject based on
23 expected operational profiles in order to measure
24 internal operating parameters of the system for later
25 analysis.

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

(202) 234-4433

www.nealrgross.com

1 There are several issues we need to
2 address before this technique can be practically
3 applied to the NRC's process. For example, the fault
4 space of the system could be extremely large, thus
5 requiring a large number of fault injection
6 experiments to obtain a statistically significant set,
7 which could be impractical given the length of time
8 required for each test.

9 CHAIRMAN APOSTOLAKIS: It's not just the
10 faults. It's also the external inputs. You inject
11 the fault, then you have a whole space of external
12 inputs.

13 MR. SHAFFER: That's correct.

14 CHAIRMAN APOSTOLAKIS: Two big spaces,
15 actually, isn't it?

16 MR. SHAFFER: Well, the idea, again
17 coverage is a conditional probability given that a
18 fault exists. It doesn't care the source of the
19 fault, whether it's an operator action, whether it's
20 a random hardware failure. The faults represent
21 conditions of the system as a result of a fault. The
22 fault represents conditions of the system under
23 certain adverse consequences.

24 CHAIRMAN APOSTOLAKIS: Given one fault --

25 MR. SHAFFER: Which could represent

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

1 anything.

2 CHAIRMAN APOSTOLAKIS: -- there's a lot of
3 space of inputs.

4 MR. SHAFFER: That's correct. And it
5 could represent inputs, hardware failures, whatever.

6 CHAIRMAN APOSTOLAKIS: What is the typical
7 number of faults in these applications people have
8 produced?

9 MR. SHAFFER: In this process that UVA has
10 applied, they have injected over 100,000 faults in one
11 case.

12 CHAIRMAN APOSTOLAKIS: There is an
13 intelligent way for defining those faults?

14 MR. SHAFFER: Yes, at the lower blocks
15 there, 4, 5, 6, and 7, that's where the detailed
16 knowledge of the system is required. Further
17 compounding the problem of the large fault set is the
18 issue of no response faults. Assuming a tractable
19 sample set of experiments could be found, it is
20 possible that many of the faults selected will not
21 result in any noticeable effect on a system. These
22 are called no response faults. These are essentially
23 latent errors that have not caused any noticeable
24 effect for the duration of the experiment. Other
25 issues related to practicality include actual

1 construction of the test harness, how we can actually
2 perform the fault injection experiments, and test
3 automation. How do we, as we perform a test, and we
4 get a response that may lock up the system, there has
5 to be some way to automatically reset the system.
6 Because if you need an operator there to reset every
7 time, the total test time could be intractable, given
8 the number of experiments that have to be performed.

9 The digital system dependability research
10 will allow confirmation that the fault injection
11 process we have selected addresses these issues
12 sufficiently enough so that it can be applied to
13 digital systems of interest to the NRC. We want to
14 effectively determine how safety systems behave under
15 faulted conditions. Such information could
16 potentially be used to augment and supplement the
17 current process for reviewing license applications,
18 and that direct testing of qualified systems in
19 approved configurations could lead to realistically
20 conservative licensing decisions, based on both
21 deterministic and probabilistic criteria.

22 An illustration of what we plan to do is
23 in this figure. We will have the capability to model
24 both the hardware, the software, and its interfaces.
25 Because we will have physical access to the systems,

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

(202) 234-4433

www.nealrgross.com

1 we will have the actual code. However, I do not
2 discount the potential need for alternative software
3 models. These are very complex systems. The hardware
4 model is based on simple fetch-execute computer
5 architecture. Again, we'll have physical access to
6 the system, and we have a generic processor model
7 which is one of the blocks in the figure on process.

8 MEMBER WHITE: Excuse me, Roman.

9 MR. SHAFFER: Sure.

10 MEMBER WHITE: Are you going to also
11 handle common failures? In other words, multiple
12 faults?

13 MR. SHAFFER: We will handle multiple
14 faults. Now, whether they're common mode, we believe
15 we'll be able to use the results of this to address
16 that issue. Whether we will actually be able to
17 define what a common mode failure is, particularly a
18 software common mode failure, I am not sure we'll be
19 able to do that because then we would need more than
20 one channel.

21 MEMBER WHITE: Okay, thanks.

22 CHAIRMAN APOSTOLAKIS: But when you select
23 the faults, in general you don't have common cause
24 failures in mind?

25 MR. SHAFFER: We're going to have a huge

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

(202) 234-4433

www.nealrgross.com

1 fault space. To really do these common mode failures,
2 we would probably need more than one channel, and
3 inject faults.

4 CHAIRMAN APOSTOLAKIS: But you could do
5 it?

6 MR. SHAFFER: In principle, yes. But the
7 scope of our work is a single channel.

8 CHAIRMAN APOSTOLAKIS: And the fault can
9 be a software problem or a hardware problem, failure?

10 MR. SHAFFER: That's correct. We're going
11 to mess with --

12 CHAIRMAN APOSTOLAKIS: And it's always
13 one?

14 MR. SHAFFER: Well, what we've found on
15 previous work is if we inject a single fault, then
16 sometimes we see multiple corruptions, multiple
17 corruptions being faults at multiple locations in the
18 system. In fact, up to five. Those are a very small
19 percentage, but we've seen that.

20 CHAIRMAN APOSTOLAKIS: Okay.

21 MR. SHAFFER: The generic processor model,
22 which we will discuss in a moment, will enable us to
23 determine the types of faults to inject. However,
24 long-term, if we could develop a process that was not
25 dependent on having the hardware available and would

1 still allow in-depth analysis, that would be ideal.
2 There is potential to develop a simulation model of
3 the hardware configuration, and use that for
4 simulation-based fault injection. And that will be
5 discussed later as well.

6 As I said earlier, we have modeling tools
7 that allow us to go to the gate level, so that is
8 always an option. But we're always looking for
9 efficiencies in our processes. If we can stay at a
10 relatively high level of abstraction, that sort of
11 releases us from having actual hardware, but then we
12 become dependent on the vendors and the engineers,
13 those who have real knowledge of the system.

14 Now we're going to discuss each block one
15 by one. This is just an overview. The analytical
16 safety model provides the mathematical framework for
17 calculating reliability and/or safety estimates. It's
18 simply a high-level representation of the faulty
19 behavior of the system under analysis. Several
20 suitable analytical models from the literature include
21 Markov models, Petri nets, fault trees, and
22 variations, colored Petri nets, dynamic fault trees,
23 etcetera. Critical fault parameters may include
24 failure rates, repair rates, fault detection
25 latencies, and fault coverage. This is the most

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 difficult to estimate, but that's the parameter we
2 want to estimate.

3 CHAIRMAN APOSTOLAKIS: It seems to me you
4 will have here the problems we discussed earlier,
5 namely whenever in real life, or even in your testing
6 processes, you find faults, you probably fix them.
7 So.

8 MR. SHAFFER: Yes, during a design process
9 you would --

10 CHAIRMAN APOSTOLAKIS: Even in whatever
11 process. I can't imagine that you find, you know,
12 faults and you just leave them there. Maybe one or
13 two you say I don't care, but in general you go and
14 correct the problem. So now, you know, the parameters
15 you want, again, is the -- are the statistics
16 collected applicable. This is a really tough problem,
17 you know. By the way, this is not unique to you.
18 NASA had that huge problem with the shuttle. Every
19 time they find a problem they fix it, and sometimes
20 the fix costs half a million dollars. And here comes
21 now the risk analyst saying 'Oh, there were five
22 failures' and the guy goes bananas. I spent half a
23 million eliminate this problem, and you're telling me
24 that it's still a failure. So I don't know. I mean,
25 this estimation of remaining faults from things that

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 I have found and I have fixed is something that I
2 don't think we know how to handle as a community.

3 MR. SHAFFER: Can I give you a little
4 background maybe?

5 CHAIRMAN APOSTOLAKIS: Yes, you can give
6 me background.

7 MR. SHAFFER: UVA developed this initially
8 as a way to design fault tolerant systems. It would
9 work in parallel between hardware and software, where
10 you would catch the faults early. We happened upon
11 this at a later time, and determined that it may be
12 useful to an assessment process. Our intention is to
13 obtain certain qualitative analyses where we may
14 already have certain information available to us, and
15 from there determine what the design safety
16 requirements were. And from there then we could
17 establish, you know.

18 CHAIRMAN APOSTOLAKIS: Are you coming back
19 to Steve's argument of earlier today that, you know,
20 no matter what the numbers are, at the end I have
21 gained a hell of a lot of insights to the system by
22 doing this. And I'm 100 percent with you.

23 MR. SHAFFER: That's right.

24 CHAIRMAN APOSTOLAKIS: I mean really, if
25 you inject 100,000 faults and you find what's going

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

(202) 234-4433

www.nealrgross.com

1 on, I mean more power to you. But when you start
2 calculating lambdas like Dr. Johnson did here several
3 months ago, then I get cold, to the point of freezing
4 sometimes.

5 MR. SHAFFER: Yes, well --

6 CHAIRMAN APOSTOLAKIS: I just don't think
7 you can do that. And I'm willing to listen. I mean,
8 I'm dying to find an argument that says this is the
9 right thing to do. I don't see it. I haven't seen
10 it. And it's not your problem. It's not your
11 problem. Don't take it personally.

12 MR. SHAFFER: No, I don't.

13 CHAIRMAN APOSTOLAKIS: Nobody knows how to
14 do that, including me.

15 MR. SHAFFER: I think that --

16 CHAIRMAN APOSTOLAKIS: We're on the same
17 boat. Sergio, you're smiling. Do you know anybody
18 who can do it?

19 MEMBER GUARRO: No. That's surprising,
20 that expression of modesty, that's all.

21 (Laughter)

22 MR. ARNDT: I can say that's
23 uncharacteristic that he should.

24 CHAIRMAN APOSTOLAKIS: I mean, do you
25 disagree with anything I just said? No. No. And I'm

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

1 telling you, we had that problem in NASA PRA of the
2 shuttle. And as you know, how political that is now,
3 right? Re-launching the shuttle after the accident
4 and so on. It was a real problem. Here you have a
5 guy who says 'I just spent a quarter of a million
6 dollars fixing this problem, and you're telling me
7 you're going to consider it a failure and do the
8 calculations as if nothing happened?' What do you say
9 to that? So they came up with a methodology for
10 discounting failures. So this was not one failure,
11 this was 0.65 of a failure, you know, that kind of a
12 thing. And you appreciate now what kind of issues
13 come out of that. But it's a real issue. It is a
14 real issue. And I think we have that here too.

15 MR. ARNDT: We do.

16 CHAIRMAN APOSTOLAKIS: There are two
17 arguments. One is can you really ignore some failure
18 that happened because you think you fixed it, and
19 second, by trying to fix it, have you introduced
20 additional problems. So anyway, as far as the
21 analysis of the structure of the software/hardware I
22 have no problem with that. I mean, all this method
23 clearly gives you good insights. But when we go to
24 numerical estimates, now I don't know. Okay. So
25 let's go on. Unless you disagree with what I said.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. SHAFFER: I think there's --

2 CHAIRMAN APOSTOLAKIS: Look, I'm trying to
3 learn here. It's not -- but somebody has to be the
4 bad guy here.

5 MR. SHAFFER: I don't think you're being
6 a bad guy at all. In the -- for whatever that's
7 worth.

8 MR. KEMPER: Let me step into this for
9 just a second. Maybe I shouldn't, but certainly the
10 intent, our desire is to come up with some way of
11 substantiating the reliability of this system. That's
12 what we desire the licensees to be able to demonstrate
13 to us.

14 CHAIRMAN APOSTOLAKIS: I'm with you. What
15 I'm saying here is that these are big issues. They
16 are not just your problem. And as a community, we
17 don't know how to attack them, and the sooner all of
18 us agree to that, and then start from there, the
19 better off we'll all be. Because I've seen a lot of
20 applications where people take existing models from
21 reliability theory and they force them onto software
22 because, you know, it's the standard thing. You know,
23 I've lost my keys and I'm looking around the lamp
24 because that's where the light is. So.

25 MR. KEMPER: Well, there may not be an

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

(202) 234-4433

www.nealrgross.com

1 obvious solution at this point, but we're certainly
2 going to continue to pursue that.

3 CHAIRMAN APOSTOLAKIS: Your use of the
4 word "obvious" was very unfortunate.

5 (Laughter)

6 MR. KEMPER: Doesn't that mean that a
7 solution cannot be achieved, right? I tell my folks
8 all the time, the world was flat for a long time until
9 we proved that.

10 CHAIRMAN APOSTOLAKIS: These days it's
11 triangular.

12 MR. KEMPER: That's right.

13 CHAIRMAN APOSTOLAKIS: Okay, Roman. Sorry
14 for the interruption.

15 MR. SHAFFER: No problem.

16 CHAIRMAN APOSTOLAKIS: I'm not really
17 sorry.

18 (Laughter)

19 MR. SHAFFER: Okay. The statistical model
20 is used to estimate critical model parameters in the
21 analytical model.

22 CHAIRMAN APOSTOLAKIS: I would skip this.

23 MR. SHAFFER: Why?

24 CHAIRMAN APOSTOLAKIS: We've discussed
25 this enough. Keep going.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. SHAFFER: Well, this is an important
2 component.

3 CHAIRMAN APOSTOLAKIS: I know, and now
4 you're -- okay.

5 MR. SHAFFER: Well, we use the statistical
6 model to determine how many fault injection
7 experiments we do. And that's a critical component of
8 --

9 CHAIRMAN APOSTOLAKIS: What did you say?

10 MR. SHAFFER: We use the statistical model
11 to estimate, or to determine the number of fault
12 injection experiments to perform. Okay?

13 CHAIRMAN APOSTOLAKIS: I'd like to see
14 that. There may be some value to it. Yes, I agree.

15 MR. SHAFFER: So we have single --

16 CHAIRMAN APOSTOLAKIS: But you haven't
17 fixed anything. Yes, good. That's fine.

18 MR. SHAFFER: The statistical model is
19 also used to determine -- I'm sorry. Okay. The
20 statistical model is used to determine the number of
21 fault injection experiments, but also that in turn
22 affects which fault injection technique we'll use of
23 the four. We'll discuss these later.

24 CHAIRMAN APOSTOLAKIS: I'll tell you what.
25 The statistical model I'm sure has value, but what

1 would have more value as far as I'm concerned is to
2 see some intelligent way of selecting the faults based
3 on the anticipated use of the system.

4 MR. SHAFFER: That's where the novelty of
5 this approach.

6 CHAIRMAN APOSTOLAKIS: That's where I
7 would really love to see how they do that. You know,
8 pretty soon before you realize it you have to
9 understand all the accident conditions you might have
10 in the plan, right? Because these are safety systems,
11 so they have to respond and control, if you will, say
12 accident situations. And my God, you're getting into
13 accident space. I don't know. Dr. Kress, do you
14 think we understand all that?

15 MEMBER KRESS: I think you do have to get
16 into accident space.

17 CHAIRMAN APOSTOLAKIS: In which case it's
18 a huge space.

19 MEMBER KRESS: It's a huge space.

20 CHAIRMAN APOSTOLAKIS: And I'd like to
21 know whether there are any intelligent ways, or semi-
22 intelligent ways of selecting where to put the fault.
23 Not just the number of faults, but also where.

24 MR. SHAFFER: Well, in this process they
25 apply those algorithms.

1 CHAIRMAN APOSTOLAKIS: I'd like to see
2 that. I mean, I'm sure Dr. Johnson, does he have
3 anything? Because he did them for trains. I don't
4 know, but maybe you guys could do it.

5 MR. ARNDT: Yes. One of the outputs of
6 this particular project will be looking at how do you
7 apply those kind of methodologies that have been used
8 in other --

9 CHAIRMAN APOSTOLAKIS: Failure and in
10 nuclear.

11 MR. ARNDT: Right.

12 CHAIRMAN APOSTOLAKIS: Okay, great.

13 MR. SHAFFER: UVA developed a behavior
14 level model of a generic processor, a basic fetch-
15 execute cycle. It was applied to a design project in
16 Europe, and was certified by TUV Germany. The generic
17 processor fault model is used to generate the fault
18 space for the system, where the fault space is defined
19 by location, time, and value. Location is where the
20 fault occurs within the system under analysis. Time
21 is the time of occurrence and duration of permanent or
22 one instruction cycle. Value is a defined corruption
23 of the correct entity called a mask. Any accessible
24 registers and memory locations can be corrupted.
25 Detailed fault models have been derived from the

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

(202) 234-4433

www.nealrgross.com

1 literature for register file and register selection
2 faults, program counter faults, control unit,
3 instruction decode logic faults, data address control
4 bus faults, and arithmetic logic units. This generic
5 model was validated by simulation, and augmented by
6 refining the masks. And then it was applied to
7 several COTS processors, two Motorola and an AMD. For
8 digital system dependability research, the generic
9 model will be applied to the processors and the
10 systems under test, and then an appropriate fault
11 space generated, which again could be very large.
12 Therefore, certain techniques to reduce the number of
13 fault injection experiments to a tractable number will
14 have to be used.

15 Before performing the fault injection
16 experiments, however, the system is placed into
17 context by determining appropriate operational
18 profiles. If it's an RPS, we'll have to define a
19 proper operational profile, if it's load sequencer,
20 etcetera. These should be representative of the
21 system under various modes of operation and
22 configuration, since various configurations may invoke
23 different hardware and software functions. To get a
24 good understanding of the system's behavior under
25 faulted conditions, a sufficient number of

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 combinations should be analyzed.

2 The operational profile is divided into
3 four phases, a startup phase, where the system is
4 allowed to reach a stable state, no faults are
5 injected due to the short time interval relative to
6 the operational time. It's statistically
7 insignificant. The second phase is a system light
8 workload where there are no faults from the simulated
9 external environment, and thus only a reduced set of
10 software and hardware functions are running in the
11 background, such as diagnostics. The third phase is
12 a system heavy workload where significant interaction
13 with the simulated external environment to exercise as
14 much of the system's resources as possible. And the
15 fourth phase is a short no activity phase so that
16 outputs can stabilize to determine externally
17 observable effects due to the fault injection. Then
18 you determine if the system failed. This sequence
19 will thoroughly exercise the system and allow us to
20 observe its behavior under the influence of both
21 transient and permanent faults.

22 After determining the appropriate set of
23 operational profiles, the experimental setup will
24 simulate the selected operational environment under
25 fault-free conditions. Data will be collected on the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 system under test, such as instruction sequences of
2 observable state data, system buses, etcetera. Note
3 that the fault diagnostic functions are also
4 monitored, and information is collected. This data
5 here is the fault-free execution trace. Equipment
6 used includes logic analyzers, bus analyzers, in-
7 circuit emulators, and software debuggers. So we're
8 going to get a lot of information.

9 The set of injected faults and the
10 analysis of the fault injection experiments are
11 dependent on the fault-free execution trace. For
12 example, when a fault is injected into the system,
13 data is again collected on the system's response and
14 compared to the fault-free trace. Therefore, the
15 fault-free execution traces should have as much detail
16 as possible to ensure accurate identification of
17 covered, uncovered, and no response faults.

18 One significant challenge with fault
19 injection is that the fault space can be quite large,
20 making it unfeasible to test the entire fault space.
21 A reduced set of faults is then randomly selected from
22 the fault space. Recall that this statistical model
23 determines the number of fault injection experiments
24 that must be performed to satisfy the confidence
25 intervals. Another challenge, however, is that not

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 all faults injected cause an observable effect.
2 Therefore, the initial statistically significant
3 subset does not provide enough data to estimate the
4 critical model parameter. Further, the no response
5 faults are the worst case result as far as time of
6 testing. Fault injection tests that yield no response
7 faults require the longest amount of time as the
8 system response is compared to the fault-free
9 execution trace. So you're waiting for a response
10 that doesn't come during the duration of the test. So
11 they're just long tests.

12 To overcome problems posed by no response
13 faults, a technique to collapse the fault list by
14 eliminating no response faults is applied. This is
15 based on work by Benso, Guthoff, Smith, et al, and
16 Iyer, Ravi Iyer, et al. However, there still leaves
17 the issue of a large set of tests to inject as
18 determined by the statistical model. For systems with
19 high coverage requirements, the number of required
20 fault injection experiments may be quite large. The
21 concept of fault equivalence may be applied to reduce
22 the number of experiments. This is essentially a
23 variance reduction technique. The algorithm seeks to
24 identify sets of faults that have an identical effect
25 on the system, even though each fault in the set is

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 distinct. These sets of equivalent faults are called
2 equivalence classes. Only one fault from each
3 equivalence class needs to be injected to determine
4 the effect of all faults in that class.

5 The earlier algorithm was received with
6 some criticisms, so they refined it. The assumption
7 is the faults are uniformly distributed in the fault
8 space, therefore they have equal probability of
9 occurrence. They randomly sample a number of faults,
10 and they determine the number of equivalent classes
11 from those faults. Since with assumption one there's
12 no bias in the coverage estimates since the faults in
13 the equivalence classes are also random.

14 Again, the effectiveness depends on how
15 much information can be derived from the execution
16 trace. In a real world example, UVA applied the
17 process to an interlocking control system, which is a
18 failsafe application of 10 years of operation, 150
19 locations throughout the country, 30,000 lines of
20 assembly code, had a time requirement of 200
21 millisecond response time, and 80 percent of the code
22 was devoted to diagnostics. They injected over
23 100,000 permanent faults. And using this fault
24 expansion technique, that approximated about 9.5
25 billion faults. They evaluated about 1,900 transient

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 faults. And that was expanded to about 136 million
2 faults. Clearly that offers us some advantages.
3 Again, as I said earlier, the work will undergo a peer
4 review, so there will be time for scrutiny of the
5 results. And getting back to Steven's point, just
6 doing the fault injection experiments, having a set of
7 faults that we know will get a response, and
8 determining the system's response will give us a large
9 amount of information. I believe that'll be useful to
10 the safety reviewers as well as the PRA.

11 CHAIRMAN APOSTOLAKIS: So this is now from
12 the Virginia work, this kind of diagram?

13 MR. SHAFFER: Yes. It is, actually. In
14 fact, most of these slides are.

15 CHAIRMAN APOSTOLAKIS: So you plan to
16 adapt it to nuclear applications?

17 MR. SHAFFER: We do indeed.

18 CHAIRMAN APOSTOLAKIS: You did already?
19 Or you will?

20 MR. SHAFFER: We're undergoing a feedwater
21 control system assessment now. And we will apply this
22 to safety-related systems.

23 CHAIRMAN APOSTOLAKIS: Because I was
24 thinking, as I said earlier, maybe you need something
25 there addressing the issue of environments, accident

1 environments. Somewhere in there, you know, you have
2 to have that.

3 MR. SHAFFER: Again --

4 CHAIRMAN APOSTOLAKIS: Given the fault,
5 what are the possible inputs to the software. If I
6 have a small LOCA, a large LOCA, if I have this, if I
7 have that. Those are different inputs.

8 MR. SHAFFER: Right, but again, coverage
9 is a conditional probability that doesn't care about
10 the source of the faults. Given a fault, does the
11 system detect it.

12 CHAIRMAN APOSTOLAKIS: Right. But what if
13 you miss a whole class of inputs because you never
14 considered a medium LOCA? Then you can't find the
15 conditional probability because you missed a lot of
16 possible inputs, given the fault. That's what I'm
17 saying. Given the fault, you may have a whole space
18 of possible inputs depending on the accident.

19 MR. KEMPER: Roman, I believe back on
20 Slide 19, is that where you? I assume that you were
21 addressing that when you said light loads versus heavy
22 loads for the operational profiles?

23 MR. SHAFFER: Yes, that's part of it.
24 Yes.

25 MR. KEMPER: Okay.

1 CHAIRMAN APOSTOLAKIS: But what I'm saying
2 is that you need to show it explicitly in those
3 figures.

4 MR. SHAFFER: Okay, well there's a way we
5 can -- when we determine the fault space, it's
6 possible for us to trace backwards to what the
7 external inputs would be, or could be. I mean, given
8 that --

9 CHAIRMAN APOSTOLAKIS: Well, I'm not
10 saying you can't do it, Roman. All I'm saying is
11 that, you know --

12 MR. ARNDT: Be sure to do it.

13 CHAIRMAN APOSTOLAKIS: Yes. I didn't say
14 you can't do it.

15 MEMBER GUARRO: I think you mentioned the
16 assumption that the faults are uniformly distributed
17 in the fault space.

18 MR. SHAFFER: That's correct.

19 MEMBER GUARRO: And is that a valid
20 assumption?

21 MR. ARNDT: Well, that is not a necessary
22 assumption. It just happens to be the going in
23 assumption. You can go in and do a parametric study
24 to look at what the distribution is, and/or what
25 effects it may have depending upon your assumed input

1 states.

2 MEMBER GUARRO: Yes, because I'm thinking
3 of an analogy. You tell me if it's out of context.
4 But I'm thinking of the difference between a pure
5 Monte Carlo sampling and a Latin Hypercube sampling,
6 in which you're worried about, you know,
7 characterizing details that are rare events. And so
8 now you go there more often than you should under a
9 theoretical assumption or uniformity. I think
10 probably something like this, my intuition tells me
11 that may apply. I may be wrong.

12 MR. ARNDT: It's a similar concept,
13 although not exactly the same thing. And the point is
14 well taken. The Virginia work did do some work on
15 statistics of the extreme to look at this as part of
16 applying this to a nuclear example, and George's point
17 that these are rare events in many cases, and it's
18 difficult to characterize them. You have to go back
19 and carefully, as Roman was saying earlier, if you
20 have a particular fault, you can go backwards and look
21 at the input state that's associated with that. So
22 what you need to do is you do the experiment, then you
23 start relaxing assumptions, and look at does the
24 uniform distribution as opposed to a different kind of
25 distribution have an issue. Is the fault space you're

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 using characteristic of an appropriate operational
2 profile and input characterization. Those are parts
3 of QA'ing the process to make sure it is applicable to
4 a nuclear example.

5 CHAIRMAN APOSTOLAKIS: Roman keeps telling
6 us that we are looking for a conditional probability
7 giving the fault. In a nuclear application, it's not
8 inconceivable that you will have a number of
9 conditional probabilities, namely given this fault,
10 and given I have a small LOCA, here is the conditional
11 probability of it. Given the same fault, but given
12 that I have a large LOCA, maybe I have another
13 conditional probability. So it's a double condition,
14 in other words. It doesn't sound too far-fetched to
15 me. I mean, different accidents create different
16 conditions.

17 MR. ARNDT: Right. And you can
18 characterize those conditions, those accident
19 conditions if you will, as input parameters. For a
20 trip circuit you have low pressure.

21 CHAIRMAN APOSTOLAKIS: Sure, but I would
22 like to know these conditional probabilities. And if
23 you just tell me given this fault the conditional
24 probability of failure is 10^{-3} , maybe you're not
25 giving me the whole story.

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

(202) 234-4433

www.nealrgross.com

1 MR. ARNDT: Yes, that goes back to what is
2 the operational profile and what's the fault space.

3 CHAIRMAN APOSTOLAKIS: Okay, okay. Let's
4 go on. It's getting late in the day, and Steve
5 threatens us with two presentations here.

6 MR. ARNDT: Yes. They're both short.

7 CHAIRMAN APOSTOLAKIS: Yes I know about
8 that. Risk assessment, short.

9 MR. SHAFFER: We have several fault
10 injection methods available to us. I won't spend too
11 much time on these. We have hardware-based fault
12 injection, which is essentially where we augment the
13 system with additional hardware so we can perform the
14 whole fault injection experiments. We have software-
15 based fault injection, and that's where we develop a -
16 - we modify, interrupt service routine to inject
17 changes in the software operation. A simulation-based
18 fault injection is where we have a complete simulation
19 model of the system. There is commercial software
20 available called SIMEX where they provide complete
21 models of certain microprocessors. We've considered
22 doing that. And then the final approach is the hybrid
23 approach, which is some combination. It's possible we
24 could do a simulation of the processor interface to he
25 hardware prototype and perform a series of fault

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 injections that way. But this will all have to be
2 determined during the project.

3 Now, there are advantages and
4 disadvantages, but I don't need to go through those.
5 We'll get into the research projects. Over the past
6 few years, we've done a Digital Feedwater Control
7 System assessment, and it's continuing under the
8 cooperative agreement with OSU. The second project is
9 the Digital System Dependability Performance project,
10 which will kick off in the end of FY05. And this is
11 a multi-year effort. This is the project where we're
12 going to evaluate a number of systems. We believe
13 there's great benefit to all parties involved here,
14 but mostly to us because we get a better assurance of
15 safety of these systems. We'll know how they fail,
16 and we'll be able to incorporate that into our
17 process. Right now we have three platforms that we've
18 generically approved. This work doesn't propose to
19 redo all that. We want to look at these in their --
20 as close to site-specific implementations as we can.

21 Future effort will explore other
22 dependability metrics, such as maintainability,
23 confidentiality, and integrity. That's under the
24 security work, which from my understanding we'll come
25 before you again later and discuss those, which are

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 also my projects.

2 The Digital System Dependability
3 Performance project for the highest probability of
4 success will require work with vendors and licensees.
5 We'll have access to the systems, but we're also going
6 to need access to their systems designers, engineers.
7 They're the ones with the knowledge of the malicious
8 faults. Those are the faults they know that if they
9 occur, an unsafe condition could happen. I'm not
10 saying that these systems are unsafe in any way, but
11 there are certain conditions that if they happen, if
12 the protections are defeated, could lead to adverse
13 consequences. During the work, we'll perform the
14 fault injection testing following the process
15 described earlier. And we estimate about 12 months
16 per system evaluation. It's actually platform.

17 CHAIRMAN APOSTOLAKIS: How does this
18 dependability work different from risk assessment?
19 Isn't this part of what you have to do to do a risk
20 assessment?

21 MR. ARNDT: To do a risk assessment you
22 need to, as you know, understand the ways the system
23 can fail.

24 CHAIRMAN APOSTOLAKIS: And this helps me
25 do that.

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

1 MR. ARNDT: This helps us do this. This
2 is going to be one possible input to the supporting
3 analysis necessary to build failure models for a PRA.
4 But the reason we've got it as a separate broken-out
5 project is, first of all, just the way systems fail is
6 not in and of itself just a reliability issue, it's an
7 understanding the system better, as well as, if you go
8 back up one slide, you can use these methods to do
9 other things, like integrity of the system, to look at
10 things like the security-type issues as well. You can
11 look at other dependability metrics other than failure
12 rate.

13 MR. SHAFFER: I think I should state that
14 as I've been talking there was an implicit assumption
15 that these safety systems we've approved have unsafe
16 failures, unsafe faults. It could very well be that
17 we don't find anything. We don't know. I don't want
18 to say ahead of time that they do.

19 CHAIRMAN APOSTOLAKIS: Well, if you find
20 anything it will be a small number.

21 MR. SHAFFER: This is true. But the idea
22 is that we know, and that's where everyone benefits.
23 It's all about assurance for us. And if it's
24 assurance for us, the licensees have assurance.

25 I do say conclusion, but I mean to say

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

1 summary. The digital system dependability research
2 will augment and supplement the current regulatory
3 process by characterizing significant hardware,
4 software, and interface errors, including system
5 interface errors that could prevent safety system
6 action or cause initiating events which could undo the
7 challenge-mitigating systems, understanding potential
8 new failure modes and the criteria for detecting these
9 failure modes prior to failure of plant safety
10 functions, identifying or developing methods and data
11 that enable the NRC to establish the risk importance
12 aspects of digital safety systems, Steven's project,
13 and modeling of digital systems that could be used to
14 support probabilistic risk assessments. And that's
15 all.

16 CHAIRMAN APOSTOLAKIS: Comments or
17 questions from the members or the consultants?

18 MEMBER WHITE: I have one question on your
19 generic process fault model. You were talking about
20 time, and you said that would include the fault
21 injection time, and the duration, and the duration
22 would be either one cycle or permanent, I think. Do
23 you think you might eventually look at fault durations
24 that are intermittent, you know, just for several
25 cycles, then off? You understand what I mean?

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 MR. SHAFFER: Yes. That's a slightly more
2 difficult problem, but yes. We could reach that
3 point.

4 CHAIRMAN APOSTOLAKIS: Anything else?
5 Well, thank you very much. Now, Steve, why don't we
6 go ahead with your self-test methods.

7 MR. ARNDT: Okay.

8 CHAIRMAN APOSTOLAKIS: I think that's
9 next, right?

10 MR. ARNDT: Yes. Just for scheduling
11 points of view, this will be a relatively short
12 presentation, and then I've got about a half hour, 45-
13 minute presentation on the overview of the risk
14 program.

15 CHAIRMAN APOSTOLAKIS: Maybe we'll take a
16 short break between the two?

17 MR. ARNDT: Yes. That would be good.

18 MR. SHAFFER: Did you say self-test
19 methods?

20 MR. ARNDT: Yes.

21 CHAIRMAN APOSTOLAKIS: So let's finish
22 this because with the next one, we start the whole
23 issue of risk assessment.

24 MR. ARNDT: Well, this was originally
25 intended to be a fairly short presentation because we

1 haven't really done a lot of background work on this.
2 This is just something new that we're going to be
3 starting, and we wanted to give you some general
4 overview. When Mike Waterman gave this presentation
5 this morning when talking about the discussion of the
6 comments on the research program he discussed a lot of
7 this, so some of this will be redundant, so I'll go
8 through this relatively quickly.

9 As we talked about this morning, this
10 program is under the Software Quality Assurance
11 program. It need not necessarily be there. It could
12 have been under the emerging technology part of the
13 program, or the systems aspect program. The reason we
14 put it here as opposed to some other place was a lot
15 of these issues are software issues. Not all self-
16 testing is software. Some of it's hardware. But this
17 just seemed like the easiest place to put it.

18 As we discussed this morning, self-testing
19 methods can be hardware or software tests that are
20 done on a continuous basis to improve the system
21 available. They're designed into the system to
22 improve the availability or functionality of the
23 system. This is distinguished from a subject that we
24 have in another part of the plan that talks about
25 system diagnostics. That talks about is the system as

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 a whole working, or system issues associated with
2 evaluation of calibration and things like that. This
3 is aspects of the system that are specifically
4 designed to improve the hardware/software, the digital
5 part of the system.

6 One of the issues associated with this
7 over the years was the overhead associated with these.
8 That's pretty much gone away. Even with real-time
9 safety-critical systems, the power of these systems
10 from a computational standpoint has significantly
11 reduced the overhead issues associated with that. The
12 performance issues are different. The issues
13 associated with is the system going to have an issue
14 associated with too much crammed into a cycle time, or
15 locking the diagnostic system up, or having a fault in
16 the diagnostic system affecting the performance of the
17 overall system. Those issues still exist. It's just,
18 the point of the bullet is the fact that because the
19 overhead is not such a big deal, these systems are
20 more commonly used.

21 And these can be very, very simple kinds
22 of things, like checking to make sure that the system
23 has executed all of its programs in the allotted time,
24 various kinds of very simple self-checks. It can be
25 inversion programming kinds of things to determine

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 whether or not two different versions of the code came
2 up with the same answer, and then going forward.
3 There's a number of different kinds of things that
4 we're talking about.

5 One of the big issues, as NRR talked about
6 earlier when they presented, as we talked about
7 earlier in several programs is the complexity issue.
8 The idea of these systems is to improve the
9 availability by making sure the thing doesn't fail
10 when it doesn't have to. But the problem is you're
11 adding additional complexity in the overall system as
12 you add more and more self-checking type applications.
13 So the real issue here is we want to understand, one,
14 is there a tradeoff between how much complexity you
15 add and the failure modes associated with the added
16 complexity and the actual system itself. The other
17 thing is are there systems or types of self-checking
18 that are preferred as opposed to not preferred. An
19 analogy would be an effort that we did a few years ago
20 on safe programming language applications. We did a
21 study on what was the preferred methodologies for
22 coding. The idea behind that project was to give NRR
23 a potential list of things that are likely to be good
24 coding practices, and things that might not be so
25 good. When you see them in a review, you need to

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 spend more time looking at them.

2 As we talked about this morning, there's
3 a limited amount of time you can spend in a review.
4 And you have significant time resources associated
5 with that. So the idea of this project, the outcome,
6 is to provide additional information to the regulatory
7 review staff on aspects of self-testing that they
8 might want to look at more closely. What does the
9 experience tell us? What does the theory tell us
10 associated with what's the best way to do these, and
11 where might there be some problems?

12 I've gone through a lot of these in the
13 overview. The issue is what effects, if any, might
14 this have on system performance, what adverse effect
15 may it have, what are the most acceptable testing
16 methodologies versus the least acceptable testing
17 methodologies, and what is the theoretically best or
18 most acceptable amount of self-testing. So the
19 project is basically going to focus on those kinds of
20 aspects, as well as what operational history has told
21 us. Mike Waterman this morning gave you two examples
22 of systems in nuclear applications that failed because
23 of self-testing issues, not because of the actual
24 systems that they were designed to -- the functional
25 aspects of the system. There's been a lot of cases in

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 clearly the software part of it, and there's been
2 examples in other areas where because they didn't
3 think through some of the ways systems -- the
4 diagnostics could fail, they put them into
5 application, and they had faults because the
6 complexities associated with the self-test got the
7 best of them. So. How much self-testing is enough?
8 How much is too much? What kind is appropriate is
9 really what we're trying to look for, both from a best
10 practices operational experience, and theoretical
11 standpoint.

12 So that's what this project's about. We
13 haven't kicked it off yet. As Mike mentioned before,
14 we'll probably have a lot of interactions -- we intend
15 to have a lot of interactions with our NRR colleagues
16 associated with this. We've discussed this with them
17 once already on what aspects of this they think is
18 most appropriate. And we'll go through the process of
19 --

20 CHAIRMAN APOSTOLAKIS: Have you decided
21 who's going to do this?

22 MR. ARNDT: No. We have not decided.

23 CHAIRMAN APOSTOLAKIS: Okay. Thanks
24 Steve. You say your next presentation is a 45-minute
25 presentation?

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

(202) 234-4433

www.nealrgross.com

1 MR. ARNDT: Half hour, 45 minutes.
2 Depends on how many questions we get.

3 CHAIRMAN APOSTOLAKIS: Okay. So let's
4 recess till 4:20.

5 MEMBER KRESS: Let's go ahead and do it.
6 We don't need a recess. Let's go ahead and do it.

7 CHAIRMAN APOSTOLAKIS: No, let's break for
8 awhile.

9 MR. ARNDT: Let's break.

10 CHAIRMAN APOSTOLAKIS: Okay, 15 minutes.

11 (Whereupon, the foregoing matter went off
12 the record at 4:05 p.m. and went back on the record at
13 4:24 p.m.).

14 CHAIRMAN APOSTOLAKIS: Okay, Mr. Arndt.
15 Risk assessment. You're speechless.

16 MR. ARNDT: Absolutely. I'm in awe by
17 your greatness.

18 MEMBER KRESS: Bow down.

19 MR. ARNDT: The purpose of this
20 presentation, like the overview presentation that Bill
21 and I gave earlier in the day is to give some general
22 background on the overall risk assessment program, get
23 some general ideas on why we think we should be doing
24 it, why we think it's important, and the structure of
25 the overall program. Tomorrow we will go into the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 individual programs and some intermediate results
2 associated with them.

3 As we all know, the NRC has a PRA policy
4 statement which encourages the use of PRA to the
5 extent supported by the state-of-the-art and data.
6 One of the big issues that is central to this is what
7 is the state-of-the-art. Do we have sufficient
8 information and techniques to be able to do this kind
9 of work? And it really gets to, and I'm going to talk
10 about this a little more in a couple of slides, the
11 fact that there's two issues here. The issue that
12 we've been primarily focusing on is the state-of-
13 the-art such that we can inform the regulatory process
14 in approving and evaluating digital systems for
15 applications based on risk-informed information. The
16 other issue, of course, is that all the rest of the
17 risk-informed applications are based on a complete
18 PRA. And of course, as the licensees put more and
19 more digital systems into the plant, a general PRA
20 that doesn't model digital systems and their
21 interactions is less complete. So we have both those
22 issues as potential outcomes and issues associated
23 with this.

24 So the research is oriented toward
25 improving the NRC's knowledge and providing consistent

NEAL R. GROSS

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

(202) 234-4433

www.nealgross.com

1 processes for regulating digital systems. So what we
2 want to do is all the kinds of things you want to do
3 when you develop risk models. We're going to gather
4 and understand the data, assess the modeling methods
5 that might be used, what is adequate, understand the
6 systems that need to be modeled, and what level of
7 detail. This is one of the big issues. Like any
8 other modeling application, there may be some models
9 that can be modeled fairly simplistically, and there
10 may be some systems that you have to model at a much
11 greater level of detail simply because of the
12 complexity of the system, and/or how they interface
13 with other systems. We have to develop and test
14 methods. Now we don't necessarily have to develop
15 them ourselves, but we have to understand what the
16 modeling capabilities are, what the limitations are,
17 and whether or not we can live with those limitations.
18 And then we have to develop regulatory acceptance
19 criteria. This is the point we made earlier. By
20 acceptance criteria, what we mean is those aspects of
21 digital system analysis in reliability space that are
22 particular issues for digital systems. So for
23 example, regulatory acceptance criteria might be a
24 version of the 1.74 series specific to digital systems
25 that highlights those additional issues that you want

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 to look at in digital system analysis.

2 As we've talked about extensively,
3 licensees are replacing analog systems with digital
4 systems. In some cases, these are fairly sporadic
5 occasional type issues in non-safety systems. In
6 other cases, like the Oconee case, they're looking at
7 doing a very complete digital system replacement of a
8 large number of safety systems, trip systems, SFAS
9 systems, and things like that.

10 Some of the current deterministic
11 licensing criteria are challenges. The one that has
12 been most in the news recently is BTP-19, which is the
13 staff guidance on diversity and defense-in-depth. One
14 of the challenges associated with this is how that
15 analysis has to be done. The industry has expressed
16 interest in using risk-informed ideas as an
17 alternative method for meeting some of these more
18 challenging issues, like diversity and defense-in-
19 depth. And I'll talk about that briefly later. So
20 there is some interest in using risk information, or
21 risk perspectives in the current licensing framework.
22 So the real issue is what are the limitations of
23 digital system reliability models, and can they be
24 used, can they be expanded, can they be used in a
25 limiting kind of a thing, or some certain aspects, or

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 do we need to do a full modification of PRAs.

2 The real issues are not easy ones, as
3 Professor Apostolakis mentioned. In addition, even if
4 we got a risk-informed application, our current
5 methods and data within the agency to do an
6 independent assessment aren't up to par either. So if
7 we get an application either in the forms of a topical
8 report, and we have one for review, or of an actual
9 application based upon a risk-informed application, we
10 currently don't have methods available to us to do an
11 independent assessment.

12 CHAIRMAN APOSTOLAKIS: Now, can you --
13 maybe you covered it, I don't know. Let's go back.
14 I'm intrigued by the sub-bullet that says that some of
15 the current licensing criteria are difficult to meet.
16 Can you give an example or two?

17 MR. ARNDT: The example that is used is
18 the diversity and defense requirement. The way the
19 diversity and defense requirement, BTP-19, is written,
20 you have to do an analysis of what would happen in the
21 case of a common mode software failure. The
22 recommended analysis associated with that, and someone
23 correct me if I don't get this quite right, makes
24 certain assumptions that basically says if you have a
25 software failure, you have to assume a large part of

1 your systems fail, and then go through all your design
2 basis accidents and determine that even with this
3 software failure, you can withstand in Part 100 space
4 the design basis accidents. Now, some of that's not
5 very difficult to do because you have auxiliary backup
6 systems which are not safety grade. You have operator
7 actions. You go over and punch out the system and
8 things like that. But there are some accidents that
9 that becomes a real challenge for. Large-break LOCA
10 is the one that comes to mind, and that's primarily
11 because of the timing issues associated with it. So
12 because that is a deterministic analysis making
13 certain what most people would call very conservative
14 assumptions, you have some challenges in meeting that.

15 Now, the alternative is you put it in a
16 diverse backup system in addition to your digital
17 systems. Now, obviously if you believe your digital
18 systems are of high quality and reliable in the first
19 place, you don't want to have that added burden
20 associated with them. But when I say some current
21 licensing criteria are difficult to meet, it means
22 there are certain criteria that if you take them at
23 their base, they're believed by many in the industry
24 to be overly conservative and force you to make design
25 tradeoffs they would prefer not to make. Did I get

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 that roughly correctly?

2 MR. TOROK: May I comment?

3 CHAIRMAN APOSTOLAKIS: Identify yourself,
4 please.

5 MR. TOROK: My name is Ray Torok. I'm
6 from EPRI, and I'm the project manager on the industry
7 guideline on this subject. And all I was going to add
8 to what Steve said there was that in a case like the
9 large-break LOCA, obviously it's a low probability
10 kind of event, but also what you find when you look at
11 it in PRA space is that the probability of failure of
12 the system is dominated not by the INC in the system,
13 but by the large rotating machinery, so that even if
14 you add a diverse backup like Steve's talking about,
15 from a risk standpoint it doesn't help in terms of
16 core damage frequency and so on. And it does add
17 complexity that may actually increase the likelihood
18 of a problem.

19 MR. ARNDT: So, in any case, the point is
20 there are reasons that the industry is interested in
21 some form of risk-informing some of our regulations
22 because of these kinds of issues. How exactly that's
23 done --

24 CHAIRMAN APOSTOLAKIS: So ultimately you
25 would like to be able to use Regulatory Guide 1.174?

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 That's really what you would like to do?

2 MR. ARNDT: The industry has, that's the
3 approach it would like.

4 CHAIRMAN APOSTOLAKIS: Well, you do. I
5 mean, the Commission's policy is to be risk-informed,
6 right?

7 MR. ARNDT: Yes.

8 CHAIRMAN APOSTOLAKIS: All of us.

9 MR. ARNDT: And we'll go into that more.
10 In the June 2004 ACRS letter, Professor Apostolakis
11 also in his added comments recommended that in this
12 particular area, databases containing software-induced
13 failures should be reviewed, and their contributions
14 should be used, the information we gained from that.
15 And he also recommended available methods for
16 assessing reliability systems that are software-driven
17 should be reviewed critically. And this is a bit of
18 a paraphrase, but I believe that's generally the idea.

19 MEMBER KRESS: You realize, of course,
20 that the reason these are added comments is the rest
21 of the ACRS rejected them.

22 MR. ARNDT: I understand. I was there
23 when --

24 CHAIRMAN APOSTOLAKIS: So the next slide
25 will not do either of these, right?

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

(202) 234-4433

www.nealrgross.com

1 (Laughter)

2 MEMBER KRESS: Remember, we attempt to
3 accommodate all perspectives.

4 CHAIRMAN APOSTOLAKIS: Thank you very
5 much.

6 MR. ARNDT: Both of these are very
7 appropriate comments. In deriving what we're trying
8 to accomplish, we need to understand -- and they both
9 go to the issues associated with the PRA policy
10 statement. What we want to do is understand what the
11 state-of-the-art is and what the state-of-the-data is,
12 and what we want to do is build on that in our
13 Research Program Plan. So the point of highlighting
14 these here is it goes back to my first slide. What
15 we're trying to do is understand the state-of-the-art,
16 build on the state-of-the-art, and try and get to
17 where we need to be, which is both the policy in terms
18 of how we're going to interface with the licensees,
19 and also our own internal methodologies.

20 So the research program is designed to use
21 the available information in data to understand the
22 capabilities, as I said on the last slide. The big
23 issues here are to look at what's going on and use the
24 most promising methods, or at least try to use the
25 most promising methods and investigate them. We

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

(202) 234-4433

www.nealrgross.com

1 really have two issues here. We need to understand
2 what is and is not possible, and what are the
3 limitations of the modeling effort. We need to do
4 that for two reasons. One, to direct our research in
5 the right way for internal analysis techniques, but
6 also to help us support development of regulatory
7 guidance. So when EPRI or one of the licensees comes
8 in with an application, we understand what the
9 limitations are so we can ask better questions. So
10 what we want to do is work on that.

11 So as part of our program, we're going to
12 look at, and develop, and integrate new methods. And
13 "new methods" is probably too strong of a word. It's
14 new methods to the NRC. We also want to pilot these
15 things using both traditional methods and dynamic
16 methods where appropriate. We want to benchmark the
17 capabilities of different methodologies. One of the
18 biggest issues, of course, in any new methodology is
19 you need some benchmarks. How well did these work in
20 specific applications. So as we talk about what is
21 exactly in our program, one of the things we want to
22 do is for certain applications, for certain kinds of
23 systems, we want to benchmark the different kinds of
24 methodologies that have been proposed, and understand
25 based on both the theoretic aspects and the benchmarks

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 what the limitations are. So as part of that, we can
2 get out guidance for regulatory applications.

3 And my EPRI colleagues have chided me
4 already on this first bullet. EPRI has proposed a
5 methodology. The biggest issue associated with that,
6 which is not a sub-bullet, but please pencil it in, is
7 the fact that their methodology relies on the measures
8 that are designed into the system to enhance its
9 reliability. Things like fault tolerant behavior, and
10 things like that. They want to take credit for how
11 these systems are designed. They rely also on the
12 issue that Ray just brought up, that a lot of the
13 systems, total systems, not just the digital systems,
14 have aspects associated with the failures of the big
15 spinning parts. So their methodology looks at
16 understanding the system from a total system
17 perspective, particularly the bounding assumptions
18 associated with the reliability of the digital system
19 compared to the system it is controlling, or it's
20 actuating.

21 CHAIRMAN APOSTOLAKIS: Has EPRI submitted
22 this report for formal review by the NRC?

23 MR. ARNDT: It's been submitted. It's
24 under what is known as acceptance review consideration
25 right now. As part of review of topical reports, we

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 look at it and say, all right, do we want to review
2 it. And this has a number of different issues
3 associated with it, associated with resources, and do
4 we think it's an acceptance methodology, and do we
5 want to review it or not. So right this particular
6 second we're trying to determine if we're going to
7 review it, and what the schedule's going to be. Yes?

8 MR. TOROK: May I offer a couple more
9 comments?

10 MR. ARNDT: Sure.

11 MR. TOROK: This is Ray Torok from EPRI
12 again. And yes, I just wanted to offer a couple of
13 clarifications there. The first bullet says it's a
14 method for incorporating digital systems into current
15 generation PRAs. And I would characterize maybe a
16 little differently in that what we were trying to do
17 was apply risk insights to defense-in-depth and
18 diversity evaluations for digital upgrades. Now, that
19 does lead you to addressing the issue of modeling
20 digital systems in PRA. They're obviously related.
21 And what we do is we use estimated failure
22 probabilities for the digital equipment to get it into
23 the same playing field as the other hardware in the
24 system that the digital licensee happens to be. So in
25 that sense it's a qualitative approach, really, where

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 you apply engineering judgment, and in some cases
2 standards, like the one that's mentioned, the IEC
3 standard. But it really comes back to engineering
4 judgment at some point.

5 Now, what Steve mentioned about these
6 defensive measures things is very important for both
7 determination of susceptibility, where you may be
8 susceptible to the common cause failure, and for
9 estimating failure probability of the digital
10 equipment. We go back to looking at these defensive
11 measures that are built into the digital system. And
12 that's really important because it gets you beyond
13 just looking at the process. Because what you really
14 want to know is what the real system behaviors are,
15 and make your decisions based on that. Because there
16 are large uncertainties in the digital equipment
17 failure probabilities, we address that now with
18 uncertainties, which means that if the NRC research
19 work comes up with better ways to determine those
20 probabilities of failure, they're certainly applicable
21 within the framework. So I see that as all fitting
22 together in a nice way. Thanks.

23 MR. ARNDT: Thank you, Ray. Our research
24 is focused a little bit differently. We're focusing
25 more on the, if you will, the fundamentals of the

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

(202) 234-4433

www.nealrgross.com

1 reliability modeling, understanding what kind of
2 models might be appropriate, developing both
3 traditional and dynamic methods, and seeing whether or
4 not they're applicable, if they work, where they work,
5 investigating model acceptability, and doing some
6 benchmarks. So we're going at it from a slightly
7 different perspective. As Ray mentioned, hopefully
8 our framework will be sufficiently broad that we can
9 include what they're doing, and they're hopefully
10 going to do the same thing. So the issue really is
11 we're attacking it from slightly different
12 perspectives, but the objective is to have a
13 methodology where we can include risk insights into
14 the regulatory process.

15 This is a historical graph, and I'll only
16 spend about a minute on it. This is what I presented
17 last March when we talked about this. I found a
18 better way of doing it, so I'm just putting it up here
19 to remind you. The concept is there are certain
20 aspects of this that we're investigating. We're
21 trying to understand PRAs and digital systems in them
22 as our final product. To do that, you need to
23 understand the digital system itself. You have to
24 understand the hardware, the software, and the
25 supporting analysis that provides you the failure

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 modes, and things like that. As we've tried to
2 develop this program a little bit better, we've come
3 up with a somewhat I hope better way of looking at all
4 the different aspects of our program, which is on
5 Slide 9.

6 What we're really doing from a project
7 standpoint within the program is trying to accomplish
8 certain things. If you look at the left-hand side of
9 your screen, one of the aspects that's very important
10 in both choosing what kind of models you do, as well
11 as supporting the models, is understanding what the
12 failure data is. Another aspect is reviewing the
13 current reliability modeling methodologies, and coming
14 up with ideas on what might work best, choosing the
15 candidates for possible inclusion. Those both tie
16 into the development of approaches for modeling the
17 systems.

18 That center box there is really what we
19 were talking about this morning, and early this
20 afternoon, supporting analysis. You need to
21 understand how this system works in one way or the
22 other to be able to characterize it in some kind of
23 model, be it a fault tree model, be it a dynamic flow
24 graph model, be it any kind of model. You need to
25 understand how the system works, and not just the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 visual system, but how it works with the process that
2 it's interfacing with. And you can do this in a
3 number of different ways. You can use hazard
4 analysis, you can use failure modes and effects
5 analysis, you can use software testing, or fault
6 injection, or a number of other methodologies to
7 understand how the system works. Those we don't
8 include in the digital system reliability program
9 because those are outside the program, but they're
10 feeding into it. Those are the things that we need to
11 understand to develop the reliability models.

12 On the left-hand side is traditional
13 method, fault tree/event tree modeling methodologies,
14 and on the right-hand side is dynamic methodologies.
15 One of the big issues, as Professor Apostolakis has
16 highlighted, and a lot of other people have
17 highlighted, is there's a lot of ways you could
18 potentially do this. A lot of ways that people do it.
19 And there's a lot of argument. Well, is this
20 appropriate. Is that appropriate. Can you do this.
21 There is no consensus in the community. We need to,
22 one, understand what the limitations of the various
23 models are, and also we need to understand for our
24 internal needs what is the best way to do this. One
25 of the biggest issues is when you model these things,

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 what are the limitations. And are you willing to live
2 with the limitations for that particular application.
3 The whole point of developing a PRA quality standard
4 is saying, all right, in some applications you can
5 live with a less sophisticated model. In some
6 applications you can't live with a less sophisticated
7 model. You need a greater amount of details, or a
8 better understanding of things. To write a regulatory
9 position on that, be it a Reg Guide 1.17x, or be it
10 into the quality standard, or whatever, you need to
11 have an appreciation of that.

12 To do that, what we've done in our program
13 is specifically had two different sets of researchers
14 looking at it from two different aspects, and trying
15 to independently assess whether or not this is
16 possible, and what the limitations are in particular
17 cases. As we develop methodologies to do that, then
18 we're going to also develop benchmarks. Right now
19 we're looking at two benchmarks that have certain
20 aspects associated with them. One would be a control
21 system, probably an aux feedwater system. It has
22 less, quote unquote "safety significance" but it has
23 a lot more process interactions. The other would
24 probably be a reactor protection system trip signal.
25 It has a lot more safety significance, but from a

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 modeling standpoint it's much simpler. We want to get
2 some benchmarks that give us the biggest bang for the
3 buck, we learn the most from doing the analysis. And
4 the idea would be to use two or three different
5 methodologies, both traditional fault tree/event tree
6 methodologies, and maybe some of the dynamic
7 methodologies, and understand both from a modeling
8 perspective and an understanding of how hard or easy
9 it is to actually do these kinds of models. Based on
10 that, we will then decide how to, or if we should
11 update NRC tools and data to provide independent
12 assessments.

13 Now, I've spent a fair amount of time
14 talking about the graph, and the next three or four
15 slides basically are redundant to what I've just said,
16 but I'll go through them quickly anyway. But this is
17 really the concept behind what we're trying to do.
18 And what we'll talk about tomorrow is particular
19 pieces and parts of that.

20 CHAIRMAN APOSTOLAKIS: I'm not disagreeing
21 with anything you said, but my -- the thrust of my
22 comments in the letter that you cited, but also other
23 people's comments, is that in this particular case of
24 software, we shouldn't just jump into Markov models or
25 whatever. We should really question the basic

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

(202) 234-4433

www.nealrgross.com

1 assumptions behind it, precisely because the evidence
2 is that most of the problems come from specification
3 errors, requirements, you know, design type errors.
4 So it's really a different way of thinking about
5 reliability models. And it's very easy to just say,
6 oh okay, well I'll use a Markov in a discrete state,
7 and move from here to there. What does this lambda
8 223 mean? What are the random events that you're
9 assuming are occurring, and you know, at a constant
10 rate? So this is really the critical review that I
11 was talking about. And I think it's important to do
12 that, and I assure you we can do it.

13 MR. ARNDT: Right. And we specifically --
14 and I agree. And there's two issues associated with
15 that. One, you have to do as good a job of reviewing
16 possible strengths and limitations in the various
17 models as you can before you start spending money to
18 do development. And we think we've done a pretty good
19 job, and you're going to hear some of that tomorrow.
20 The other issue is at some point you have to start
21 doing a little bit more detailed analysis and modeling
22 to understand the limitations. Can you choose any
23 particular methodology, dynamic flow graph methodology
24 for example? What are the limitations in terms of
25 practicality? Can you get enough data? Can you get

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 the prime implements? Is there a methodology that can
2 be used so you have both the understanding of the
3 limitations as well as understanding the practicality.

4 CHAIRMAN APOSTOLAKIS: But the most
5 fundamental thing is the theoretical basis. You know,
6 you can have a practical method that is not
7 theoretically sound, you're in trouble. That doesn't
8 mean that you go with the best theoretical method.
9 Practicality comes in, there is no question about it,
10 but the theoretical basis I think is very important.

11 MR. ARNDT: It is.

12 CHAIRMAN APOSTOLAKIS: And there is
13 literature on these issues. I don't know if you guys
14 have found it. In the past people have argued back
15 and forth.

16 MR. ARNDT: Yes, we've done a fairly
17 sophisticated review of a lot of the literature,
18 including the paper you referenced in your additional
19 comments, among others. Both the development of a
20 theoretical -- or the set of assumptions we're going
21 to choose to use, I should say. It's not so much a
22 theoretical argument, but it's a choice of what
23 arguments we're going to choose to use, as well as an
24 evaluation of what seems most promising is something
25 that we're specifically working on.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN APOSTOLAKIS: All right.

2 MR. ARNDT: Let me reiterate a couple of
3 things as I go through these other slides. Like I
4 said, most of it I've already talked to you about.
5 The outcome is to really understand what systems need
6 to be modeled, what level of detail they need to be
7 modeled, what kind of accuracy are we talking about,
8 what uncertainty, if you will, are we talking about.
9 Developing the capability to independently verify
10 these systems, and developing acceptance criteria.
11 What is we want out of the licensee application. So
12 as I mentioned before, we're specifically looking at
13 several different methodologies. We've got two
14 different research teams specifically so we don't miss
15 anything, so we look at it from several different
16 aspects.

17 This is the part of the project that's
18 looking at the data. We're going to have some more
19 discussion on it tomorrow so I won't dwell on it. But
20 as part of this, we're looking at what's out there,
21 what can be used, what more information do we need.
22 One of the biggest problems is most of the digital
23 failure databases don't have enough information in
24 them to support reliability calculations directly.

25 CHAIRMAN APOSTOLAKIS: But this is all

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 nuclear you mean? When you say failure data, nuclear
2 failure data? Or you're looking at other industries?

3 MR. ARNDT: We're looking outside as well.
4 But I'll give you one example, the LER database, which
5 is used for a lot of different things. The problems
6 associated with that are numerous. It will give you
7 some digital system failures, but in many cases it
8 doesn't give you a sufficient level of detail to
9 characterize it in one way or the other.

10 CHAIRMAN APOSTOLAKIS: But we also don't
11 have extensive experience with these things, do we?

12 MR. ARNDT: We have less than great
13 experience in many areas. We don't have time between
14 failures, we don't have number of systems deployed,
15 and issues like that to get basically the denominator
16 in the equation. So there's a lot of issues
17 associated with it, but we want to use as much data as
18 we can, if nothing else to inform the process, but
19 also to develop these kinds of databases that are
20 going to be needed.

21 The purpose of part of our research is
22 really to understand what is out there, what are the
23 advantages and disadvantages. And I've talked about
24 this fairly significantly. The issues associated,
25 what the risk-important characteristics are, what are

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

(202) 234-4433

www.nealrgross.com

1 the things you have to include in the model is
2 something that's very important. Basically the
3 methodologies, which ones are the most appropriate.
4 Can you use one kind of methodology, or another kind
5 of methodology, and if you use one kind of
6 methodology, what limitations do you have to place on
7 your results?

8 So in summary, the research is designed to
9 solve basically the issues that we have. And we've
10 also designed it as a broad-based program looking at
11 a number of different potentially viable options. And
12 one of the things we really, really, really want is to
13 have a proactive interactive relationship with the
14 subcommittee on these issues. Because this is a
15 controversial issue, we're trying to build in peer
16 review wherever it makes sense. To some extent you
17 can't peer review everything or all you do is spend
18 time making presentations like this. But wherever it
19 makes sense, we want to get interaction with the
20 technical community, be it papers, and conferences,
21 and journal articles. We want to get interactions
22 with the licensee community. We're planning to have
23 a workshop probably summer, late summer, fall, to talk
24 about some of the aspects of the regulatory issues
25 that we're looking at. We've had some external peer

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 reviews on some of our research products. We'd like
2 to have that same kind of rapport with the committee.
3 And what we're really looking for is how can we do
4 things better, where are things that might prove more
5 promising, and issues like that. Things that we may
6 not have considered, or you think we might consider
7 more, those kinds of interactions are something we
8 would appreciate.

9 Like I say, we're going to go into some of
10 the details much more extensively tomorrow, both in
11 terms of planning for each of the blocks that we had
12 up here, as well as some of the preliminary results
13 we've had in a couple of the areas.

14 CHAIRMAN APOSTOLAKIS: Okay. That's it?

15 MR. ARNDT: That's it for my overview.

16 MR. KEMPER: That's all we have to present
17 today. So if you'd like to continue on tomorrow we
18 could do that I guess. Or we could continue on this
19 afternoon if you prefer.

20 CHAIRMAN APOSTOLAKIS: Any comments,
21 questions, from our people around the table? No?
22 Jim, no? Shall we go around the table you think, or
23 should we do it tomorrow afternoon? Jim and Sergio
24 will send us a written report.

25 MEMBER KRESS: So we can wait till

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

1 tomorrow.

2 CHAIRMAN APOSTOLAKIS: Wait until tomorrow
3 I think. Okay. Any comments from the audience?

4 MR. WATERMAN: Professor Apostolakis, I
5 just wanted to add one thing that Jim White pointed
6 out during the break was in all of these projects in
7 the research plan, you'll notice the last product is
8 a training curricula for whatever the product might be
9 such that not only do we have, for example, a review
10 procedure, but we also intend to incorporate into our
11 contract some form of curricula development so that
12 when we deliver that product to our supported offices
13 they also get training on how to use that product in
14 a consistent manner, which is just absolutely
15 critical. Instead of just dropping something on
16 somebody's desk and saying 'Now, go use' we really
17 want to emphasize that all of these things need some
18 form of curricula developed so that as new staff come
19 on down the road they can be sent off to be trained on
20 how to use those products, and so we can build up our
21 infrastructure so that people like Paul Loeser aren't
22 just on their own. It's unfortunate that we have to
23 use GS-14s and GS-15s to do a lot of the grunt work
24 that you can take a kid straight out of school to do,
25 but right now we're kind of stuck with you need an

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 expert to review every aspect of the system because
2 that's all you've got. And a training curricula is
3 designed to help resolve some of that by providing
4 some of that expertise to some of our junior staff
5 members to bring them along. Thank you.

6 CHAIRMAN APOSTOLAKIS: Okay. So, thank
7 you very much Steve. And this first day is over.
8 We'll reconvene tomorrow at 8:30. No? Well, this
9 subject at 1:00. 8:30 we have another meeting.
10 Right? Okay. Thank you.

11 (Whereupon, the foregoing matter was
12 concluded at 5:02 p.m.).

13
14
15
16
17
18
19
20
21
22
23
24
25

CERTIFICATE

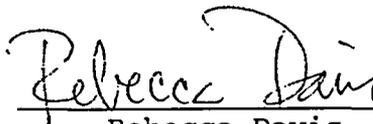
This is to certify that the attached proceedings
before the United States Nuclear Regulatory Commission
in the matter of:

Name of Proceeding: Advisory Committee on
Reactor Safeguards
Digital Instrumentation
And Control Systems
Subcommittee Meeting

Docket Number: n/a

Location: Rockville, MD

were held as herein appears, and that this is the
original transcript thereof for the file of the United
States Nuclear Regulatory Commission taken by me and,
thereafter reduced to typewriting by me or under the
direction of the court reporting company, and that the
transcript is a true and accurate record of the
foregoing proceedings.



Rebecca Davis
Official Reporter
Neal R. Gross & Co., Inc.

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

(202) 234-4433

www.nealgross.com



RESEARCH PLAN COMMENTS

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS DIGITAL INSTRUMENTATION AND CONTROL SUBCOMMITTEE MEETING

JUNE 14, 2005

Michael E. Waterman, Sr. I&C Engineer

William E. Kemper, Section Chief

I&C Engineering Section

Engineering Research Application Branch

Division of Engineering Technology

Office of Nuclear Regulatory Research

(301-415-2818, mew1@nrc.gov)

(301-415-5974, wek@nrc.gov)



OVERVIEW

- NRC Licensing Bases
- NRC Licensing Process
- Emphasis on Communications
- Comment Disposition Summary Table
- Disposition of Comments
- Summary



SUMMARY

- 34 comments were received from NRR, NMSS, and NSIR
- 31 of the 34 comments were incorporated into the Research Plan
- The remaining 3 comments address topics that are outside the scope of this Research Plan or required no change
 - Metrics to evaluate research effectiveness (NRC internal reviews of programmatic effectiveness)
 - Incorporation of human factors considerations in PRAs (Human Performance Plan)
 - NRR SRP considered sufficient guidance by NMSS/FCSS
- RES revised the Research Plan to reflect the need for additional information in several areas on the basis of communications with the supported Offices
- The Research Plan will continue to be updated in response to communications with the supported Office(s) as new needs are identified and as research projects are completed



NRC LICENSING BASES

- The NRC uses an extensive set of regulations, guidance, standards, and technical reports to license digital safety systems
 - Code of Federal Regulations
 - Commission policy statements
 - Standard Review Plans (SRPs)
 - Branch Technical Positions in SRPs
 - Consensus standards
 - Regulatory Guides endorsing consensus standards
 - Topical reports
 - Research reports



NRC LICENSING PROCESS

- The regulations, guidance, standards, and technical reports identify several hundred important attributes and associated criteria that must be addressed appropriately for digital systems to be licensed for safety-related applications
- The purpose of conducting research is to investigate current and emerging methods and knowledge and, where appropriate, to augment and supplement NRC processes to enable NRC staff to evaluate digital systems consistently and effectively



ADDITIONAL EMPHASIS ON COMMUNICATIONS

- The Research Plan was revised to provide additional emphasis on
 - Development of research products (review procedures, tools, etc.) that augment and supplement existing NRC review plans and processes as part of a general process improvement initiative
 - Enabling communications between RES and supported Office(s) during the initial stages of research project planning to identify specific research products that must be developed, and during performance of research to keep the supported Offices informed on the progress of research
- Meetings were held with supported Offices to describe the Research Plan, and to discuss changes to the Research Plan that better reflect the objectives of the research projects. These meetings are the precursor for future TAG meetings to address specific issues.



COMMENT DISPOSITION



COMMENT DISPOSITION

SECTION CHANGED	RESEARCH PLAN SECTION TITLE	COMMENT #	TYPE OF CHANGE			
			REVISED INFO	ADDED INFO	REVISED SCOPE	NO REVISION
2.1	Objective of the Research Plan	NMSS/IMNS 2	X	X		
2.2	Scope of the Research Plan	NRR/SPSB 5		X		
3.1.1	Environmental stressors	NRR/EEIB 1	X	X		
3.1.3	COTS digital systems	NMSS/IMNS 3		X		
3.1.3	COTS digital systems	NRR/EEIB 5	X	X	X	
3.1.4	Electrical power distribution system interactions with nuclear facilities	NRR/EEIB 2	X	X	X	
3.1.6	Operating systems	NMSS/IMNS 3		X		
3.1.6	Operating systems	NRR/EEIB 3	X	X		
3.2	Software Quality Assurance	NMSS/IMNS 3		X		
3.2.1	Assessment of software quality	NRR/EEIB 5	X	X	X	
3.2.2	Digital system dependability	NRR/EEIB 5	X	X	X	
3.2.3	Self-testing methods	NRR/EEIB 4	X	X		



COMMENT DISPOSITION (cont.)

SECTION CHANGED	RESEARCH PLAN SECTION TITLE	COMMENT #	TYPE OF CHANGE			
			REVISED INFO	ADDED INFO	REVISED SCOPE	NO REVISION
3.3	Risk Assessment of Digital Systems	NRR/SPSB 11	X			
3.3.2	Investigation of digital system failure assessment methods	NMSS/IMNS 3		X		
3.3.2	Investigation of digital system failure assessment methods	NRR/SPSB 2		X	X	
3.3.3	Investigation of digital system characteristics important to risk	NRR/SPSB 7	X		X	
3.3.3	Investigation of digital system characteristics important to risk	NRR/SPSB 6	X			
3.3.4	Investigation of digital system reliability assessment methods	NRR/EEIB 5	X	X	X	
3.3.4	Investigation of digital system reliability assessment methods	NRR/SPSB 1	X	X		
3.3.4	Investigation of digital system reliability assessment methods	NRR/EEIB 4	X			
3.3.4	Investigation of digital system reliability assessment methods	NRR/SPSB 8	X			



COMMENT DISPOSITION (cont.)

SECTION CHANGED	RESEARCH PLAN SECTION TITLE	COMMENT #	TYPE OF CHANGE			
			REVISED INFO	ADDED INFO	REVISED SCOPE	NO REVISION
3.4	Security aspects of digital systems	NSIR/DNS 1	X	X		
3.4.1	Security assessments of cyber vulnerabilities	NSIR/DNS 2				X
3.4.2	Security assessments of EM vulnerabilities	NSIR/DNS 3	X			
3.4.2	Security assessments of EM vulnerabilities	NRR/EEIB 6	X	X		
3.4.3	Network Security	NRR/SPSB 3	X	X		
3.4.3	Network Security	NSIR/DNS 4		X	X	
3.5.2	Radiation-hardened integrated circuits	NRR/EEIB 7	X	X	X	
3.5.5	ASICs and FPGAs	NRR/EEIB 8	X	X		
3.6	Advanced Nuclear Power Plant Digital Systems	NRR/SPSB 5		X		
3.6.3	Advanced NPP digital system risk	NRR/EEIB 5	X	X	X	
GENERAL		NMSS/FCSS 3	X			
GENERAL		NMSS/FCSS 2	X			
GENERAL		NRR/SPSB 9	X			
NONE		NMSS/FCSS 1				X
NONE		NMSS/IMNS 1				X
NONE		NRR/SPSB 10				X



RESEARCH PLAN RELATIONSHIP TO THE NRC STRATEGIC PLAN

- A general comment from NRR was that the research projects should have as their purpose a focus on safety, security, effectiveness, or openness
 - In section 4 of the Research Plan, each research project is linked to specific NRC Strategic Plan supporting strategies for achieving the NRC Goals of Safety, Security, Openness, and Effectiveness (Management is the other Strategic Goal)
 - An in-depth discussion relating each research project to corresponding Strategic Plan supporting strategies would have been repetitive and distracting. The tabular format in section 4 was considered the best alternative for succinctly relating the NRC Strategic Plan goals to the research projects



SECTION 2 OBJECTIVE AND SCOPE

- Schedule periodic, formal briefings for the supported Offices on the interim results and status of the tasks (§ 2.1)
 - RES is developing more formal processes to improve communications with the supported Offices
 - TAGs, project development meetings, project status reviews, etc.
- Advanced instrumentation and controls research would also be beneficial for existing plants undergoing digital retrofits (§ 2.2)
 - Recommendation incorporated into Section 2.2 and Section 3.6
 - These sections were revised to reflect the potential applicability of advanced reactor research products to existing plants



SECTION 3.1

SYSTEM ASPECTS OF DIGITAL TECHNOLOGY

- The justification in Section 3.1.1 is to “reduce licensing uncertainty.” The justification should be focused on safety, improved efficiency, effectiveness and realism, or openness.
 - Recommendation incorporated into Section 3.1.1
 - Additional focus was placed on safety, although, because licensing uncertainty is a key issue in the nuclear industry with regard to digital retrofits, the focus on reducing licensing uncertainty was retained
- Section 3.1.4 is not clear why this SBO research is included in the digital research plan
 - Recommendation incorporated into Section 3.1.4
 - This section was revised to address the effect of grid voltage fluctuations on digital equipment in NPPs
 - This research supports on-going research, and could be used to identify safety-related components and systems that are vulnerable to grid voltage fluctuations



SECTION 3.1 SYSTEM ASPECTS OF DIGITAL TECHNOLOGY (cont.)

- The Research Plan and SOWs should include digital technology involving byproduct materials
 - Recommendation incorporated into Sections 3.1.3, 3.1.6, 3.2, 3.3.2, and other sections as appropriate

- The state-of-the-art in software engineering may not be sufficiently matured for [quantitative] digital safety system reviews. This concern applies to the activities described in Sections 3.1.3, 3.2.1, 3.2.2, 3.3.4, and 3.6.3.
 - Recommendation incorporated into Sections 3.1.3, 3.2.1, 3.2.2, 3.3.4, and 3.6.3
 - Various methods will be validated as part of research and before recommendations are made to develop digital safety system review procedures
 - The research projects are expected to validate and increase the state-of-the-art in digital system licensing capabilities



SECTION 3.1 SYSTEM ASPECTS OF DIGITAL TECHNOLOGY (cont.)

- Section 3.1.6 is not clear on how proprietary restrictions for “COTS operating systems” can be resolved in a way that can improve the assessment of digital systems
 - Section 3.1.6 was revised to reflect that not all operating systems are proprietary, and to address issues regarding features of operating systems that may adversely affect safety
 - Nuclear industry digital system developers have expressed willingness to allow access to proprietary operating system design and development information



SECTION 3.2

SOFTWARE QUALITY ASSURANCE

- The plan should recognize that integrating digital systems into PRAs may not be practical and that a PRA may not be an efficient or accurate tool for digital system reviews.
 - Recommendation incorporated into Section 3.3
 - Acknowledged potential conclusion
 - This issue ultimately will be addressed by the “Risk” research projects
- Link the objective of Section 3.2.3 to safety, improved efficiency, etc., and explain how NRC reviews can be improved to assess self-test features
 - Section 3.2.3 was lengthened to discuss the development of technical guidance regarding the use and review of self-testing features in digital safety systems



SECTION 3.3 RISK ASSESSMENT OF DIGITAL SYSTEMS (cont.)

- Include the integration of external events, environmental, and security issues unique to digital system risk
 - Section 3.3.2 was revised to state that these failure modes will be evaluated as part of the investigation of digital system failure assessment methods
 - Initial development efforts will exclude external events, etc., until the methodology is sufficiently developed to address these additional issues
- The goal of the Section 3.3.3 research should be to provide methods for incorporating a digital component or system into a PRA
- In addition, acceptance guidelines should be considered as part of the deliverable
 - Section 3.3.3 was revised to address these comments



SECTION 3.3 RISK ASSESSMENT OF DIGITAL SYSTEMS (cont.)

- Section 3.3.3 should be clarified to reflect potential capabilities and to ensure “risk” is not used as in the plan as a synonym for “safety”
 - Section 3.3.3 was revised to reflect the comment and the Research Plan was revised to ensure that the term “risk” is used where “risk” is required
- Risk assessment should investigate advantages and disadvantages of analog and digital system architectures and implementation characteristics
 - Section 3.3.4 was revised to include a discussion on the evaluation of an analog RPS and FW control system for comparison with equivalent digital systems
 - Ongoing research is addressing this suggested approach



SECTION 3.3 RISK ASSESSMENT OF DIGITAL SYSTEMS (cont.)

- Justify Section 3.3.4 statement that digital reliability assessment methods will reduce staff review effort by 20 to 30 percent
 - Recommendation incorporated into Section 3.3.4
 - The statement was removed
 - The Research Plan was revised to emphasize that the research products will augment and supplement existing review processes



SECTION 3.4 SECURITY ASPECTS OF DIGITAL SYSTEMS

- Support development of 10CFR73 requirements that implement NRC post-September 11, 2001, security-related orders and regulatory guidance
- Support NSIR development of a comprehensive cyber security plan
 - Recommendations incorporated into section 3.4
- Section 3.4 should include research that supports industry implementation of NUREG/CR-6847, “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants”
 - Recommendations incorporated into section 3.4.1 and section 3.4.3



SECTION 3.4 SECURITY ASPECTS OF DIGITAL SYSTEMS

- Section 3.4.2 does not directly support NSIR plans, but it seems prudent to conduct research. Though the Commission has not considered EM weapons as a credible threat to nuclear power facilities, some limited anticipatory research in this area is likely warranted
 - Comments incorporated into section 3.4.2
- Section 3.4.2 describes an assessment of electromagnetic (EM) vulnerabilities. How does this activity relate to TEMPEST programs?
 - Recommendation incorporated into Section 3.4.2
 - The discussion of EM attacks was amplified to state that measures to address EM attacks are different than measures to address passive surveillance of emanated signals by unauthorized personnel (TEMPEST)
 - This project will address only EM attack vulnerabilities



SECTION 3.4 SECURITY ASPECTS OF DIGITAL SYSTEMS (cont.)

- Wireless technology and firewalls should be subsets of a network security research project
 - Section 3.4.3 was renamed, “Network Security;” and the discussion in Section 3.4.4, “Firewalls,” was incorporated into the renamed Section 3.4.3
 - The focus of section 3.4.3 was revised to address network security issues, including wired communications, wireless communications, and firewalls.



SECTION 3.4 SECURITY ASPECTS OF DIGITAL SYSTEMS (cont.)

- Section 3.4.3 should reference NUREG/CR-6847, ["Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants"] which covers the assessment of wireless devices. The proposed research projects described in this section should be informed with the assumption that licensees will implement the cyber security self-assessment tool described in the NUREG/CR
- Section 3.4.4, Firewall Security, should state that NUREG/CR-6847 can be applied to assess all digital devices, including firewalls, in nuclear power plants. Revise the proposed research project to develop regulatory guidance on the use of firewalls and expand review guidance of NUREG/CR 6847 to assist reviewers in evaluating the security risk of different firewalls
 - These comments were incorporated into the Research Plan



SECTION 3.5 EMERGING DIGITAL TECHNOLOGY AND APPLICATIONS

- Discuss use of system diagnosis, prognosis, on-line monitoring (SDPM) for virtual instrumentation and parameter estimation
 - Section 3.5.1 was revised to include a discussion on the advantages and disadvantages of using virtual instrumentation. The research objectives remain the same
- The regulatory applicability is not clear for the confirmatory studies of radiation-hardened integrated circuits in Section 3.5.2
 - Recommendation incorporated into Section 3.5.2
 - The tasks and products were revised to reflect the focus on guidance for the staff
 - Discussions with the supported Offices clarified the issue as presented in the Research Plan



SECTION 3.5 EMERGING DIGITAL TECHNOLOGY AND APPLICATIONS (cont.)

- Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs) described in Section 3.5.5 are not currently used in generically-qualified safety platforms. Include, early on, an assessment of the existing or potential uses of this equipment in power reactors
 - The first paragraph of Section 3.5.5 was revised to reference current and future applications of ASICs and FPGAs



SECTION 3.6 ADVANCED NUCLEAR POWER PLANT DIGITAL SYSTEMS

- Advanced instrumentation and controls research would also be beneficial for existing plants undergoing digital retrofits
 - Recommendation incorporated into Section 2.2 and Section 3.6
 - These sections were revised to reflect the potential applicability of advanced reactor research products to existing plants



NMSS/FCSS GENERAL COMMENTS

- Review guidance in NRR SRP has been used recently by NMSS/FCSS for digital system reviews
 - Section 1.4 was revised to state the NRC is conducting research to continually augment and supplement NRC capabilities (including the NRR SRP) for reviewing and assessing digital technology implementations in safety systems
- NMSS/FCSS Regulations (10CFR70) are based on a risk-informed approach supported by qualitative acceptance criteria. Therefore, quantitative safety assessments and quantitative acceptance criteria may not be useful for FCSS needs
 - The Research Plan projects in section 3.3 address development of risk-based approaches for licensing digital safety systems. The results of this research may support existing risk-informed licensing approaches



SPSB GENERAL COMMENTS

- The terms “software reliability” and “software quality” are used somewhat interchangeably
 - The Research Plan was revised to ensure there is a clear distinction between the use of the term “reliability” and the term “quality”



SUMMARY

- 34 comments were received from NRR, NMSS, and NSIR
- 31 of the 34 comments were incorporated into the Research Plan
- The remaining 3 comments address topics that are outside the scope of this Research Plan or required no change
 - Metrics to evaluate research effectiveness (NRC internal reviews of programmatic effectiveness)
 - Incorporation of human factors considerations in PRAs (Human Performance Plan)
 - NRR SRP considered sufficient guidance by NMSS/FCSS
- RES revised the Research Plan to reflect the need for additional information in several areas on the basis of communications with the supported Offices
- The Research Plan will continue to be updated in response to communications with the supported Office(s) as new needs are identified and as research projects are completed





COMMUNICATIONS BETWEEN RES AND SUPPORTED OFFICES

I&C TECHNICAL ADVISORY GROUP [RES & SUPPORTED ORG(S)]			RES		SUPPORTED ORG(S) WITH RES		SUPPORTED ORG(S)
Concepts	Requirements	Design	Implementation	Acceptance Testing	Licensing Process Integration	Training	Use
SUPPORTED ORGANIZATION(S)			RES		SUPPORTED ORGANIZATION(S)		
SUPPORTED ORGANIZATION(S)			RES				SUPPORTED ORGANIZATION(S)
SUPPORTED ORGANIZATION(S)			CONTRACTOR (optional)				SUPPORTED ORGANIZATION(S)



Draft Guide DG-1128
“Criteria for Accident Monitoring Instrumentation
for Nuclear Power Plants”
(Proposed Regulatory Guide 1.97, Revision 4)

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee Meeting
June 14, 2005

George Tartal, I&C Engineer
I&C Engineering Section
Engineering Research Applications Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research



OVERVIEW

- BACKGROUND
- REGULATORY GUIDE 1.97, REVISION 3
- IEEE STANDARD 497-2002
 - Selection, performance, design, qualification, display and quality assurance criteria
- DG-1128 (REGULATORY GUIDE 1.97, REVISION 4)
 - Regulatory positions
- APPROACHES CONSIDERED
- CONCLUSION



BACKGROUND

- Instrumentation required to monitor variables and systems under accident conditions
 - 10 CFR Part 50, Appendix A, Criteria 13, 19, 64
- Reg Guide 1.97 Rev. 1 issued in August 1977
 - Provided general design and qualification criteria
- Lessons learned from TMI
 - NUREG-0737
 - 10 CFR Part 50.34(f)
- Reg Guide 1.97 Rev. 2 issued in December 1980
 - Implementation via NUREG-0737 Supp. 1
- Reg Guide 1.97 Rev. 3 issued in May 1983



REGULATORY GUIDE 1.97, REV. 3

- Endorses ANSI/ANS-4.5-1980
 - This standard has been withdrawn and is inactive
- Organizes accident monitoring variables by variable type
 - Type A are for planned manual actions with no automatic control
 - Type B are for assessing plant critical safety functions
 - Type C are for indicating breach of fission product barriers
 - Type D are for indicating safety system performance and status
 - Type E are for monitoring radiation levels, releases and environs
- Design and qualification criteria applied by category
 - Cat 1 is for indicating accomplishment of safety function (~SR)
 - Cat 2 is for indicating safety system status (~AQ)
 - Cat 3 is for backup and diagnostic variables (~NSR)
- Rev. 3 is the defacto standard for accident monitoring



IEEE STANDARD 497-2002

- Consolidates and updates criteria from ANSI/ANS-4.5-1980, IEEE Std 497-1981 and Reg Guide 1.97 Rev. 3
- Technology-neutral approach intended for advanced design plants
- Performance-based, non-prescriptive approach to accident monitoring variable selection
 - Prescriptive tables of variables are replaced by criteria for selection based on the accident mitigation functions in EOPs, etc.
 - This is the most significant difference from Reg Guide 1.97 Rev. 3
- Selected variable type determines the applicable performance, design, qualification, display and QA criteria
- Recent industry standards cited in the criteria
- Provides criteria for digital instrumentation



IEEE STANDARD 497-2002 CRITERIA

- Selection
 - Defines variable types A, B, C, D and E and lists typical sources
- Performance
 - Range; Accuracy; Response Time; Duration; Reliability
- Design
 - Single & Common Cause Failure; Independence; Separation; Isolation; Power Supply; Calibration; Portable Instruments
- Qualification
- Display
 - Characteristics; Identification; Display Types; Recording
- Quality Assurance



DRAFT GUIDE DG-1128 (REGULATORY GUIDE 1.97, REV. 4)

- Responds to User Need Request NRR-2002-017
- Regulatory Guide 1.97, Revision 4, endorses IEEE Standard 497-2002 with exceptions and clarifications
- Intended for new nuclear power plants
- Conversion to this new method by current operating plants may be done on a comprehensive, voluntary basis
- Regulatory positions



DG-1128

REGULATORY POSITIONS

1. How might current operating plants using Rev. 2 or 3 of Reg Guide 1.97 apply the criteria
 - “The guidance provided in this standard may prove useful for operating nuclear power stations desiring to perform design modifications or design basis modifications.”
 - Licensees may be interested in converting to Rev. 4
 - IEEE Std 497-2002 provides no guidance in translating from RG 1.97 Rev. 3 to the IEEE Std 497-2002 selection criteria
 - Generally: Type A,B,C = Cat 1, Type D = Cat 2, Type E = Cat 3
 - ex.: Subcooling Margin Monitor is a Type B Cat 2 variable
 - New criteria may be more or less stringent than existing criteria
 - Partial conversions could result in an incomplete analysis
 - The draft guide recommends conversion to be comprehensive and is strictly voluntary by the licensee



DG-1128

REGULATORY POSITIONS (cont.)

2. Calibration during an accident

- IEEE Std 497-2002 requires this by means of recalibration, interval specification, equipment selection or cross-calibration
- DG-1128 reduces requirement to “extent possible.”

3. Does not address severe accidents

- IEEE Std 497-2002 requires Type C variables to have extended ranges
- DG-1128 clarifies the requirement for extended ranges based on current regulatory requirements



DG-1128 REGULATORY POSITIONS (cont.)

4. Excludes contingency actions from the scope of selecting variables
 - IEEE Std 497-2002 assumes all contingency actions are to mitigate accident conditions that are beyond the licensing basis of the plant
 - DG-1128 recommends considering all EOP actions for design basis events during the selection process, regardless of contingency or otherwise
5. Number of points of measurement
 - IEEE Std 497-2002 does not address this topic
 - DG-1128 states that the number of points of measurement should be sufficient to adequately indicate the variable value



APPROACHES CONSIDERED

1. Take no action
2. Revise Reg Guide 1.97 to incorporate approved deviations, clarifications and rule changes for current operating plants and endorse IEEE Std 497-2002 for current and new plants
3. Produce new regulatory guide 1.XXX to endorse IEEE Std 497-2002 for new plants and leave Regulatory Guide 1.97 at Rev. 3 for current plants
4. Revise Reg Guide 1.97 to endorse IEEE Std 497-2002 intended for new plants, and current plants may voluntarily and comprehensive convert to Rev. 4
 - This is the approach chosen by the staff
 - NRR and OGC have no technical or legal concerns



CONCLUSION

- DG-1128 (proposed Regulatory Guide 1.97, Rev. 4) endorses current IEEE Standard 497-2002 with exceptions and clarifications
- Consistent with NRC requirements
- SRP Chapter 7 will require updating
- Intended for new nuclear plants, with current operating plant conversion on a comprehensive, voluntary basis
- No backfit issues
- Final Comments or Questions?

Digital Systems Review



Presentation to ACRS

June 14, 2005

**Jose A. Calvo, Chief
Evangelos Marinos
Paul Loeser
Electrical and Instrumentation & Controls Branch
Division of Engineering, NRR
U. S. Nuclear Regulatory Commission**



SUMMARY OF STAFF REVIEW OF DIGITAL SYSTEMS

- **The Staff reviews the process, not the product.**
- **We depend on the licensee using a good process to develop and test the system, and, should the worst occur and the system does not work correctly, we depend on diversity and defense-in-depth.**
- **We sample portions of the product to check in greater detail during the thread audit.**



Project 3.3.2

Digital Systems Failure Assessment Methods

- **Project will survey various analytical methods of identifying system faults, assess these methods by conducting case studies, and recommend methods for NRR use.**
 - **The reason for this study is because not all failures may be safety-significant.**
- **EEIB fails to see how this will be useful to assess digital systems.**
- **This project may have been requested by some other branch or office.**



PAST DIGITAL SYSTEM REVIEWS

- **Westinghouse Eagle 21 - Completed 1993**
- **B&W Star - Completed 1995**
- **Siemens (Now Framatome) Teleperm XS - Completed 2000**
- **Westinghouse ASICS - completion 2000**
- **ABB-CE (Now Westinghouse) Common Q - completed 2000**
- **Triconex PLC - completed 2002**



CURRENT AND UPCOMING DIGITAL REVIEWS

- **HF Controls topical report on HFC 6000 - submitted November 19, 2004.**
 - **Microprocessor based digital I&C replacement system.**
 - **HFC 6000 used in Korean nuclear plants and non-nuclear applications.**

- **Oconee digital replacement of RPS and ESF with Framatome TXS**
 - **License amendment received February 16, 2005.**
 - **The first safety related use of TXS, and first use of a single system to replace all RPS and ESF safety systems.**

- **Toshiba Field Programable Gate Arrays (FPGA)**
 - **Originally Submitted in Spring of '04.**
 - **Put on hold while Toshiba prepared documentation.**

- **Framatome AV-42 Priority Logic Module - expected summer of '05**
 - **Module combines safety and non-safety signals to control safety-related equipment.**
 - **May require policy decision on combining safety and non-safety.**

- **NRC expects an additional major digital replacement from a W plant this summer.**

- **Within 2 years, NRC expects one Navy reactor, NASA reactor, and new commercial reactor submissions.**



RESEARCH PLAN

- **RES should identify in each of the proposed projects the problem to be solved, and why current guidance is not sufficient.**
- **The method we use to review digital systems is contained in the SRP.**
 - **The SRP was written by knowledgeable engineers.**
 - **The SRP was reviewed by industry, senior management, and various groups such as EPRI, IEEE and ACRS.**
- **While this may not be the perfect document, it does exist, is being used, and it works. Research should be aimed at the type of review we actually do.**



NEEDED RESEARCH

- **Housekeeping stuff - Updates to old Reg Guides endorsing new versions of standards, or new Reg Guides on new standards.**
- **State-of-the-Art stuff. Monitoring the cutting edge of what is being done in other industries or in academia.**
- **New ways to regulate. At the moment, these are primarily software related.**
 - **Requires an explicit discussion on application of this method, and how to tell if the licensee application of this method good enough.**
 - **How do we know that the method is properly applied, and that the licensee knows what he is doing? Detailed acceptance criteria is needed.**
 - **We need justification for rejection of the licensee submittal if the required quality is not present.**
 - **If RES suggests a change to regulation or methods, exact changes are needed.**
- **Most important RES & NRR working level staff must work together to ensure that the application of the digital technology in NPP's continues to be safe.**

<u>Research Project</u>	<u>Desirable to EEIB</u>	<u>Discussed with EEIB</u>
3.1.1 Environmental Stressors	No	Yes*
3.1.2 System Communications	No	Not Discussed
3.1.3 COTS Digital Systems	No	Yes*
3.1.4 Develop Models, Tools, and Methodologies to Simulate Station Blackout	No	Yes*
3.1.5 Determine the Effect of Total Harmonic Distortion on Digital Systems	No	Not Discussed
3.1.6 Operating Systems Used in Digital I&C Systems	No	Yes*
3.1.7 Investigate the Vulnerabilities of Digital I&C Systems to Determine Adequacy of D3	No	Not Discussed
3.2.1 Assessment of Software Quality	No	Yes*
3.2.2 Digital System Dependability	No	Yes*
3.2.3 Self-testing Methods	No	Yes*
3.3.1 Development and Analysis of Digital System Failure Data	No	Not Discussed
3.3.2 Digital Systems Failure Assessment Methods	No	Not Discussed
3.3.3 Model Digital Systems, Including Embedded Systems for Risk - Importance	No	Not Discussed
3.3.4 Investigation Digital System Reliability Assessment Methods	No	Yes*
3.4.1 Provide Security Assessments of Cyber Vulnerabilities	No	Not Discussed
3.4.2 Security Assessments of EM Vulnerabilities	No	Yes*
3.4.3 Wireless Network Security	No	Not Discussed
3.4.4 Firewall Security	No	Not Discussed
3.5.1 System Diagnosis, Prognosis, and On-line Monitoring	No	Not Discussed
3.5.2 Radiation-hardened Integrated Circuits	No	Yes*
3.5.3 Advanced Instrumentation and Controls	No	Not Discussed
3.5.4 Smart Transmitters	No	Not Discussed
3.5.5 Application Specific Integrated Circuits (ASICS) and Field Programmable Gate Arrays (FPGAS)	No	Yes*
3.5.6 Wireless Technology	No	Not Discussed
3.6.1 Advanced NPP Instrumentation	No	Not Discussed
3.6.2 Advanced NPP Controls	No	Not Discussed
3.6.3 Advanced NPP Digital System Risk	No	Yes*
3.7.1 Standards Development	Yes	Not Applicable
3.7.2 Maintenance of Resources and Knowledge Management	Yes	Not Applicable
3.7.3 Collaborative and Cooperative Research	Yes	Not Applicable

* Project discussed, but final version of project has not been seen, and therefore may still not meet EEIB expectations.



NRC DIGITAL SYSTEM RESEARCH PLAN

Overview of Software Quality Assurance Program

3.2

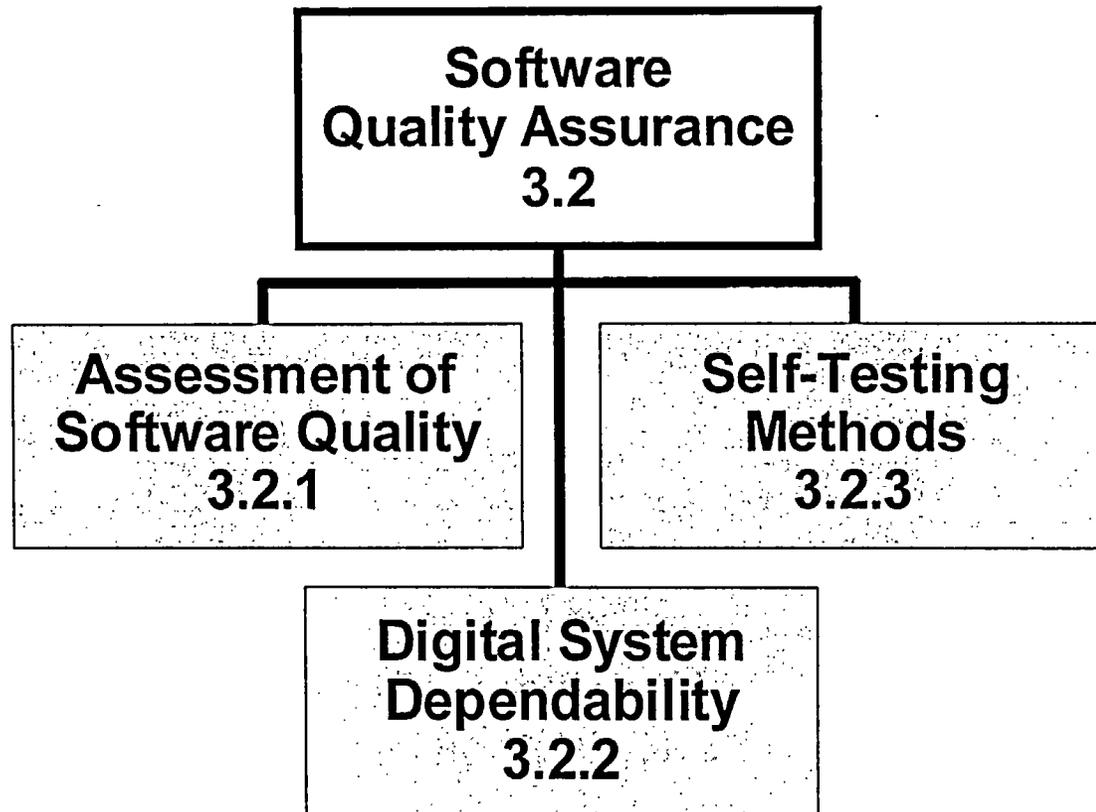
Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control subcommittee

June 14, 2005

William E. Kemper
Chief, I&C Engineering Section
Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-7585, wek@nrc.gov)



SOFTWARE QUALITY ASSURANCE PROGRAM 3.2





SOFTWARE QUALITY ASSURANCE

- NRC SRP Chapter 7, Rev. 4, June 1997 provides the regulatory framework for the review and approval of digital safety systems
- As part of its review of digital safety systems, NRC evaluates safety related software quality by reviewing
 - development processes (e.g., V&V, CM) and
 - Software development products (e.g., SRS, SDD, Test plans, Code listings, RTM)
- The SRP is adequate to provide guidance (i.e., what to review) to the staff in performing safety reviews pertaining to digital safety systems



SOFTWARE QUALITY ASSURANCE

- Review and approval of digital safety systems currently depend on qualitative evaluations of digital system features and development processes
- SQA evaluations are performed manually, without the aid of assessment tools or other means of obtaining quantitative measures of software quality
- NRC SRP Chapter 7 BTP HICB-14 identifies digital system development attributes that should be reviewed, but does not provide detailed guidance on the process for confirming that the software conforms to the acceptance criteria



SOFTWARE QUALITY ASSURANCE

- NRC reviews the results of software development processes and safety assessments, but the reviews do not include a means for independent assessments of software products
- Given the complexity and sophistication of current digital safety systems, **the goal of this Research Program is to provide independent assessment methods and objective acceptance criteria that can supplement and augment the existing guidance in Chapter 7 of the SRP**
- This information can be provided as formal review procedures for verifying consistency with SRP Guidelines, which could improve effectiveness and consistency of SQA reviews



SOFTWARE QUALITY ASSURANCE

- The current state-of-the-art in software system safety assessment includes a number of methods and tools for quantitatively assessing the quality of software:
 - Software system analysis techniques (e.g., Petri-net analysis, Markov Analysis, Dynamic Flow Modeling)
 - Software metrics
 - Formal verification methods
 - Testing Techniques (e.g., Data Flow Testing, Fault Injection, and Mutation Testing)



SOFTWARE QUALITY ASSURANCE RESEARCH FOCUS

- Research in this area will focus on assessing possible analysis methods that are currently used in design and analysis of safety critical software systems for use in the regulatory process
- Will focus on methods that have likely short term application without the need to do extensive development and apply these to nuclear industry applications
 - Fault injection testing has been used by a number of industries including some nuclear platform suppliers
 - Formal methods have been used in several industries to support safety critical applications
 - Software metrics are currently used for software quality control and continuous improvement (e.g., for programs at CMM level 4 and 5 respectively)



SOFTWARE QUALITY ASSURANCE SUMMARY

- This research area currently focuses on three initiatives to develop independent methods for assessing software quality and/or reliability
 - The use of Software Metrics to evaluate quality
 - The use of Fault Injection Techniques to evaluate digital system dependability
 - Technical guidance and review procedures for evaluating self-testing features in digital systems
- These research projects will provide objective acceptance criteria and review procedures that augment and supplement existing SRP guidance for approving (or denying) digital safety system license applications



3.2.1

ASSESSMENT OF SOFTWARE QUALITY

Norbert N. Carte
Steven A. Arndt
I&C Engineering Section
Office of Nuclear Regulatory Research
(301-415-5890, nnc@nrc.gov)
(301-415-6502, saa@nrc.gov)

Ming Li
University of Maryland
Center for Reliability Engineering
College Park, MD 20705
(301-405 1705, mli@wam.umd.edu)



OVERVIEW

(3.2.1 Assessment of SW Quality)

- Issues Facing NRC
- Current Research
- Future Work
- Conclusions



Issues Facing NRC

(Increasing Size and Complexity of Submittals)

- SW is Being Used in More Systems
- Increase in Use of Self Checking SW and Other Techniques Result in More Complex Systems
- More Powerful Development Environments
 - SW Programming is Becoming more Abstract
 - More Details are Hidden
- SW Engineering Methods are becoming more Powerful and Usable



Current Review Processes

(SRP Rev. 4 - June 1997)

- SW Development Process Review
 - Sample Thread Audits (Selected by Reviewer)
 - Manual
- Generic Plan
 - Requires Application Specific Review Plan
- Different Programming Paradigms
 - SP (i.e. C), OO (i.e. C++), & PLC (i.e. Function Block)
- Reg. Guides Endorse Generic IEEE Stds
 - The 3 SERs are for PLCs
- Does Not Address Use of Measures



Current Research Goals

The objective of this research is to perform a large scale validation of measures, identified previously, to quantitatively assess the quality of software.

- Quantifiable SW Quality Assessment
 - Incorporation of Measures
 - Standardized Quantifiable Evaluations
 - Objective Acceptance Criteria
 - Theoretical,
 - Benchmarked against Current Methodology, or
 - Benchmarked Theoretically
- Flexible
 - Useable by Licensee, NRC, and/or Both
 - Compare/Combine Different Assessments
 - Probability/Confidence Goals are Met (i.e. Bayesian), or
 - Normalized Quality Assessment (i.e. Defect Density or Reliability)
- Address Issues Raised Previously



Current Research

(Basis - Quantifying SW Quality)

- Large Body of Literature on Metrics (Both Technical & Managerial)
 - IEEE 982.1 Dictionary of Measures To Produce Reliable SW
 - IEEE 982.2 Guide for the Use of 982.1
 - IEEE 1061 Software Quality Metrics Methodology
 - “... the use of software metrics does not eliminate the need for human judgment in software evaluations. The use of software metrics within an organization or project is expected to have a beneficial effect by making the software quality more visible.”
 - IEEE 1045 Software Productivity Metrics
- Lawrence Livermore National Laboratory
 - Identified Pool of 78 Measures
- University of Maryland
 - Selected 30 Measures
 - Categorize Measures
 - Life-cycle Phase (i.e. Design, Test, ...), & Semantic Family (i.e. Size, Complexity, ...)
 - Breadth – Cover all Areas of Interest
 - Elicitation of Expert Opinion to Rank Measures & Families
 - Peer Review of Research Performed
 - Publication in peer Reviewed Journals
 - Preliminary Validation - NUREG/CR-6848



Large Scale Validation

- Use a Sample of Measures for Validation
 - Ranking for use in Predicting Proper System Operation
 - Class of Measures
 - High Ranked Measures
 - Cyclomatic Complexity, Mean Time to Failure, Defect Density, & Coverage Factor
 - Medium Ranked Measures
 - CMM, Fault Days Number, Requirements Specification Change Requests, Requirements Traceability, & Test Coverage
 - Low Ranked Measure
 - Function Points, Bugs per Line of Code, Cause & Effect Graphing, & Mutation Testing
 - Family
 - Functional Size (i.e. Feature Point, Function Point, & Full Function Point)
 - Complexity (i.e. Cyclomatic Complexity)
- All Phases of SW Development
- Nuclear RPS (Safety System)



Large Scale Validation (Issues Raised Previously)

- NUREG/CR-6848
 - Peer Review
 - Relatively Small SW Application
 - Application Not a Nuclear Safety System
 - Benchmark of Measures did not use real Operational Profile
 - Looked at only one Phase of SW Development
 - Looked at a low Reliability System
- ACRS
 - Ease of Obtaining Metric
 - Ease of Use Evaluation will be Included in Final Report
 - SW Centric vs. System Approach
 - Uncertainty Greater than Required Reliability
 - Issue Not Visible in a Qualitative Evaluation Process
 - Measures “ ... do not eliminate the need for human judgment ...”
 - Validity / Robustness of Measures
 - Different Types of Functions (RPS vs. Door Entry)
 - Different Programming Languages (C & Assembler vs. C++)



Measures for Assessing SW Quality

- Goal
 - Quantify SW Quality through SW engineering measurement
- Philosophy
 - SW Quality is determined by:
 - Software product characteristics (number of defects)
 - Project characteristics
(application type, application's functional size, etc)
 - Process characteristics
(personnel skill, budget, development method, tools, etc.)
 - How software is used (operational profile)
- Steps:
 - Estimate the number of defects remaining in the SW
 - Quantify the likelihood that these defects result in System Failures



Defect Density

- Defect Density (DD) Definition
 - A ratio of unique defects found by inspections (requirements, design and code) to the size of the product.
 - Defects are classified into different criticality levels.
 - The product can be either requirements/design document or source code
- Research on Defect Density
 - Included in IEEE Standard 982.2 “IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software”
 - A *de facto* standard measure of software quality [Fenton].
 - Quality indicator: Grady 1987, *IEEE Software*
 - Quality indicator: Mohagheghi, 2004, ICSE
 - Module size vs DD: Malaiya 2000, ISSRE
 - etc.



Defect Density

- Number of Known Defects
 - # of defects = $DD * Size$
- Number of Latent Defects
 - Capture/Recapture (CR) models: were initially developed to estimate the size of an animal population.
 - The use of CR models in software inspection
 - # of defects ~ Animal population size
 - Inspectors ~ Traps
 - Error discovery ~ Animal trapped and marked



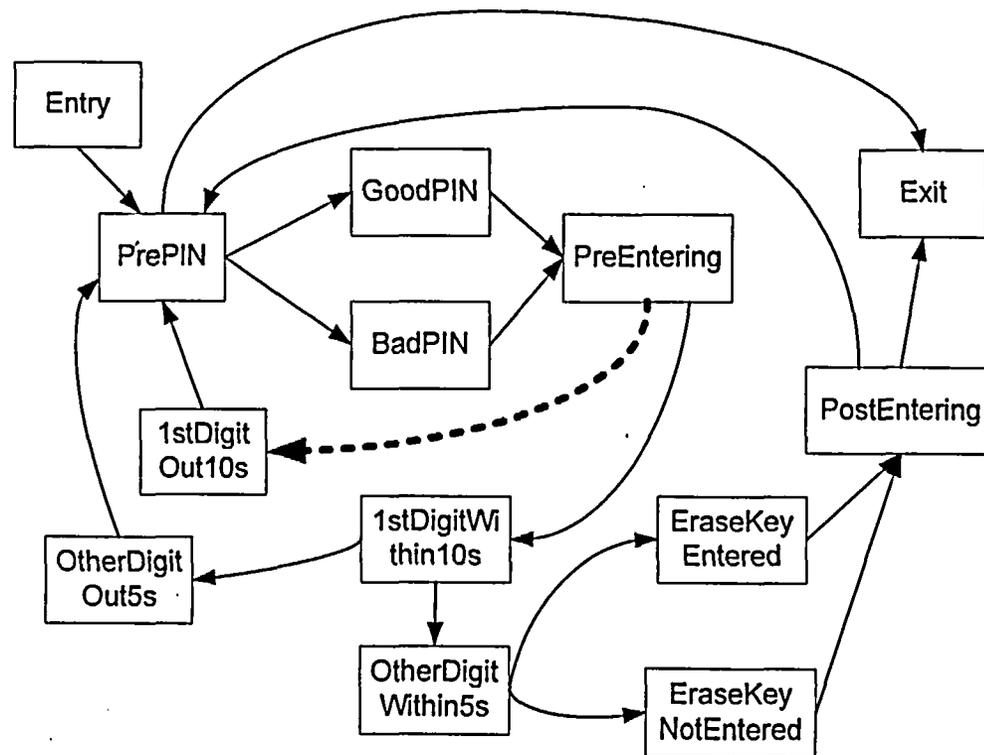
System Failure Estimation

- From Defect to Failure
 - E: probability that a particular section of a program (termed “location”) is executed.
 - I: probability that the execution of a problematic location (defect) affects the data state.
 - P: probability that an infection of the data state affects system output.
- DD RePS
 - The probability of failure per demand is given by:



Estimation of Impact of Defect Density to an Example System

- Quantification (Defect Propagation)
 - Finite State Machine Model (FSM)
 - An Example





Test Coverage (Statement)

- Test Coverage (TC) Definition
 - The portion of SW statements executed against a set of test cases.
- Research on Test Coverage
 - Included in IEEE Standard 982.2 “IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software”
 - Widely accepted in industry to control testing process:
 - Fenton, Pfleeger, 1997, PWS Publishing
 - Briand, Pfahl, 2000, *IEEE Transactions on Reliability*
 - # of defects vs. TC: Malaiya 1994, ISSRE.



Test Coverage

- Test Coverage vs. Number of Defects
 - Derive the number of defects remaining from the number of defects found in testing.

C_0 : defect coverage

C_1 : statement coverage

a_0, a_1, a_2 : coefficients

N : number of defects remaining

N_0 : number of defects found in testing



Test Coverage

- Number of Defects and Impact on System Operation
 - K : fault exposure ratio obtained using the finite state machine model.



Current Project Status

	<u>Completion Date</u>
• Measurement in Progress	
– Completeness	June 22
– Requirements Traceability	July 7
– Requirements Spec. Change Request	July 8
– Test Coverage	July 15
– Coverage Factor	July 31
– Fault Days Number	August 15
– Defect Density	August 31
• Analysis in Progress	
– Operational Profile	July 15
– Finite State Machine	August 15
– Testing	August 15
– Calculations & Comparisons	September 30



Current Project Status

(Preliminary Results)

- Measurement Completed (No. of Defects Predicted)
 - High Ranked Measures
 - Cyclomatic Complexity (210.37)
 - Medium Ranked Measures
 - CMM (4.58)
 - Low Ranked Measures
 - Function Point (8.0)
 - Bugs per LOC (590)
 - Cause Effect Graphing (5)



Future Work

- Large Scale Validation
 - Develop Regulatory Guidance
 - Acceptability of Methods
 - Acceptance Criteria
 - Benchmark
 - Other Industries
 - Training on Usable Measures
- Coordinate Subsequent Research with NRR
 - Validate & Train on Additional Measures
 - Technology Specific Measures (i.e. PLC)



Conclusions

- SW Engineering Measures are Sufficiently Mature for use in Assessing SW Quality in Safety Related Nuclear Applications
- Measures of SW Quality are Related to Proper System Operation
 - This large scale validation project provides a promising methodology for estimating the impact of SW quality on proper system operation.



DIGITAL SYSTEM DEPENDABILITY (3.2.2)

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Sub-committee Meeting

June 14, 2005

Roman Shaffer and Steven Arndt

Engineering Research Application Branch

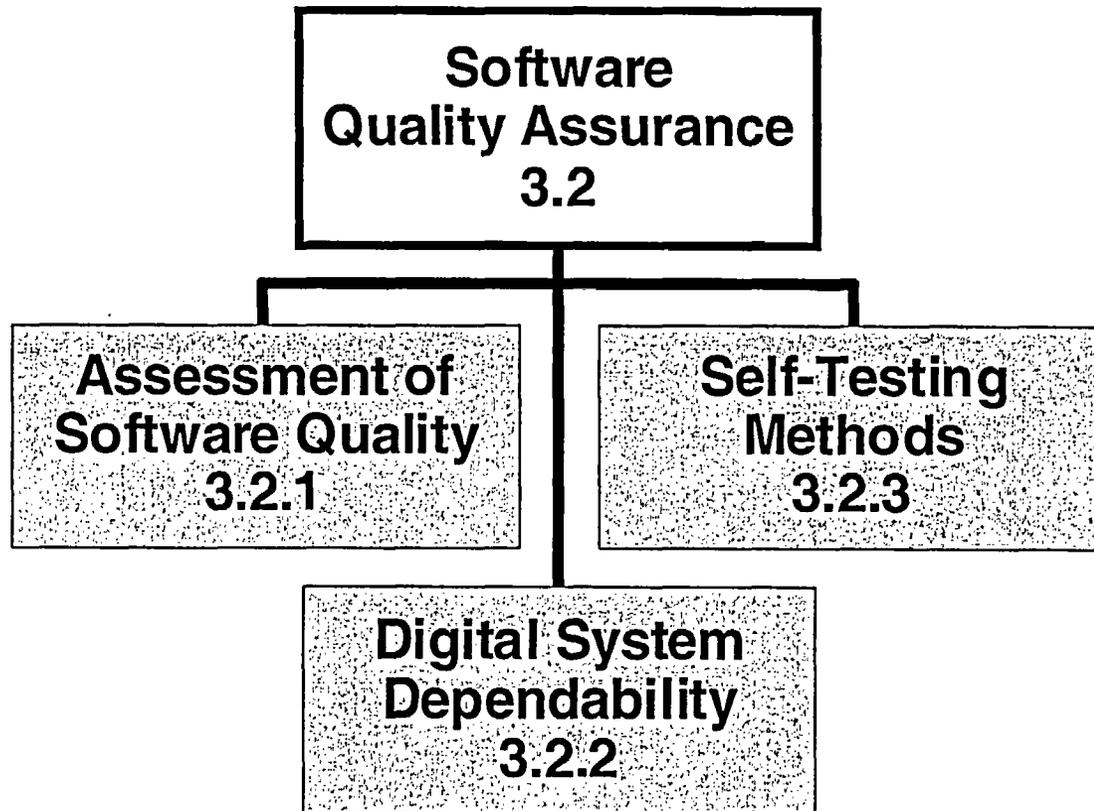
Division of Engineering Technology

Office of Nuclear Regulatory Research

(301-415-7606, ras3@nrc.gov, 301-415-6502, saa@nrc.gov)



SOFTWARE QUALITY ASSURANCE PROGRAM 3.2





SOFTWARE QUALITY ASSURANCE

- The current state-of-the-art in software system safety assessment includes testing techniques such as fault injection testing that permits analysis of the systems under review
- Information obtained as part of testing can support software system analysis techniques (Petri-net analysis, Markov, DFM, etc)
- Methods can be use to Characterize the behavior of digital systems



3.2.2 DIGITAL SYSTEM DEPENDABILITY: OVERVIEW

- GOALS
- MOTIVATION
- CONCEPTS
- PROCESS
- PROJECTS
- CONCLUSION



3.2.2 DIGITAL SYSTEM DEPENDABILITY: GOALS

- Support acceptability decision-making pertaining to digital system safety
- Refine the technical basis for digital systems to obtain objective acceptance criteria
- Augment and supplement current process with modeling/analysis methodology and tools that are not technology dependent



3.2.2 DIGITAL SYSTEM DEPENDABILITY: GOALS, cont.

- Understand behavior of hardware/software systems
 - Under the influence of internal and external faults
 - Analyze any consequent errors that might produce system failures
- Properly characterize and analyze systems for:
 - Performance
 - Reliability/Availability
 - Failure modes
 - Subsystem and system safety
 - Integration into PRAs

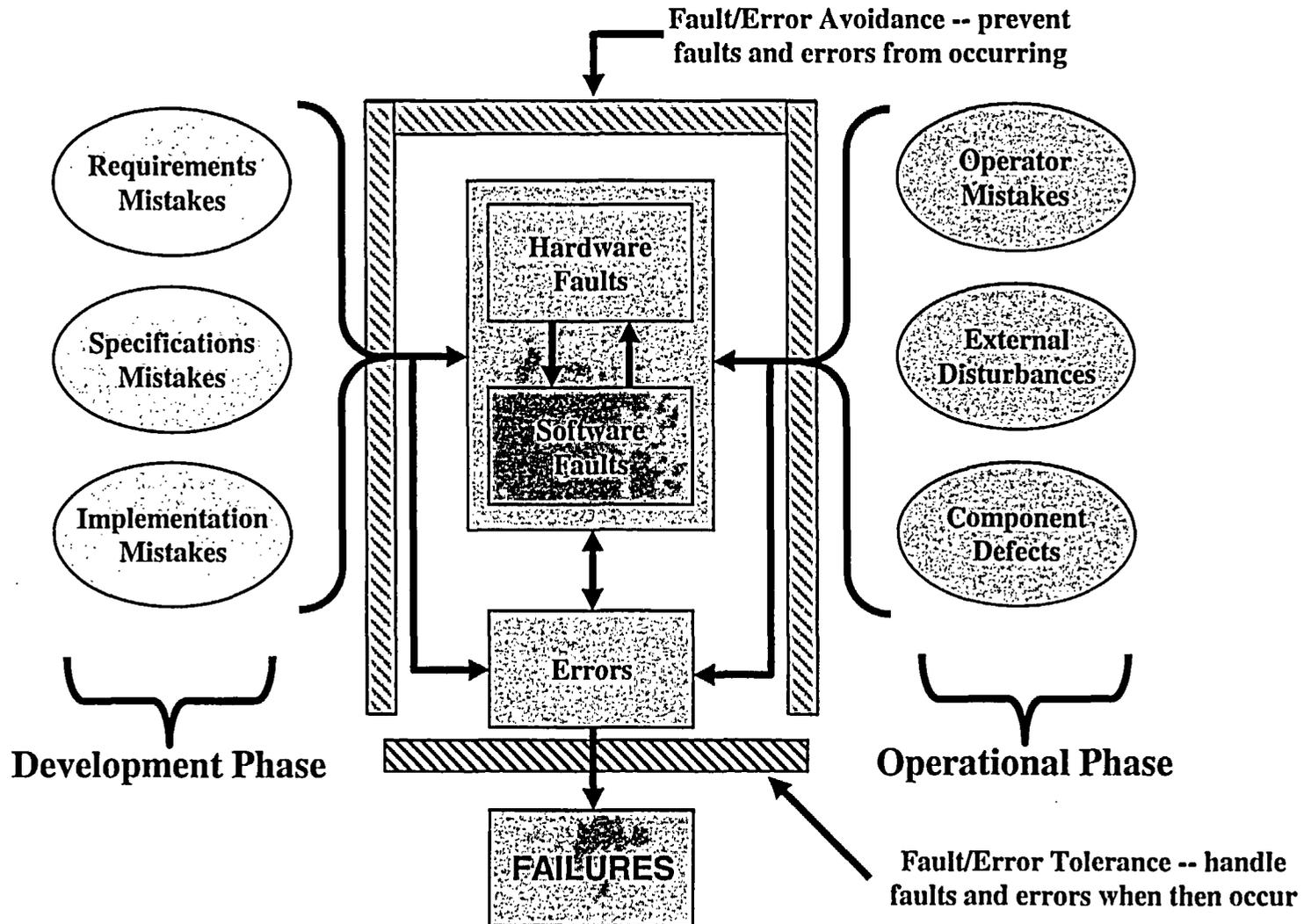


3.2.2 DIGITAL SYSTEM DEPENDABILITY: MOTIVATION

- Data and experience indicate that:
 - Software in digital systems can have severe design defects even after V&V
 - There is a greater reliance on software-based systems
 - Digital hardware components can have design and random defects
 - The interaction of hardware and software defects can cause a new class of defects
- Understanding of defects
 - How frequent are defects triggered?
 - How critical are the defect on the system?
 - What are the practical methods for determining their risk?

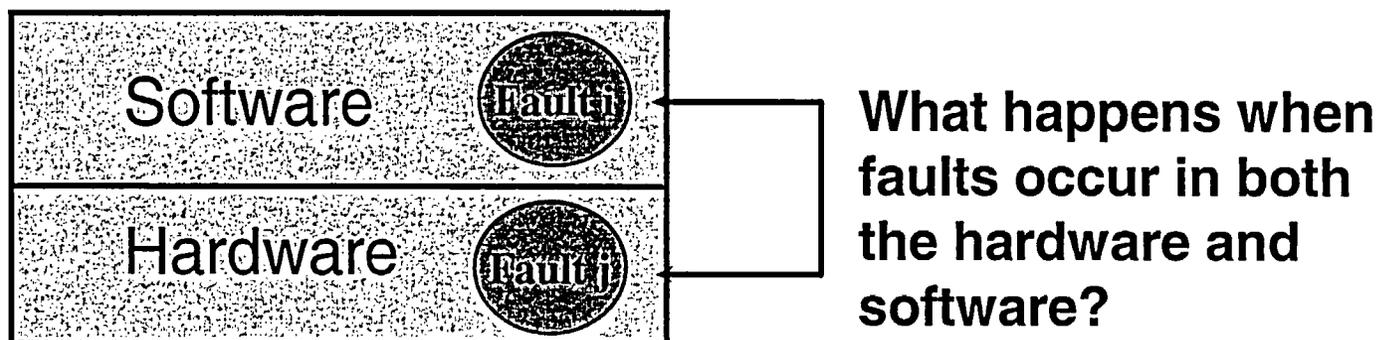


3.2.2 DIGITAL SYSTEM DEPENDABILITY MOTIVATION, cont.





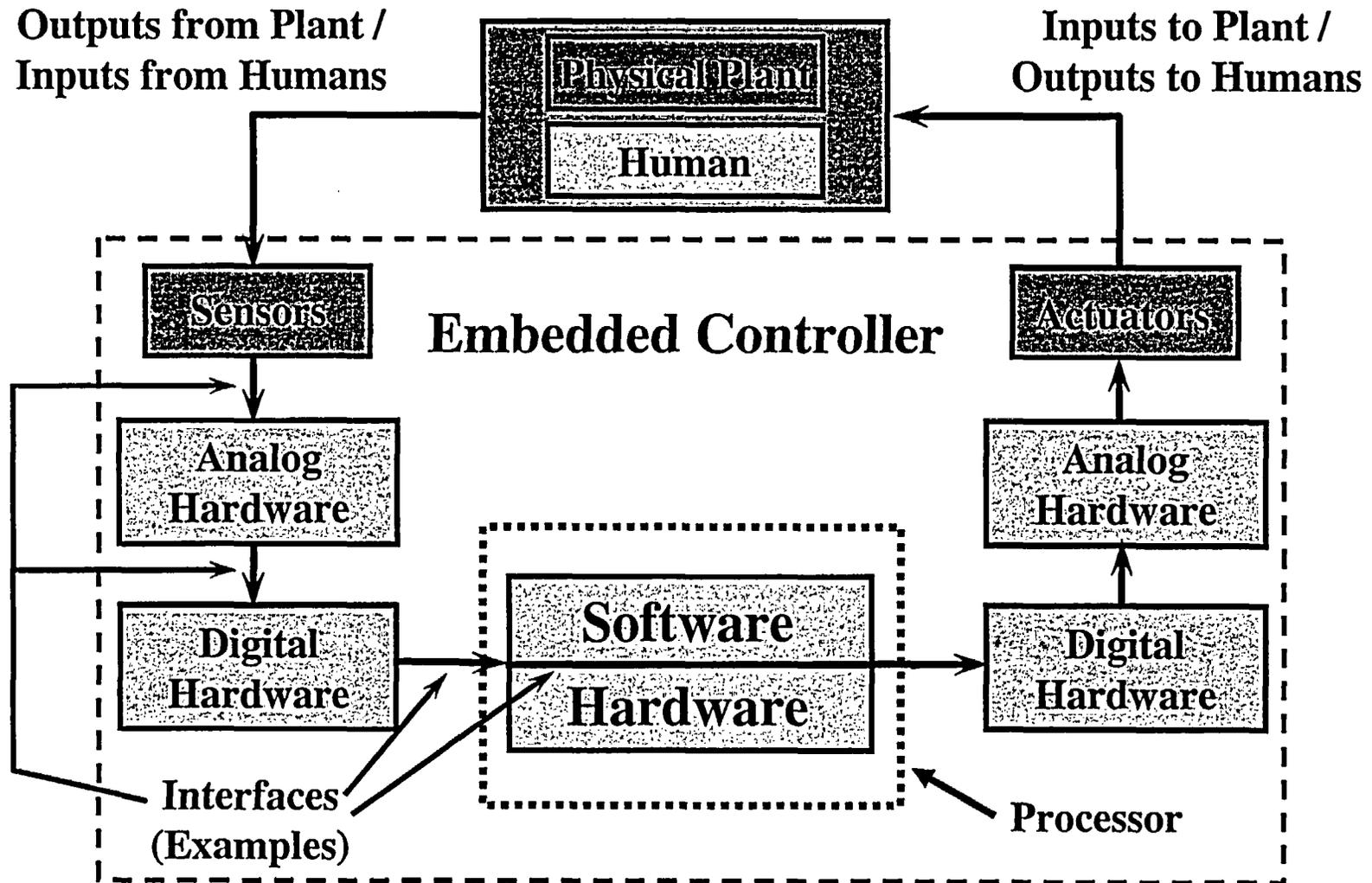
3.2.2 DIGITAL SYSTEM DEPENDABILITY MOTIVATION, cont.



- Software must execute on a hardware platform. The operation of the integrated hardware/software system is critical.
- A fault in software (Fault i) in combination with a fault in hardware (Fault j) could result in unsafe conditions and/or unreliable operation.
- Much of the software in safety-critical systems is designed to handle fault detection, fault location, fault isolation, and fault recovery. Such software may not be exercised sufficiently.



3.2.2 DIGITAL SYSTEM DEPENDABILITY: MOTIVATION, cont.





3.2.2 DIGITAL SYSTEM DEPENDABILITY: CONCEPTS

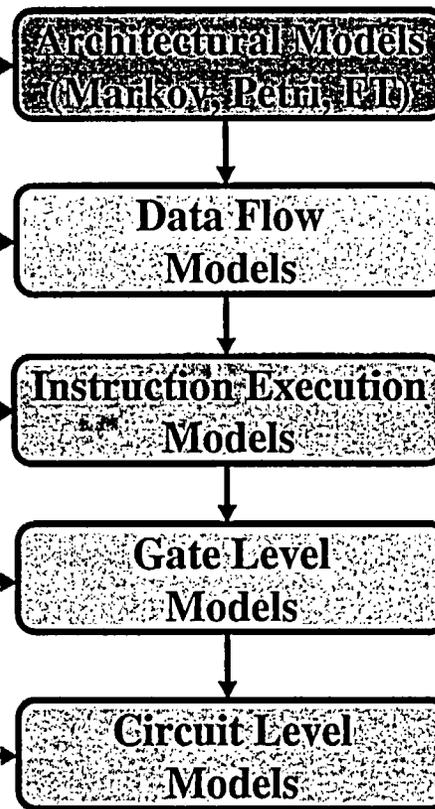
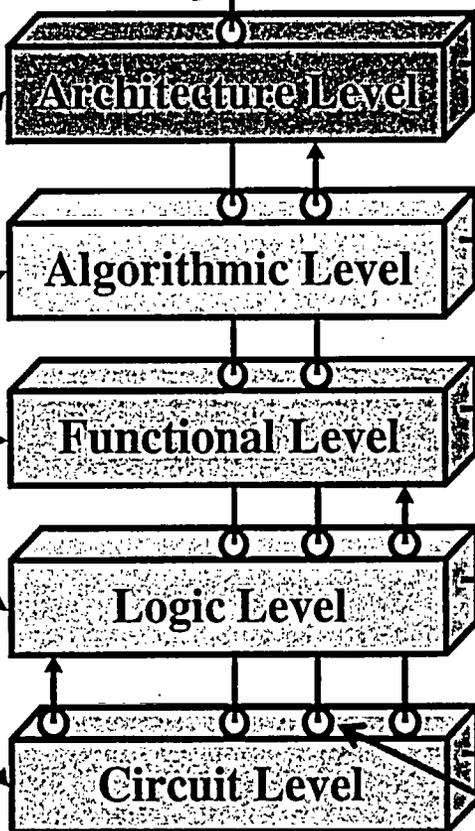
Faults that defeat all layers yield system failure

System Failure

Layers of Design and Protection

Layers of Modeling

Possible Design Faults



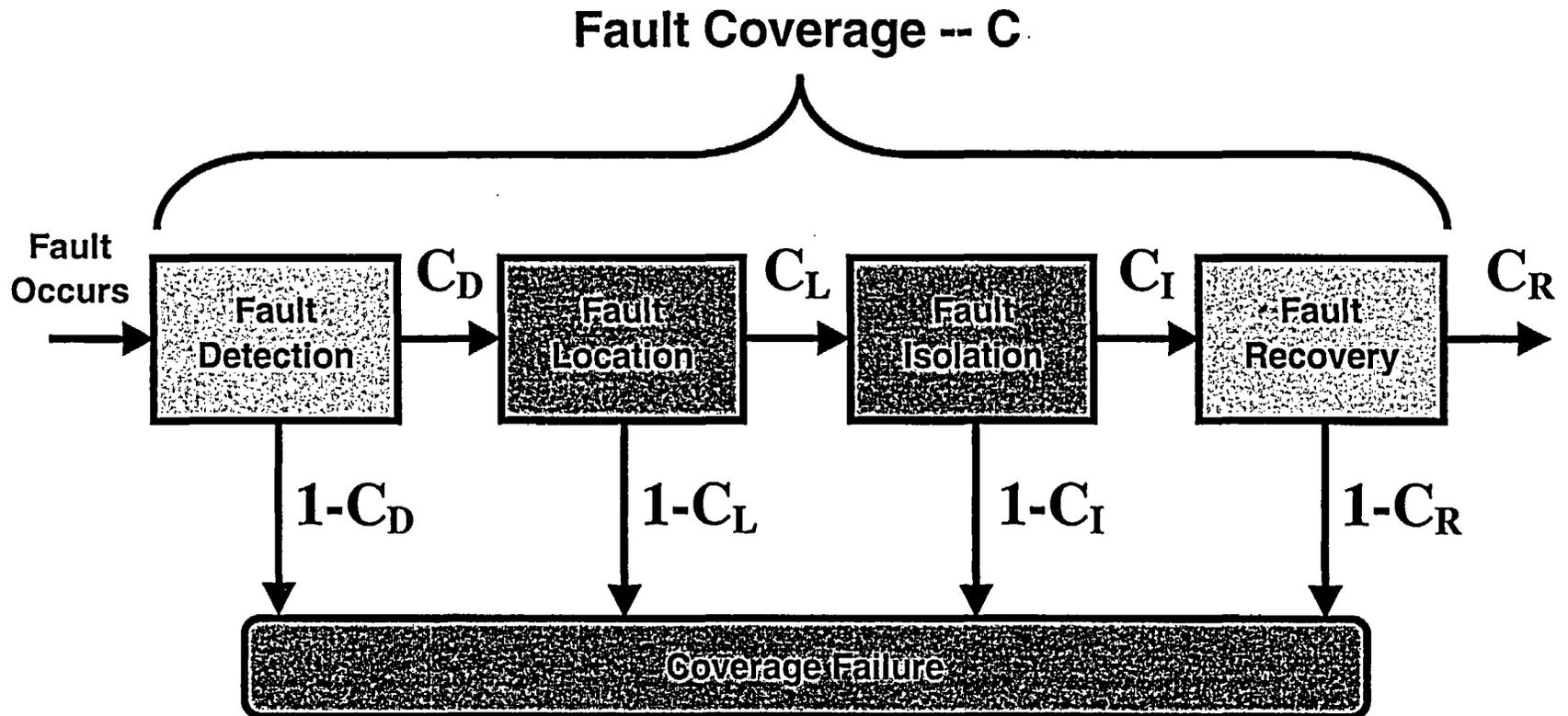
Parameter Estimates

Possible Physical Faults

Faults defeat certain layers of protection



3.2.2 DIGITAL SYSTEM DEPENDABILITY: CONCEPTS, cont.



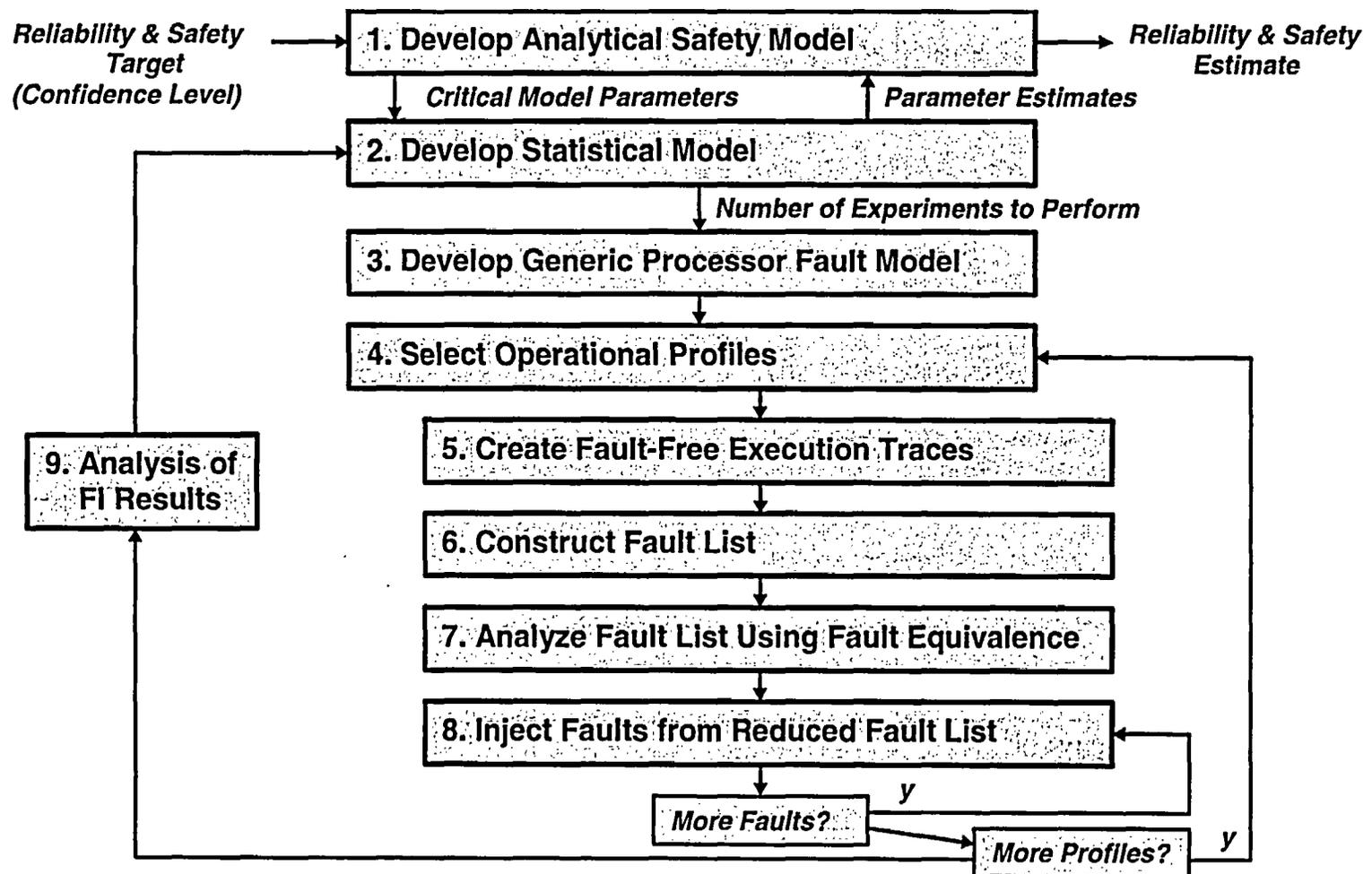


3.2.2 DIGITAL SYSTEM DEPENDABILITY: CONCEPTS, cont.

- **Digital reliability assessment methods**
 - **Several reliability assessment methods have been used by other industries and show potential for use in the nuclear industry**
 - **The Digital System Dependability research will undertake several case studies of nuclear-qualified digital systems**
 - **Achieve better understanding of failure behavior**
 - **Diverse applications of the methodology**
 - **Criteria for their proper use will be developed in order to supplement and augment the current regulatory process**

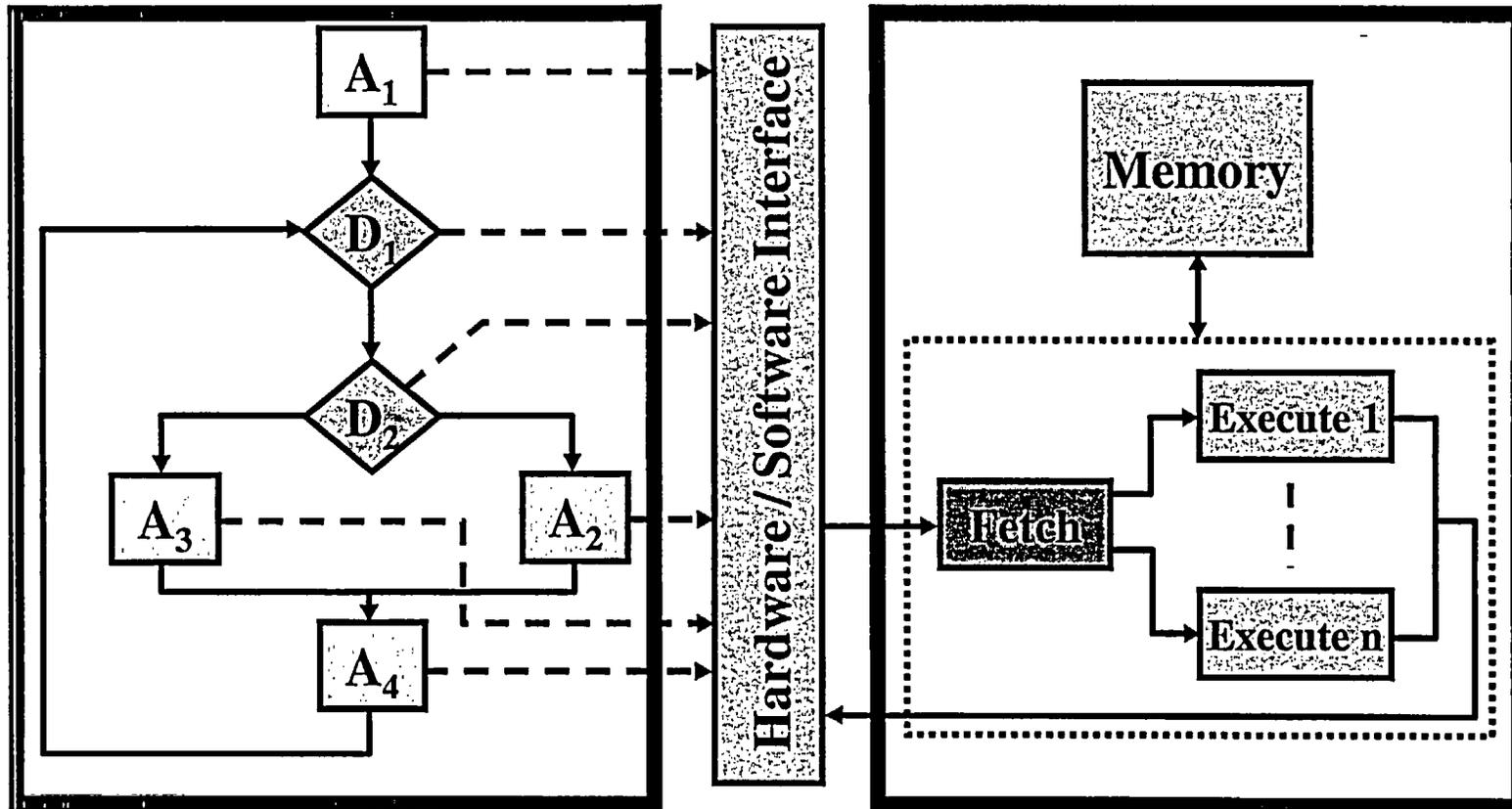


3.2.2 DIGITAL SYSTEM DEPENDABILITY: PROCESS





3.2.2 DIGITAL SYSTEM DEPENDABILITY: PROCESS, cont.



Software Model

- Data Flow
- Actual Code

Hardware Model

- Execution Model
- Gate-level Model



Analytical Model

- The analytical safety model provides the mathematical framework for calculating Reliability and/or Safety estimates
- Represents the faulty behavior of the system under analysis
- Several suitable analytical modeling techniques available from the literature
- Critical model parameter of interest is Coverage

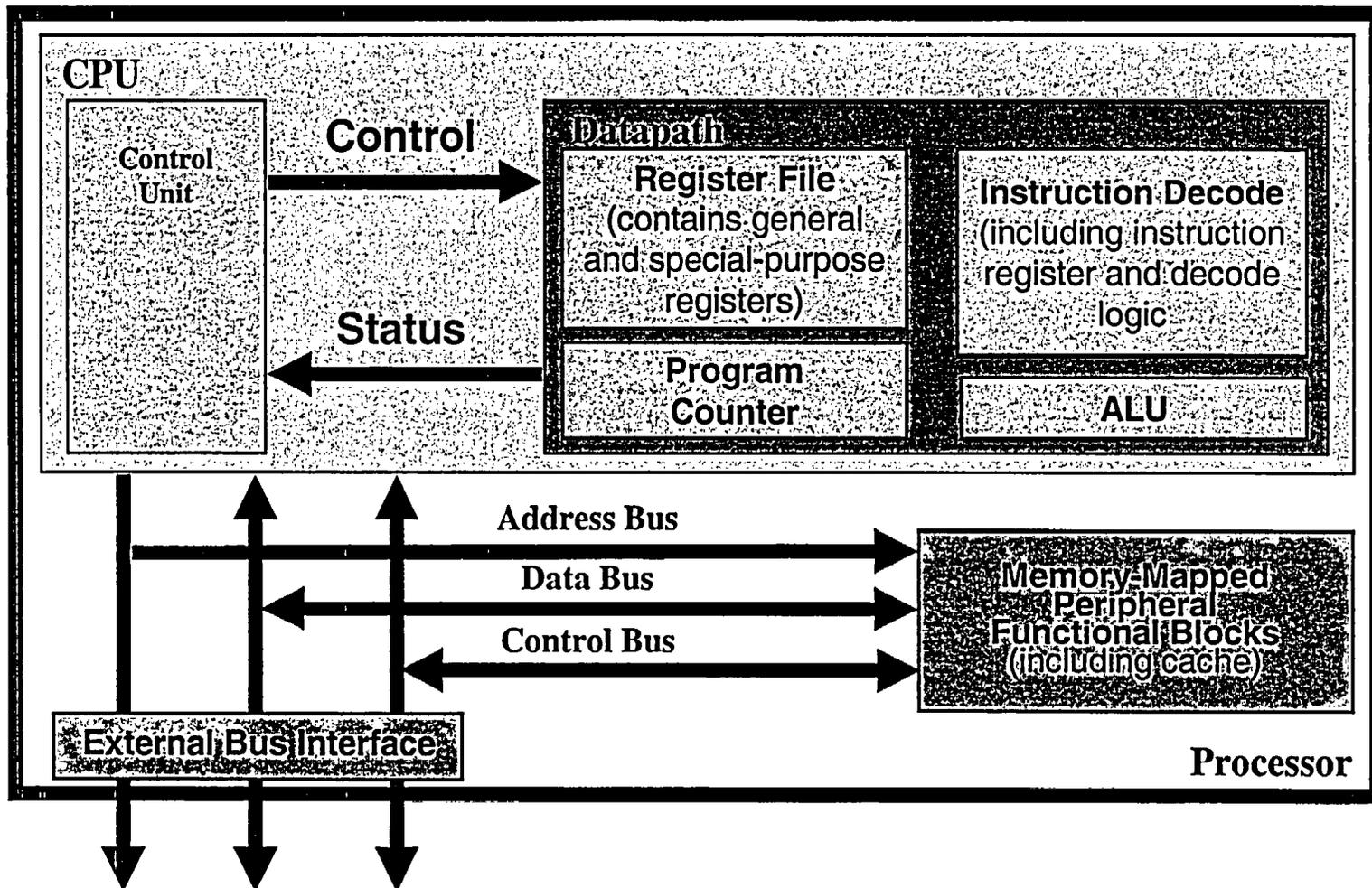


Statistical Model

- The statistical model is used to estimate the critical model parameters required by the analytical model
- Several statistical models from the literature can be used to estimate critical model parameters
- The statistical model is also used to determine the number of fault injection experiments necessary to achieve the desired confidence levels of the parameter estimates



Generic Processor Fault Model, cont.





Operational Profiles

- Operational profiles to be used in the experiments must be representative of the system under various modes of operation and configuration
 - light workloads
 - heavy workloads
- Transient and permanent faults have different activation characteristics under different workloads

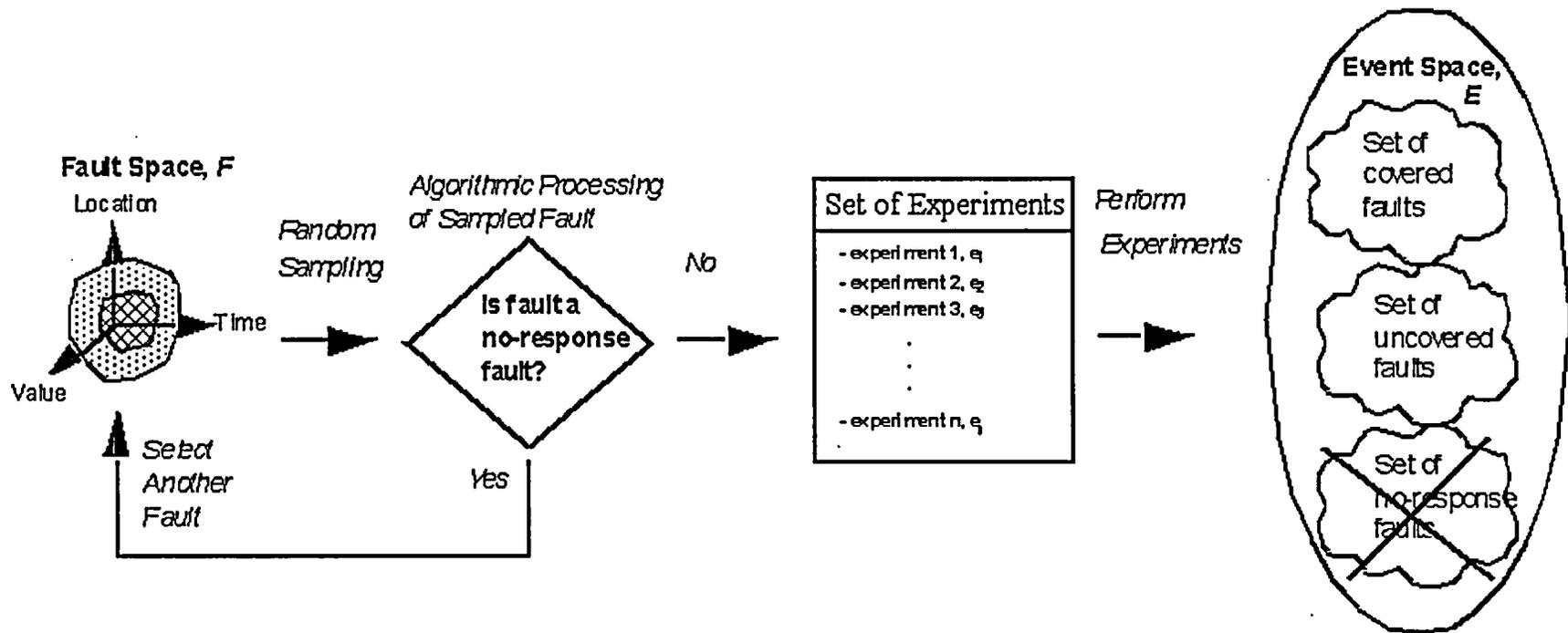


Fault-free execution traces

- For each operational profile selected, a fault-free execution trace must be created
- Trace contains sequence of instructions as well as state information that is visible
- Experimental environment is used to generate trace using Logic analyzers, Bus analyzers, In-circuit emulators, and Software debuggers
- Effectiveness of the fault list generation and analysis efforts depends on amount of detail in fault-free execution trace

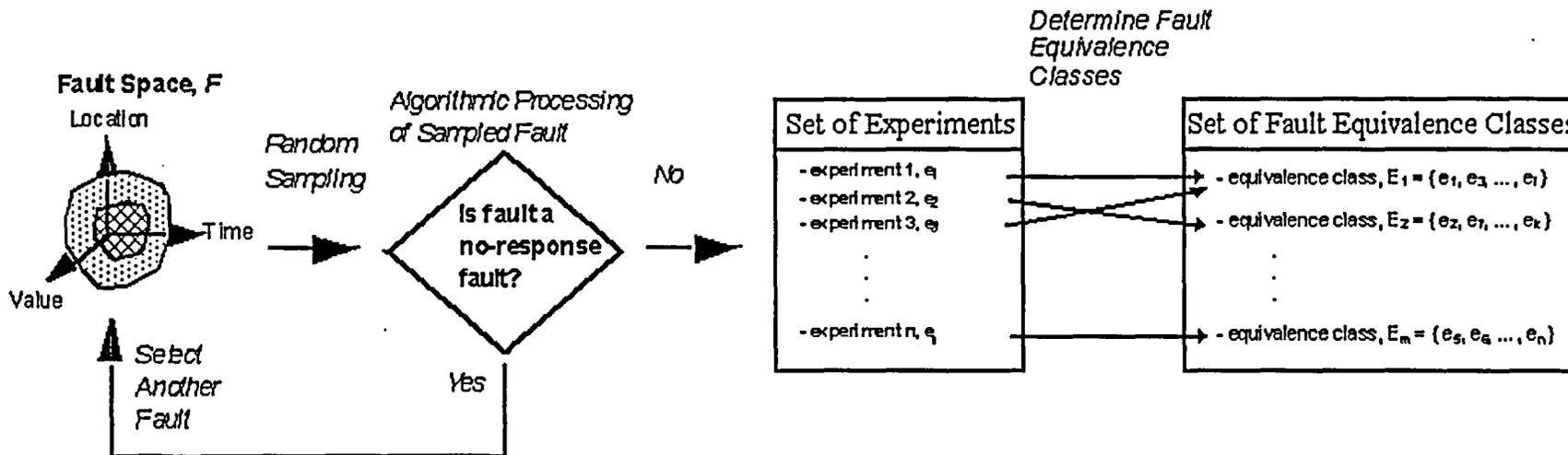


Fault list construction





Fault Equivalence





Fault-Injection Methods

- Hardware-based fault injection
 - Augment system with fault injection hardware to allow injections at pin-level (or sometimes internal to processor)
- Software-based fault injection
 - System software is modified in order to provide the capability to modify the system state (processor registers and memory) according to programmer's model
- Simulation-based fault injection
 - Construct a simulation model, including detailed model of processor
- Hybrid approaches
 - Combinations of above three approaches



3.2.2 DIGITAL SYSTEM DEPENDABILITY: RESEARCH PROJECTS

- Digital Feedwater Control System assessment, continuing under cooperative agreement with OSU
- Digital System Dependability Performance
 - Kick-off end of FY05
 - Multi-year effort
- Future effort will explore other dependability metrics (i.e., maintainability, confidentiality, integrity)



3.2.2 DIGITAL SYSTEM DEPENDABILITY: RESEARCH PROJECTS, cont.

- Digital System Dependability Performance
 - Work with vendors and licensees to
 - Obtain access to safety systems
 - Obtain engineering support on determine relevant design details
 - Perform fault-injection testing following the process described earlier
 - Approximately 12 months per system evaluation



3.2.2 DIGITAL SYSTEM DEPENDABILITY: CONCLUSION

- The Digital System Dependability research will augment and supplement the current regulatory process by:
 - Characterizing significant hardware, software and interface errors;
 - Understanding potential new failure modes and the criteria for detecting these failure modes;
 - Identifying or developing methods and data that enable the NRC to establish the risk of digital safety systems; and
 - Modeling of digital systems that could be used to provide system reliability metrics.



SELF-TEST METHODS PROJECT 3.2.3

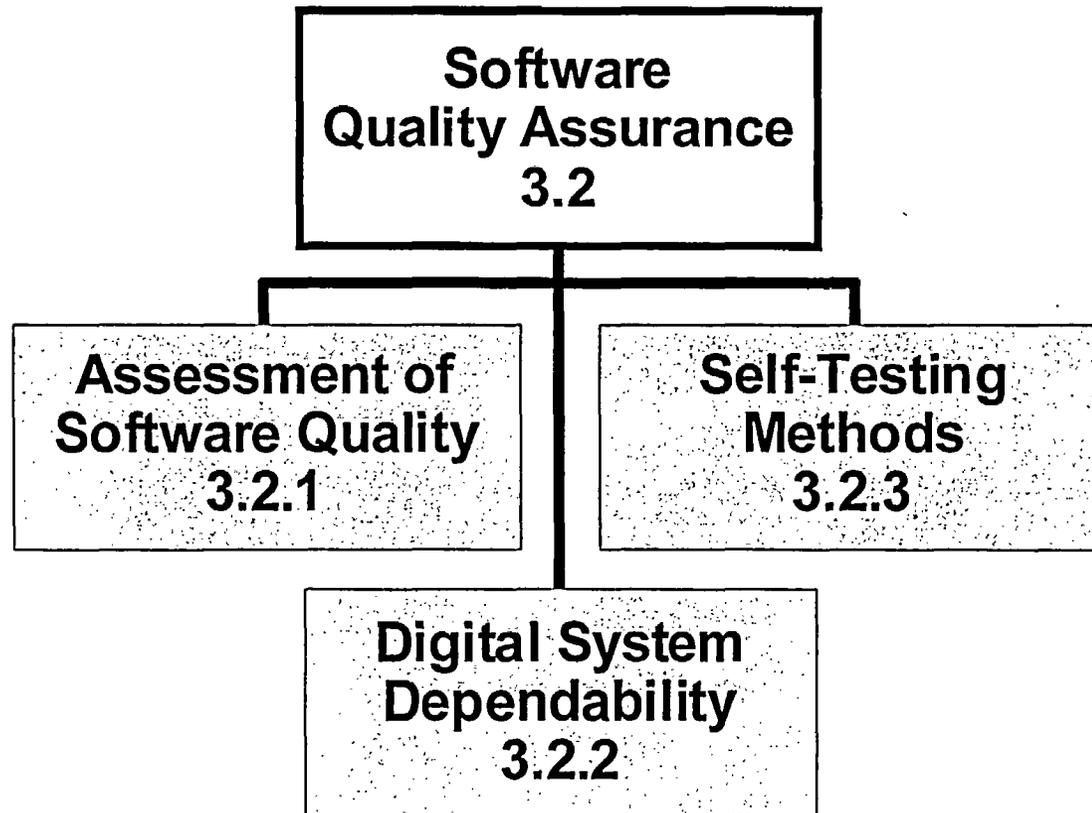
Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 14, 2005

Steven A. Arndt
Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)



SOFTWARE QUALITY ASSURANCE PROGRAM 3.2





OVERVIEW

- Self-testing methods test hardware and software on a continuous basis to improve system availability
- Because of the power of the systems has dramatically increased over the few years the overhead associated with self-testing methods are less of a concern
- Self-testing is used in basic acceptance tests as well as a number of fault tolerant applications including recovery blocks, N-version programming, etc.
- There is no consensus as to how to trade increased availability associated with self-testing versus the negative effects of increase code size and complexity



CURRENT SITUATION

- Currently NRC reviews of digital safety systems focus on safety function of the digital system
- Only limited focus is placed on interaction of self-testing features with safety functions
- Staff resource and time constraints during reviews limit the amount of time that can be spent on self-testing features



Self-testing Methods Research Program

- Technical issues concern
 - Effectiveness in determining system performance
 - Adverse effects on safety system performance
 - Identifying acceptable self-testing methods
 - The amount of self-testing that is sufficient
- This research project will develop technical guidance and review methodologies for evaluating self-test features in digital systems



SUMMARY

- This research will provide technical guidance regarding the use and review of self-testing features in digital systems
 - The effect of self-test methods on system performance
 - Characteristics of self-testing methods that might have adverse effects on safety systems performance
 - Develop information that will permit assessment of the most appropriate amount of self-testing
- Answer the questions
 - How much self-testing is enough, how much is too much
 - What kind is appropriate for real-time safety-critical and what kind is not appropriate



OVERVIEW OF RISK ASSESSMENT OF DIGITAL SYSTEMS PROGRAM 3.3

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 14, 2005

Steven A. Arndt
Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)



OVERVIEW

- NRC PRA Policy Statement
- Research is oriented toward improving NRC knowledge and providing more consistent processes for regulating digital system applications
 - Gathering, understanding and using failure data
 - Assessing what modeling methods might be usable
 - Determining which systems need to be modeled and at what level of detail
 - Developing and testing methods
 - Developing regulatory acceptance criteria



CURRENT SITUATION

- Issues facing NRC
 - Licensees are replacing analog systems with digital systems
 - Licensing these digital systems presents challenges to NRC
 - Some of the current licensing criteria (BTP-19) are difficult to meet
 - Industry has expressed interest in using risk-informed regulation (Regulatory Guide 1.174) as an alternate method for licensing these systems
 - Research into the limitations of digital systems reliability modeling to support the needed analysis does not currently support expanded use of risk information in licensing digital systems
 - As the NRC licensees replace analog systems with digital systems the current PRA's are not keeping up with these changes
 - NRC risk analysis tools and data (SAPHIRE and SPAR models) do not provide an independent means of assessing licensee analyses at present



ACRS Comments 6/9/2004

- In additional comments to the June 9, 2004, ACRS letter, Prof. George Apostolakis recommended that:
 - Databases containing software-induced failures should be reviewed and their conclusions should be used
 - Available methods for assessment of reliability of systems that are software driven should be reviewed critically



Digital System Risk Program

- **The research program is designed to use available information, including failure data and known capabilities of available methods to develop the needed outcomes**
- **Available methods and tools for including digital system models will be reviewed and the most promising ones will be investigated**
- **Review of current data and development of application-specific databases will be completed**



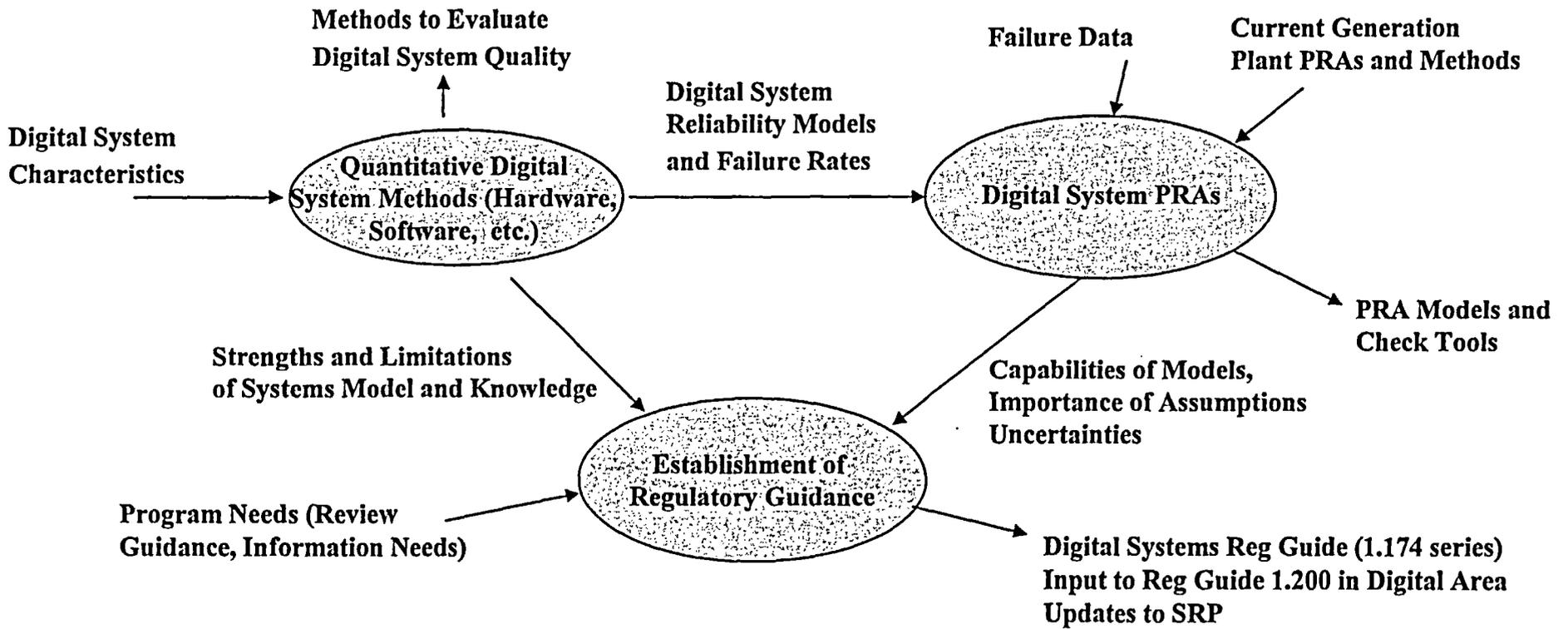
Digital System Risk Program

- **New methods for integrating current digital system models into PRAs will be developed**
 - Pilot methods using both traditional methods and dynamic methods using models
 - Benchmarks of the capabilities of several methods will be completed
 - Uses and limitations of both methods will be explored
- **Guidance for regulatory applications involving digital systems reliability**
 - acceptance criteria
 - limitations
 - evaluation methods
 - reliability data



NRC Approach Verse EPRI Approach

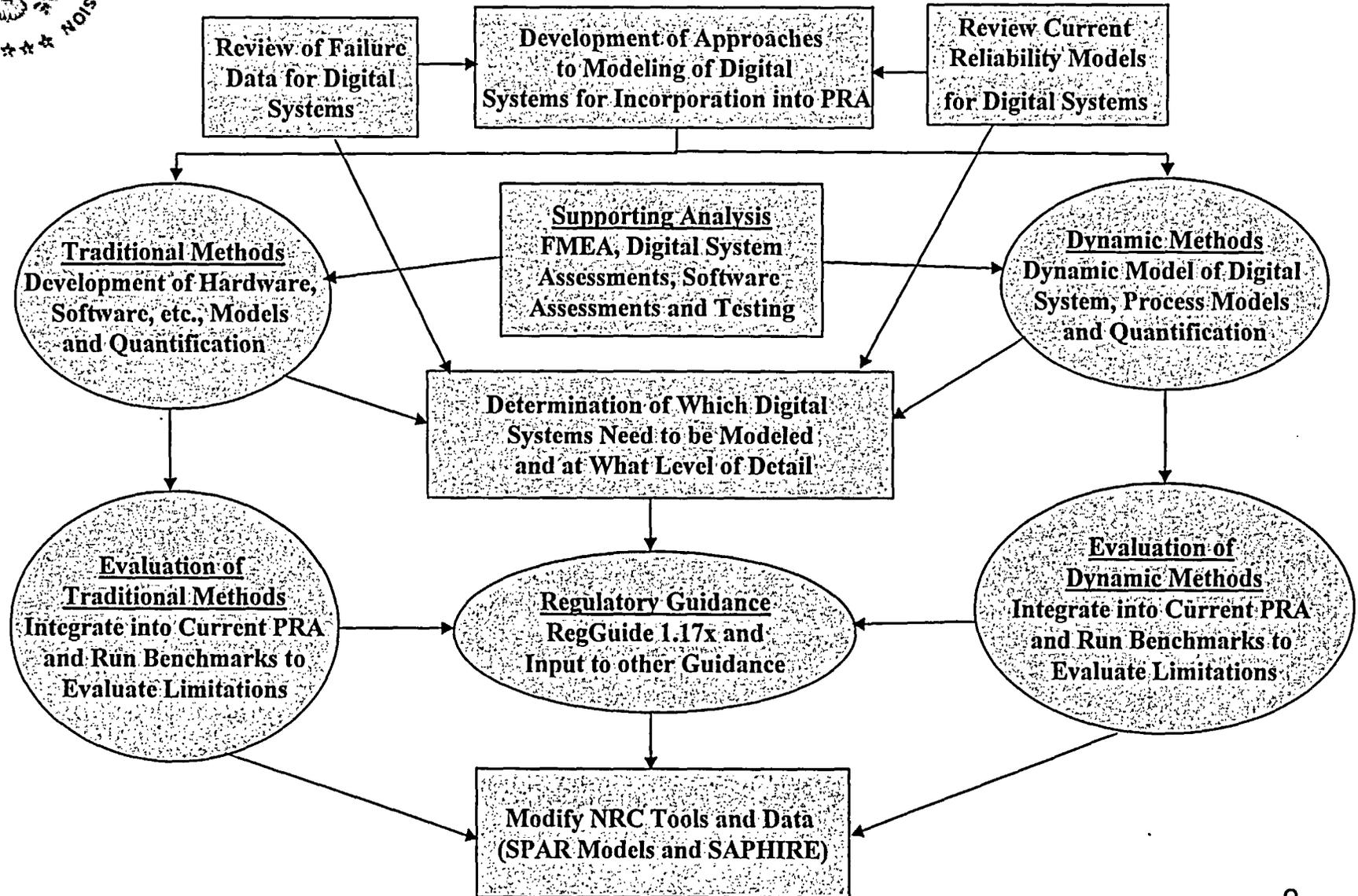
- EPRI has proposed a method for incorporating digital systems into current generation PRAs to support their Diversity and Defense-in-Depth Topical Report (TR-1002835)
 - Includes digital systems with assumed failure rates and beta factors based on IEC 61226 and other assumptions
 - Relies on digital system failure probabilities being bounded compared to the probability of random hardware failures
- NRC research is focused on development of detailed models of digital systems and development of reliability modeling methods that can integrate these models into traditional PRAs
 - Review of available methods
 - Development of both traditional and dynamic methods
 - Investigation of what models are acceptable
 - Benchmarking results



NRC Digital System Risk Program



NRC Digital System Risk Program





RESEARCH FOCUS

- Structured to support three major outcomes
 - Determine what systems need to be modeled, at what level of detail, and what level of accuracy
 - Develop new capability to support independent analysis of digital systems
 - New or modified versions of current NRC PRA tools and data
 - Develop acceptance criteria for application of risk-informed approaches
- Broad-based research, focusing on review of possible methods, and data to support reliability analysis and acceptance criteria



DEVELOPMENT AND ANALYSIS OF DIGITAL SYSTEM FAILURE DATA

- To assess failure probabilities the NRC needs to have a standard process for collecting, analyzing, and using digital system data
- There is currently very little directly applicable failure data
- This part of the research will
 - Collect and assess digital system failure data (from international databases, LER database, EPIX, data from other industries, etc.)
 - Evaluate digital system failure assessment methods and data used by defense, aerospace, and other industries
 - Develop a process to identify the frequency, severity, cause, and possible prevention of digital system failures
 - Maintain the digital system reliability data to support modeling of digital systems in PRAs



INVESTIGATION OF DIGITAL SYSTEM RELIABILITY METHODS

- ACRS recommended that NRC review methods for assessment of the reliability of software driven systems
- Guidance and criteria on the use of these methods and how to support risk assessments of digital systems in an integrated process needs to be defined
- This part of the research will
 - Survey analytical methods for identifying digital system faults and their impact on safety
 - Describe the advantages and disadvantages of each method
 - Provide guidance for using digital system failure assessment techniques, and the criteria for using the techniques



INVESTIGATION OF DIGITAL SYSTEM CHARACTERISTICS IMPORTANT TO RISK

- PRAs currently model digital systems as “black boxes”
- There is not a clear understanding as to what level of detail is needed to support inclusion of digital systems into PRAs
- An approach and acceptance criteria is needed for developing digital system PRAs and reviewing risk-informed applications
- This research project will
 - Evaluate risk models of digital systems
 - Identify systems to be modeled and at what level of detail
 - Identify sub-components that may warrant attention
 - Develop methods for performing these activities
 - Complete Benchmarks



INVESTIGATION OF DIGITAL SYSTEM RELIABILITY ASSESSMENT METHODS

- Without a methodology, NRC can not independently assess risk-informed digital system applications
- The NRC does not have a standard methodology for analyzing digital system reliability
- This research project will
 - Analyze digital system reliability assessment methods
 - Develop a digital system reliability assessment methodology
 - Conduct case studies to assess usability of the methodology
 - Update NRC PRA tools
 - Support the development of acceptance criteria



SUMMARY

- This research will provide data, analysis methods, and acceptance criteria to support the use of risk-informed regulatory methods for the review of digital systems
- Broad-based program that will look at a number of potentially viable methods for developing acceptable digital system risk models to assess the capabilities and limitations of the state-of-the-art and develop appropriate regulatory requirements
- RES is looking forward to working closely with the ACRS as these programs are implemented