

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
551st Meeting

Docket Number: (n/a)

Process Using ADAMS Template
ACRS/ACNW-005
SUNSI Review Complete

Location: Rockville, Maryland

Date: Friday, April 11, 2008

RECEIVED
APR 17 2008

Work Order No.: NRC-2115

Pages 1-122

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

T 204

DISCLAIMER

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

April 11, 2008

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on April 11, 2008, 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

+ + + + +

551TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARD
(ACRS)

+ + + + +

FRIDAY

APRIL 11, 2008

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear
Regulatory Commission, Two White Flint North, Room
T2B3, 11545 Rockville Pike, at 8:30 a.m., Dr. William
J. Shack, Chairman, presiding.

NEAL 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

COMMITTEE MEMBERS:

WILLIAM J. SHACK, Chairman

MARIO V. BONACA, Vice-Chair

SAID I. ABDEL-KHALIK, Member-at-Large

GEORGE E. APOSTOLAKIS, Member

J. SAM ARMIJO, Member

SANJOY BANERJEE, Member

DENNIS C. BLEY, Member

MICHAEL CORRADINI, Member

OTTO L. MAYNARD, Member

DANA A. POWERS, Member

JOHN D. SIEBER, Member

JOHN W. STETKAR, Member

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

(202) 234-4433

www.nealrgross.com

I-N-D-E-X

1		
2		<u>PAGE</u>
3	OPENING	
4	Chairman Shack	4
5	INTRODUCTION	
6	Dr. Apostolakis	4
7	PRESENTATIONS	
8	BY THE STAFF:	
9	<u>Digital I&C</u>	
10	Mr. John Grobe	
11	Steering Committee Review	6
12	Mr. Mario Gareri	
13	Review of Cyber Security	22
14	Mr. Paul Loeser	
15	Review of Licensing Process	37
16	Mr. Glenn B. Kelly	
17	Review of New Reactor DI&C PRAs	53
18	Mr. Michael E. Waterman	
19	Review of Operational Experience	
20	And Clarification of Digital Systems	66
21	BY NEI:	
22	Mr. Gordon Clefton	
23	Digital Instrument & Controls	
24	Industry View	80
25		

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

BY EPRI:

Industry Review of Operational Experience

Mr. Ray Torok 94

Mr. Bruce Geddes .104

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

(202) 234-4433

www.nealrgross.com

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

8:30 a.m.

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

CHAIRMAN SHACK: The meeting will now come to order. This is the second day of the 551st meeting of the Advisory Committee on Reactor Safeguards. During today's meeting, the Committee will consider the following: Digital I&C Interim Staff Guidance and Related Matters; Future ACRS Activities and Report of the Planning and Procedures Subcommittee; Reconciliation of ACRS Comments and Recommendations; and Preparation of ACRS Reports.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Tanny Santos is the designated federal official for the initial portion of the meeting. We have received no written comments or requests of time to make oral statements from members of the public regarding today's session. A transcript of a portion of the meeting is being kept, and it is requested that the speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume so they can be readily heard.

Just passing out a daily announcement that most of you have probably already heard that Bill

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

(202) 234-4433

www.nealrgross.com

1 Borchard is succeeding Luis Reyes as the EDO, so a new
2 leadership at the NRC.

3 Our first item this morning will be the
4 interim staff guidance and George will be leading us
5 through that. So, George, turn it over to you.

6 DR. APOSTOLAKIS: The subject is digital
7 instrumentation and control. We had a subcommittee
8 meeting on March 20th where the staff presented their
9 work and we had detailed discussions.

10 There are three segments that remain
11 subject of today's meeting. There is interim staff
12 guidance on cyber security, on the licensing process,
13 and new reactor digital I&C PRAs. Naturally, most of
14 the discussion was on the last one, the PRA one, but
15 we also had some comments on the cyber security. The
16 one on the licensing process is more or less straight
17 forward. We just tell the industry what they should
18 be submitting and when. So, for a change, the
19 subcommittee didn't have much to say about that.

20 We received a memo from the staff after
21 the subcommittee, I don't know if everybody has that,
22 where they list a number of the comments we made and
23 how they plan to handle them. But they also promised
24 to do that today, so you don't necessarily have to
25 look at that memo. But if you want it, we will 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 give it to you.

2 (Laughter.)

3 DR. APOSTOLAKIS: As I said, the one that
4 was discussed the most was the PRA one and that
5 shouldn't be a surprise to the Committee. By the way,
6 the members present were Jack, John, and Dennis, and
7 we had our consultant there, Myron Hecht, from Los
8 Angeles.

9 The staff is expecting a letter on the
10 three ISGs. Although today, we'll also have a
11 presentation on the operating experience review and
12 categorization of systems. The industry will also
13 make some comments, but I don't think we should write
14 a letter on these items.

15 So, without further ado, Mr. Grobe.

16 MR. GROBE: Thank you very much, George.

17 My name is Jack Grobe. I'm Associate
18 Director for Engineering and Safety Systems in the
19 Office of Nuclear Reactor Regulation. I first want to
20 compliment the ACRS on the diversity and defense and
21 depth in their digital video display units. It's
22 pretty impressive.

23 (Laughter.)

24 MR. GROBE: We'll see if we have a common
25 cause failure during this meeting. I want 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 introduce Stu Bailey. You met Belkys Sosa previously.
2 Belkys was an acting person in providing some
3 leadership for the digital activities. We determined
4 that we needed more stability in that area, so we
5 created a new deputy director position in the division
6 of engineering in NRR and Stu Bailey was selected to
7 fill that.

8 Stu's primary responsibility is to provide
9 leadership for the digital activities and the steering
10 committee interface. So he's here today to answer any
11 questions that you have and I'm going to give a little
12 presentation. So all the tough directions go directly
13 to Stu.

14 Next slide, please.

15 I just wanted to summarize a brief
16 background since we haven't been here for a while.
17 The steering committee was formed after a November
18 2006 commission meeting. At that time, it wasn't
19 clear that we were on a success path for integrating
20 all of the activities of the agency. So the steering
21 committee was formed with five senior executives, one
22 from each of NRR, NRO, research, NCER, and NMSS.

23 The goal of the steering committee is to
24 provide strategic direction to the activities, the
25 agency, and the digital I&C area to ensure 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 offices are properly integrating to solve the problems
2 and to ensure that we're having effective
3 communication and interaction with our external
4 stakeholders on the issues.

5 There are seven task working groups that
6 support the activities of the steering committee. Six
7 are led by managers in the various offices. One is
8 led by a senior staff member. Overall, there's more
9 than 50 staff involved in the task working groups.
10 The industry has created a shadow organization to our
11 organization and they've established interfaces and
12 lead individuals so that that facilitates effective
13 communication.

14 Within the seven TWGs we have defined with
15 the industry 25 specific problems. Not all problems
16 are created equally. Some of them are very complex
17 and detailed. Some of them are simpler.

18 We're developing interim guidance to
19 resolve each of those problems. To date there's been
20 four interim staff guidance documents issued and those
21 resolve 10 of the 25 problems. You saw three of those
22 last time we met in October. That was the interim
23 staff guide on diversity and defense of depth and the
24 two interim staff guides on highly integrated control
25 rooms, one dealing with communications and the other

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 dealing with human factors.

2 The fourth interim staff guide that was issued
3 has not yet been reviewed by the ACRS full committee
4 and that's the one on cyber security. We'll be
5 talking about that today. In addition, there's two
6 interim staff guidance that are in draft, and you'll
7 see those also today, and those resolve an additional
8 five problems. So 15 of 25 problems are either
9 resolved or well on the way to being resolved.

10 Next slide.

11 Since last October, which is the last time
12 we met, we've had 18 public meetings of the task
13 working groups, three public steering committee
14 meetings, and we have established the seventh TWG on
15 fuel cycle issue. Fuel cycle was not making
16 sufficient progress to clarify the specific issues
17 that they needed to resolve, so there's now a separate
18 task working group. They've got their problems
19 defined in collaboration with the industry and they're
20 moving forward.

21 The two draft interim staff guides, as
22 George mentioned that we'll be discussing today, are
23 probabilistic risk assessment. That's primarily
24 focused on new reactors, because new reactors are
25 required to have PRAs in their requirements for 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 Part 52 for the combined operating license. The
2 guidance is equally applicable to operating reactors,
3 but the focus of interim staff guide is for new
4 reactors to support the COL process as well as the
5 licensing process.

6 Mario Gareri is the lead of TWG 1 on cyber
7 and he'll be discussing cyber security. Glenn Kelly
8 was one of the principle authors of the probabilistic
9 risk assessment guidance and he'll be presenting that
10 material. Paul Loeser will be discussing licensing
11 process, and then Mike Waterman will be talking about
12 operating experience and classification of digital
13 systems.

14 As George mentioned, we'd appreciate a
15 letter. We appreciated the last letter we got after
16 the October meeting. There were two actions in that
17 letter that are not yet resolved.

18 One is the issue on developing some
19 guidance for how to evaluate operator reactions that
20 are less than 30 minutes. There's been extensive work
21 on that. It's ongoing. It's not yet brought to
22 closure.

23 And the other one is the spurious
24 actuations question. The digital diversity in defense
25 and depth task working group has that one for action

NEAL 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 they're working on it.

2 So we look forward to a letter on this
3 issue. I'm not sure if there'll be time, but during
4 the PRA discussion it would be helpful if we got into
5 a little bit of a discussion on whether or not the
6 state of PRA would support relaxation of some of the
7 diversity requirements. It's not on the agenda
8 specifically, but we'd be interested in your insights
9 on that as well.

10 Next slide.

11 We've revised our project plan last month
12 to bring more clarity to the long term actions.
13 There's 17 long term actions which will bring the
14 interim guidance to final guidance, and that final
15 guidance will either take the form of a revision of an
16 industry guide, for example, an IEEE standard or
17 something of that nature, an issuance of a NUREG,
18 revision of a regulatory guides, revision of the
19 standard review plan. There's a variety of formal
20 infrastructure documents that will be revised to deal
21 with these issues. Those are all now captured in the
22 project plan.

23 We've also received four industry reports.
24 There's a variety of industry white papers that
25 they're preparing. Four have been received and 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 under review or the review has been completed. As
2 George mentioned, we met with the subcommittee and
3 we've met several times with the subcommittee, and we
4 just met with the Commission I guess it was Monday,
5 things go quickly, and got support from the
6 Commission.

7 The only action item they were focusing on
8 for the staff was the need for staff training for our
9 operations activities for the new reactors, developing
10 our simulator training facilities. In Chattanooga we
11 have four simulators with analog control rooms and the
12 Commission wanted more detail on our preparation to
13 train our operations staff on the digital control
14 rooms. So we'll be looking at developing some plans
15 for what could be quite large expenditures to update
16 the technical training facility with digital control
17 rooms.

18 Next slide.

19 We have a number of remaining interim
20 staff guides. Licensing process you're going to hear
21 about today as licensing process information for
22 operating reactors. The Part 52 process is different
23 than the Part 50 process.

24 Part 52 includes design acceptance
25 criteria and inspection tests and analysis -- 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 and acceptance criteria, ITEC. That process is
2 different. It will require some difference guidance,
3 so we'll likely be developing a companion document for
4 new reactors in the licensing process area. And once
5 we finish the new requirements on security, as well as
6 the regulatory guidance for cyber security, we'll be
7 updating the licensing process in both areas to
8 incorporate necessary expectations in the cyber area.

9 I already talked about manual operator
10 reactions. Fuel cycle facilities is just now getting
11 underway, so that'll be issued later this year. And
12 then I already mentioned the cyber.

13 As we're using these interim staff guides,
14 we have a number of activities that are underway that
15 are using the interim staff guides. We have a topical
16 report on priority modules that's being reviewed. We
17 have the Oconee full retrofit application that's being
18 reviewed, and we're applying all these interim staff
19 guides for the first time in those areas, as well as
20 some topical reports for new reactors.

21 As we get feedback on the usefulness and
22 clarity of the guidance, if necessary we'll revise
23 those. If necessary, from industry feedback, we'll
24 revise the guidance. But the real focus, the goal
25 line is to get these into the formal infrastructure.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 If they're minor issues, we'll probably not revise the
2 interim guidance. We'll just incorporate those minor
3 issues into the final guidance.

4 Next slide.

5 As I mentioned, the goal, nirvana here, is
6 to -- my screen is burping here and you're are not, so
7 thank God for diversity. The goal is to retire the
8 interim staff guide. We're meeting and we have been
9 meeting regularly with the subcommittee and I think
10 this is our third meeting with the full committee.
11 These meeting are not required, but there are required
12 meetings in the standard agency processes for updating
13 standard review plans, reg guides, things of that
14 nature, so we will be coming back to you again in each
15 of these area.

16 I think that completes my remarks. We'd
17 be glad to answer any questions that you might have.
18 Actually, Stu will answer the questions.

19 DR. POWERS: I really appreciated this
20 overview you've provided. It's obvious that you've
21 got a very disciplined program moving forward to
22 resolve the 25 issues you've identified on a
23 relatively short term basis.

24 My question for you is, who's your
25 counterpart within research that's thinking about the

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 20 year time frame?

2 MR. GROBE: Interesting question. The
3 steering committee member in research Jennifer Uhle.
4 She's director of division of engineering and
5 research. Rick Croteau, her deputy, is very actively
6 involved. Right now the Office of Research is looking
7 at the long term, and it's not 20 year, it's long term
8 meaning five to ten year time frame, research plan.

9 That research plan has been in existence
10 for a number of years. We've been working on it.
11 It's time to revisit it because we have much more
12 clarity on our needs. So there's an integrated effort
13 to --

14 DR. POWERS: That's what motivates the
15 question is it seems like you had a very clear plan
16 for this 2009, 2010 type time frame.

17 MR. GROBE: Right.

18 DR. POWERS: And you have seen that
19 there's some challenges you face in the differences
20 between reactors and fuel facilities here that maybe
21 was not appreciated as much --

22 MR. GROBE: Right.

23 DR. POWERS: -- in past as it is now. And
24 so I'm wondering if there is any -- no. Who's paying
25 attention to saying, well, this is all going to change

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 faster than you guys can get out reg guides. And so
2 what does that -- which would be my aiming point at 20
3 years.

4 MR. GROBE: Two points, Dana. It's a very
5 interesting issue. If the industry were applying 2000
6 technology to the new reactors and operating reactors,
7 our job would be a whole lot easier. What's happening
8 is every time something changes, there's some
9 advancement, there's a desire to put that in with no
10 operating experience, little understanding of the
11 sophistication of that new change, I don't think our
12 guidance can keep up with that.

13 DR. POWERS: It cannot.

14 MR. GROBE: I used a tricky phrase in the
15 Commission meeting that complexity is an anathema to
16 predictability. If the desire is to have a
17 predictable licensing process, there has to be some
18 stability in how we move forward, and this is, you
19 know, the digital arena is one that has no stability.
20 So that's a very difficult issue.

21 There is clear direction in the research
22 arena. There's a very detailed, written, long term
23 research plan and research has just initiated in an
24 effort to go back and look at that and make sure it's
25 the right plan. So that's an integrated effort

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 between research and NRR, NRO, NMSS. I believe NCER
2 has a piece in that also.

3 The steering committee will be getting
4 updates on that. I think maybe in the six month time
5 frame it might be a good idea for us to have that on
6 the agenda for the subcommittee to look at that the
7 long term plans are. The stickiest wicket is risk
8 analysis.

9 DR. POWERS: Well, that's one of the brick
10 walls of the future to be able to do that kind of
11 thing.

12 MR. GROBE: Pardon me?

13 DR. POWERS: I mean that's clearly one of
14 the real challenges that exists out there.

15 MR. GROBE: Well, I think enough said.

16 DR. POWERS: Absolutely.

17 MS. UHLE: Can I add something? This is
18 Jennifer Uhle from research, and I think as Jack has
19 said that with regard to the rate of change of the
20 technology is hard to keep up from the standpoint of
21 the regulatory process here at the NRC. However,
22 there are other industries that are I would say more
23 able to keep up with the change and, in fact, are
24 motivating that change, and so part of our program in
25 research is to go out and tap that technology

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 experience that other industries have.

2 And so we had a program at Pacific
3 Northwest Laboratory to go and identify the right
4 contacts and we are now pursuing aggressively to
5 establish those, and I can point to high speed rail,
6 to FAA, to various --

7 DR. POWERS: I don't think you want to
8 pointing to FAA right now.

9 (Laughter.)

10 DR. POWERS: It may not be a good choice
11 today.

12 MS. UHLE: Well, we can learn what not to
13 do. And as well as naval reactors and other
14 organizations that, perhaps, have kept up on a more
15 dynamic basis. So, we again, as Jack said, we can
16 come and discuss the research program and what our
17 efforts are later on as we complete the recent update
18 that we're undergoing right now.

19 DR. APOSTOLAKIS: It would be nice to meet
20 with you before you complete anything. I think with
21 a subcommittee it's a good idea.

22 DR. POWERS: It's research. They never
23 complete anything.

24 (Laughter.)

25 MS. UHLE: The word complete, obviously,

NEAL R. GROSS

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

1 the research plan is a dynamic document. By complete
2 we mean to have vetted it fully within the staff to
3 get the staff views so that what we present to you is
4 just not one person's opinion, but it is a consensus
5 view of the staff. I think that's more an efficient
6 process.

7 DR. APOSTOLAKIS: I view this type of --
8 I think it's very similar to what we did with
9 regulatory guide 1.174 where we had very frequent
10 meetings with staff. Nobody knew really where we were
11 going, and, you know, we tried ideas, we talked about
12 them without any expectation that the staff would get
13 something finished. So I think this is part of the
14 problem. This would be a good policy here as well
15 because some ideas and so, oh, come here and -- not to
16 the full committee, I mean the subcommittee.

17 MS. UHLE: Yes.

18 DR. APOSTOLAKIS: Talk about it and see
19 what other people are thinking.

20 DR. POWERS: It seems to me you may be
21 speaking to the research program. I don't think that
22 this program that Jack's outlined for us is where you
23 want to take that kind of approach.

24 MS. UHLE: Yes.

25 MR. GROBE: Let me just be clear. There

1 are specific formal places where we have to come to
2 the ACRS and we will definitely do that. But we get
3 substantial benefit from the insights that you
4 provide, and we've been meeting regularly with the
5 subcommittee and it's our intention to continue that.

6 DR. APOSTOLAKIS: This ISG, in fact, you
7 didn't have to bring it before us, right?

8 MR. GROBE: That's right.

9 DR. APOSTOLAKIS: The ISG, we don't
10 formally review. They brought it because they wanted
11 to.

12 MR. GROBE: Right.

13 DR. POWERS: They have certain
14 masochistic --

15 (Laughter.)

16 DR. POWERS: The quality of our work
17 benefits the insights provided by this August body.

18 MR. GROBE: Any other questions?

19 DR. POWERS: No.

20 MR. GROBE: Thank you very much.

21 DR. APOSTOLAKIS: So have you gentlemen
22 prepared also to tell the committee where the points
23 of discuss were at the subcommittee and what you plan
24 to do, or should I make sure that this happens?

25 MR. BAILEY: The main points of discussion

NEAL R. GROSS

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

1 were related to the task --

2 DR. APOSTOLAKIS: During your presentation
3 are you going to refer to those?

4 MR. BAILEY: For the one that I recall the
5 points of discussion, and that was on task working
6 group number three, related to PRAs, yes, we will be
7 discussing that.

8 DR. APOSTOLAKIS: Well, for the benefit of
9 the full committee, the fundamental point of view I
10 think of the subcommittee, which was not necessarily
11 shared by the staff, although they may be thinking
12 about it, was that at this point we don't have a good
13 understanding of the failure modes of systems that
14 have digital instrumental control imbedded in them,
15 and once you accept that, then a lot of other
16 conclusions come. Can you really assign
17 probabilities, can you do this, can you do that? And
18 we urge the staff to think about it, to focus on
19 identifying potential failure modes, and that was one
20 of the main comments.

21 And, of course, it's much more relevant to
22 the ISG on the risk part, but, also, on the others,
23 except for the second one which is really
24 administrative. And for cyber security it was the
25 identification of the threats, that there is 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 implicit assumption, at least in the NEI document,
2 that the threat is coming from the outside. I don't
3 know if you agree with that.

4 MR. GARERI: Yes, I'll address that.

5 DR. APOSTOLAKIS: Okay, great. But that's
6 the thing that was a view that we really don't
7 understand the failure modes yet. So you draw your
8 own conclusions. If you don't understand the failure
9 modes, what is it that you cannot do. John, you want
10 to say something?

11 MR. GROBE: No. Thank you.

12 DR. APOSTOLAKIS: Okay. So I think that
13 was an important theme throughout the subcommittee
14 meetings.

15 MR. GARERI: Good morning. My name is
16 Mario Gareri with NRO division of engineering. I'm
17 the lead for the cyber security task working group.
18 And, actually, before I get into it, let me address
19 that first.

20 As far as the scope of this TWG, it was
21 very limited. So what was just referred to is going
22 to be addressed with the new guidance that's being
23 developed by ANSIR and research as far as threat
24 assessments and any kinds of risks dealing with cyber.
25 So you will be getting briefed on that later on, but

NEAL 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 not part of this task working group, but it being
2 looked at.

3 DR. APOSTOLAKIS: There are always two
4 issues. One is the scope of the project on which a
5 speaker is making a presentation and the other is what
6 I would call the technical part in which the
7 subcommittee has interest. So it's true that some of
8 the things we said are beyond the scope of individual
9 efforts here, but it's very important I think and
10 that's why we have the subcommittee meetings to
11 express our views regarding the actual technical work
12 of at some point has to have these elements in it.

13 MR. GARERI: Like I said, let me assure
14 you that it's being addressed in the new guidance
15 that's being developed.

16 DR. STETKAR: In relation to that, I was
17 kind of reading ahead in your slides, and the only
18 point I wanted to make regarding specifically the
19 cyber security, and it did come up in the subcommittee
20 meeting, was that when I was reading through the
21 guidance I wanted to be sure that there was a
22 sensitivity when you're evaluating the critical
23 assets, that you're also sensitive to things that we
24 think about a lot in the PRA community in terms of
25 support systems so that not only when 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 developing your threat assessment and evaluating your
2 assets, expand that boundary around to include things
3 like ventilation supplies, power supplies, and so
4 forth, that may affect several assets even though
5 they're physically separated in different rooms
6 because a lot of the cyber security and threat
7 assessment process that I saw in the document was
8 focused more on protecting the physical assets by
9 physical barriers and multiple locations and so forth,
10 that that process should be sensitive to these
11 comments.

12 DR. APOSTOLAKIS: We will have the records
13 of this committee in the sense of we would make all
14 sorts of comments before you even start --

15 DR. STETKAR: That's my name.

16 DR. APOSTOLAKIS: Usually we let the guy
17 present one slide.

18 (Laughter.)

19 DR. APOSTOLAKIS: So any other comments
20 before he starts? Go ahead.

21 MR. GARERI: Okay. Next slide.

22 I'm going to be talking about basically
23 some background. I'm going to talk about the ISG
24 itself and then the path forward.

25 From the first slide here, let me just

NEAL R. GROSS

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

1 give you a little idea. The TWG only had one problem
2 statement to address and the problem statement itself,
3 like I said it was within scope, deals with two
4 guidance documents regarding cyber security. One of
5 them was the Reg. 1.152 Rev 2 as you can see there.
6 And the other one is an industry guidance that was
7 developed, NEI 04-04 Rev 1.

8 The reg guide was issued revised in order
9 to capture the cyber security in the design and safety
10 systems in January of 2006 and the NEI 04-04 document
11 was found acceptable by the NRC in December of 2005.
12 So both documents basically came out around the same
13 time frame. The issue here is that one document is
14 specifically, which is the reg guide to address safety
15 systems, and the NEI document was more of a
16 programmatic approach to cyber security.

17 So if we go to the next slide.

18 The first bullet is basically about what
19 the task of the task working group was, and, again, it
20 was limited to basically there were concerns from the
21 industry that the two guidance documents were in
22 conflict and what the staff did and the task working
23 group did, we did a gap analysis to actually determine
24 if there were any gaps or any kind of conflicts in the
25 two documents. And in doing that, basically the end

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 result was that there were actually no conflicts.
2 There were some overlaps and some differences in the
3 two documents, but that's expected because the two
4 documents serve two different purposes.

5 So, again, the second bullet there says
6 that no inconsistencies were actually found as the
7 industry had concerns and the two documents are
8 actually complimentary to one another.

9 Next slide.

10 At that point the task working group could
11 have actually closed out the item because we were
12 finished with the problem statement. There were no
13 conflicts and there were no issues. But the industry
14 committed to revise NEI 04-04 to include and
15 incorporate the criteria regarding safety systems,
16 which was captured in the reg guide.

17 So at that point the staff agreed that to
18 provide additional clarification to the staff and the
19 industry that that would not be a bad idea to continue
20 with the effort even though, again, it went beyond
21 what we set out to do. So after revising the 04-04
22 document, what we found is that, because the two
23 documents were so different in structure and the
24 material they were covering, it was kind of difficult
25 to actually do a review using the NEI 04-04 document

NEAL 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 you're doing licensing.

2 So what we did is we developed a cross
3 correlation table to basically capture the elements
4 and the criteria in the Reg Guide 1.152 into a table
5 that would actually show where that same information
6 can be captured inside 04-04.

7 DR. STETKAR: Mario, for the benefit of
8 the rest of the committee here who were not at the
9 subcommittee meeting, you mentioned differences in
10 scope between NEI 04-04 and the reg guide. Could you
11 just briefly elaborate on a few examples of those
12 differences?

13 MR. GARERI: Sure. Well, the differences
14 are the reg guide itself deals more the development
15 life cycle and incorporating cyber security throughout
16 that life cycle when you're developing a system. And,
17 basically, it deals specifically with safety systems.
18 Where the NEI 04-04 looks at the actual setup of cyber
19 security throughout the plant, whether it's firewalls
20 or defensive measures. And, again, the information of
21 04-04 is security related and, you know, I can't go
22 into the details of that.

23 But that's the main difference is that one
24 approaches cyber security from a programmatic
25 approach, which is the 04-04. The Reg Guide 1.152

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 does it from a design perspective and deals
2 specifically with safety systems.

3 Bill may want to add something.

4 MR. KEMPER: Yes. This is Bill Kemper.

5 Just to illustrate maybe if I can. For
6 example, NEI 04-04 would have a requirement that says,
7 a licensee shall within their design an engineering
8 process, a means for securing cyber security is
9 invoked in digital systems. Now, Reg Guide 1.152 goes
10 beyond that and it says, the licensee shall ensure
11 that there are no time bombs, back doors, malicious
12 code, that sort of thing. So you see, it's a lower
13 level of detail.

14 So in reading 04-04, it's hard to draw
15 from that the this specificity that's needed in a
16 license application for NRR to be able to approve
17 that.

18 MR. GARERI: I would say, to add to that,
19 basically it looks into the box. The reg guide looks
20 really what's inside the box, where 04-04 looks
21 outside of it.

22 DR. APOSTOLAKIS: 04-04 deals with broader
23 issues than just safety systems?

24 MR. GARERI: Yes, it does.

25 And the revised 04-04 Rev 2 has

NEAL R. GROSS

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

1 incorporated safety system based on the interaction
2 we've had with industry. And that was issued December
3 31st of last year, and as of this morning I don't
4 believe the industry has any issues with the ISG.

5 DR. SIEBER: Isn't that just the reverse
6 of the way it should be, though? Shouldn't the
7 industry guides be very specific as opposed to that
8 and the reg guide and the reg guide be more general?

9 MR. GARERI: In some cases the 04-04
10 document is very specific, and that's why it's, again,
11 security related information as appendices, which
12 actually gives you the details of what to do to put
13 defensive measures in. But in some other cases, like
14 I said, I had a different goal in mind so it does not
15 address safety system in the design aspects of it.
16 That's the difference in the two documents, but it
17 does have detail.

18 DR. SIEBER: Yes, I always picture the
19 regulation and the underlying regulatory guidance --

20 MR. GARERI: Yes.

21 DR. SIEBER: -- relatively broad in nature
22 in an industry-specific document that the staff
23 accepts would be one way to comply with the overall
24 guidance based on rule --

25 MR. GARERI: The one thing we didn't --

1 one thing to keep in mind is when 04-04 came out,
2 there's still no regulations on cyber, so that was
3 really an industry -- and submission of to get
4 something there. And that's on the way. Right,
5 that's going to be my last slide.

6 Next slide.

7 The ISG itself basically provides
8 additional clarification to cyber security. Again, it
9 does cover the background of cyber security in
10 general, but it specifically talks to how to use the
11 04-04 draft 2 revision 2 document when, you know, put
12 in a license middle or dealing with cyber security in
13 a safety system. Again, the ISG includes that table
14 which makes it easier for reviewers and industry to
15 understand exactly how to use the 04-04 document when
16 dealing with safety systems.

17 And, again, either the reg guide can be
18 used or the NEI document now in conjunction with the
19 table if someone decides to actually use that to
20 address cyber security in safety systems.

21 Next slide.

22 This is the last slide and what's
23 happening now is the ISG itself has been rolled over,
24 is being rolled over to the draft guide 5022, which is
25 being developed to address cyber security. This draft

1 guide is basically going to become a reg guide which
2 will support the rule.

3 DR. APOSTOLAKIS: Why is it Part 73? Is
4 that for security stuff?

5 MR. GARERI: Yes. This deals with
6 physical security. As you can see in the sub-bullets
7 there, the long term actions of the actual regulations
8 coming out on cyber security, the regulatory guide to
9 support the rule, and the updating or revision of the
10 standard review plan, chapter 13, will all happen
11 outside of really the TWG effort, even though we're
12 still engaged with ANSIR and research.

13 DR. APOSTOLAKIS: Can you explain the
14 first sub-bullet, issuance of new rule 54 proposal 55?
15 What does that mean?

16 MR. GARERI: Right. That's what I was
17 going to get to.

18 So what happens is that the regulations
19 that are coming out, the proposed rule was under
20 73.55(m) for cyber security. In taking another look
21 at it, ANSIR has determined with research that it
22 would be best to put it into 73.54 so that it can
23 actually address more than just power reactors.

24 So, officially, it's the proposed rule of
25 73.55(m), but it will come out as 73.54. It just

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 hasn't been made public yet. That's why I have it in
2 brackets.

3 DR. APOSTOLAKIS: As has been said
4 already, this interim guidance has been issued,
5 December 31st, '07, so any comments that we may want
6 to put in our letter will be addressed really to this
7 effort of developing the regulatory documents in the
8 future?

9 MR. GARERI: Exactly.

10 DR. APOSTOLAKIS: And the staff, of
11 course, can take those under advisement or not. But
12 we are not really commenting on the guidance itself
13 because that's final, it's out.

14 Any questions? All right. Shall we move
15 on?

16 MR. GARERI: Thank you.

17 DR. APOSTOLAKIS: I have a question. I'm
18 sorry.

19 MR. GARERI: I almost made it.

20 DR. APOSTOLAKIS: There was a
21 semi-question I think on an issue that was raised
22 during the subcommittee and I'm not sure whether the
23 concern is real or not. Concern, it's not a concern.
24 What is a definition of cyber security? Are you
25 defining it some place?

NEAL 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. GARERI: I'll have Dave maybe add to
2 this if I'm incorrect in saying it, but I believe the
3 new regulatory guide that's going to be coming out,
4 we're making a point to actually describe it or define
5 it in there, because, again, there is some confusion
6 whether or not it's an outside attack or internal.

7 DR. APOSTOLAKIS: Can you tell us today or
8 is it --

9 MR. GARERI: I look at it that cyber
10 security attack would be basically something that
11 would be coming from the outside. But at the same
12 time, if you have a trojan or something, a back door
13 put into the software itself, that would also impact
14 the -- it would give you a vulnerability to a cyber
15 attack. Do you see what I'm saying?

16 So either way, if the bug or the design
17 itself is faulty, then you're vulnerable to an attack
18 from the outside. I'm not sure if maybe Dave wants to
19 add to that.

20 DR. RAHN: This is David Rahn. I'm
21 assisting in shepherding the development of the
22 regulatory guide, and the cyber security program has
23 a two-phased approach. There's an overall protection
24 of a facility, and that protection is for potential
25 outside attempts to attack the facility and insiders.

1 And there is a design basis threat rule which defines
2 what are those potential threats. That's in 73.1.
3 That document defines the overall focus of a cyber
4 security program that a facility needs to have.

5 Within the facility, there's a bunch of
6 digital assets. Many of them are performing safety
7 related, some are performing emergency preparedness
8 functions, and some are security functions. And there
9 are also systems that protect those systems. Many of
10 those have digital components in them and those
11 components have to be designed, when they put into the
12 system, they can either have their own hardening
13 against any potential threats which could take them
14 down. That means that from the initial development of
15 that digital system there would be --

16 DR. APOSTOLAKIS: Let me interrupt. You
17 are getting down into detail now. This is how to
18 achieve something.

19 DR. RAHN: Yes.

20 DR. APOSTOLAKIS: Is there a high level
21 definition of what cyber security is?

22 DR. RAHN: Within the regulatory guide the
23 focus is taken that cyber security is a portion of a
24 security function for the whole facility. The object
25 is security for the facility and it's how it affects

NEAL 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 digital assets within that facility.

2 DR. APOSTOLAKIS: Period?

3 DR. RAHN: Period.

4 DR. APOSTOLAKIS: So it doesn't matter
5 whether it's on the outside or inside?

6 MR. GARERI: Exactly. It doesn't --

7 DR. APOSTOLAKIS: -- broad definition?

8 DR. RAHN: Yes, very broad definition.

9 MS. BANERJEE: George, can I add
10 something, please? This is Maitri Banerjee. The Part
11 73 rule is supposed to come to us in May, the first
12 week of May time frame.

13 DR. APOSTOLAKIS: Coming to us means to
14 the full committee?

15 MS. BANERJEE: Actually, we are going to
16 get a copy of that.

17 DR. APOSTOLAKIS: The documents are
18 coming?

19 MS. BANERJEE: The documents are coming
20 and security subcommittee is going to take a look at
21 it and Mario is going to make a decision how much of
22 it we are going to review in May.

23 VICE-CHAIR BONACA: Supposed to look at
24 the components of the security and then make a
25 determination whether or not the committee should

NEAL R. GROSS

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

1 review them.

2 DR. MAYNARD: I have got question along
3 that line. Is there a clear definition or division
4 between what's being done for cyber security and the
5 overall security, and not so much that it be separate,
6 but that it actually fit in and not have overlap
7 between the rest of the security requirements for a
8 plant?

9 MR. GARERI: You're talking about as far
10 as the physical security?

11 DR. MAYNARD: Right, because like one of
12 John's first comments, he's talking about the support
13 equipment and that's important, but I'm not sure you
14 have to define that in cyber security if that's
15 defined as the rest of your security plan requirements
16 and stuff. I'm wondering, is there overlap, is there
17 work being done to make sure that we don't have
18 incompatible stuff here?

19 MR. GARERI: I'm not longer with NCER and
20 I haven't been engaged up to the last point. Okay,
21 Bill. He's raising his hand.

22 MR. KEMPER: Yes, Bill Kemper again. I
23 just attended a meeting with David, as a matter of
24 fact yesterday, to discuss draft language on 73.54.
25 You know, the ink's still wet on this thing so we're

NEAL R. GROSS

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

1 still working on it. But, yes, specifically, 73.54 is
2 titled protection of digital computer and
3 communication systems and networks, so it's intended
4 to provide the specificity, if you will, so that you
5 can differentiate this particular security attribute
6 from the overall physical security plan. All be it,
7 it's part and parcel of the site's physical security
8 plan. I hope that answers your question.

9 MR. SHUKLA: Dr. Apostolakis?

10 DR. APOSTOLAKIS: Yes, sir.

11 MR. SHUKLA: All these ISGs are subject to
12 further revisions and enhancement based upon their use
13 until they are rolled over to a permanent regulatory
14 document. So --

15 DR. APOSTOLAKIS: Yes, but I mean --

16 (Simultaneous speakers.)

17 DR. APOSTOLAKIS: Okay. Any other
18 questions?

19 MR. GARERI: Thank you.

20 MR. LOESER: I'm Paul Loeser. I'm one of
21 the digital I&C reviewers.

22 If you'll go to the next slide, please.

23 Basically, chapter 7 provides guidance to
24 the staff on how to do a digital review. Things like
25 BTP-14 19: However, digital systems are somewhat

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 unique within our review process in that we not only
2 look at testing for the final design, but we also need
3 a determination of a high quality design process.
4 This is because digital systems are complex enough
5 that we can never test them enough to say that they
6 are perfect. So we look at this design process and
7 this process takes too long. We can't do an actual
8 independent review, the equivalent of an independent
9 V&V ourselves because this takes too long, and,
10 frankly, we don't have the people.

11 DR. POWERS: When you say it takes too
12 long and it takes too many people?

13 MR. LOESER: Typically, the rule of thumb
14 is that it takes as long to do a thorough review of
15 the process as is spent originally in the design.

16 DR. POWERS: Right.

17 MR. LOESER: And if they have five or ten
18 people working for two or three years, we don't have
19 five or ten people who can spend two or three years
20 doing this, so we have to look at some lesser degree.
21 What can we do to achieve reasonable assurance that
22 this is really a pretty good system, was done in a
23 pretty good way, and there is a reasonable assurance
24 that it will operate the way it's supposed to and
25 perform the functions it's supposed to.

NEAL R. GROSS

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

1 DR. POWERS: And what I think I'm
2 struggling for is what's a reasonable amount of time
3 to spend on this?

4 MR. LOESER: Well, we have been spending
5 typically on a overall topical report on a new type of
6 system that we've never seen before --

7 DR. POWERS: Right.

8 MR. LOESER: -- tends to be in the
9 neighbor of one to two man years of effort if a
10 licensee is using an approved platform in exactly the
11 same manner it may take half of that, or if they have
12 modified things, it would be more.

13 One of our final products is a list of
14 documentation that shows what type of thing we would
15 need depending on the complexity of design. I'll be
16 getting to that in my last slide.

17 DR. POWERS: Okay. So I know what's too
18 much, I know what you're doing now. What's desirable?

19 MR. LOESER: Well, we thing, obviously,
20 less is desirable. But the question -- that's not
21 really the question we were asked to address here. We
22 are addressing that. As a matter of fact, last night
23 we had a brainstorming session on how could we modify
24 our current process to somehow to do this faster,
25 easier, cheaper in NASA terms.

NEAL R. GROSS

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

1 DR. POWERS: You left out better.

2 (Laughter.)

3 MR. LOESER: We want equally good. It
4 wouldn't have to necessarily be better. We think we
5 have a good determination now. We want to make sure
6 that whatever we do we come up with something that's
7 equally good.

8 DR. POWERS: Or better.

9 MR. LOESER: That is, it's still -- or
10 better would be nice, but still provides us with a
11 high degree of confidence or reasonable assurance,
12 whatever you wish to say, that this system will
13 function to perform whatever safety functions are
14 specified.

15 DR. POWERS: I actually have a reason for
16 wanting to do this. So a brand new, unfamiliar system
17 topical report gets submitted, and if you could do
18 that with one man year, then that would take this off
19 the high priority activity list or not?

20 MR. LOESER: I'm not quite sure what
21 you're --

22 DR. POWERS: Well, currently, you spend
23 you say on the order of two man years when you get a
24 brand new system in. If you cut that in half, would
25 that make everybody happy and they say, okay, let'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 MR. LOESER: I think it would make them
2 happier.

3 DR. POWERS: Happier.

4 (Laughter.)

5 DR. POWERS: I mean at what point do you
6 no longer have an action plan and things like that
7 going on and you say, well, if you can make it better,
8 that's great, but, otherwise, I'm not going to
9 emphasize it?

10 MR. LOESER: I would sort of hope that no
11 matter how good our process is we would never be
12 closed to the idea that we could improve it --

13 DR. POWERS: I'm not asking you that. I'm
14 asking you, when do you quit making it a big priority
15 and coming meeting regularly with George's
16 subcommittee and things like that?

17 MR. BAILEY: I think we're making progress
18 on that as we speak. We're reviewing --

19 DR. POWERS: I know you are. I'm asking
20 you when you quit making progress.

21 MR. LOESER: I don't think I can answer
22 that question on any process when do you decide that
23 it's good enough. I can't tell you that. And I also
24 can't predict at what point management starts telling
25 me it's taking too long or industry starts complaining

NEAL 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 it costs too much. I don't know that because I
2 can't see into their minds.

3 DR. POWERS: I'm really asking your mind.
4 I'm not asking for other people's. I'm not going to
5 hold you to this. I'm not going to put a gun to your
6 head.

7 MR. LOESER: I keep telling people I'm
8 inherently lazy. I'd like to make it as easy as
9 possible, but still be able to convince myself that
10 I'm signing my name to a good product. If I could do
11 it in 20 minutes, I would, but I can't. I don't know
12 how.

13 MR. BAILEY: I don't know that it's much
14 of an answer, but it's our own observations and
15 industry's observations of how the reviews are going.
16 When we see that they are going smoothly all around,
17 then I think we can say this needs less focus. That
18 doesn't mean we won't still be looking for
19 improvements.

20 But right now we've seen that it is not
21 always smooth. All of the documents that we would be
22 looking for are not always available right up front.
23 We're really trying to fine tune this so that it also
24 fits in with the licensee's life cycle of developing
25 and implementing one of these digital modifications.

NEAL 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. SIEBER: I think this is a function of
2 what you want as a result. For example, if you don't
3 spend a lot of time and the system fails, you know, a
4 multitude of ways, you know you haven't done a good
5 job. And right now, since we only have one project in
6 the industry that's full scale with protection and
7 control and all that in there just on it's very
8 beginnings, I think you have to look elsewhere to see
9 where others would have failed, for example, in
10 Europe, to determine what it is you have to do to make
11 sure that you don't repeat those kinds of failures.

12 MR. LOESER: That is, in fact, happening.
13 Research has a project, you'll be hearing about it
14 later, to look at other industries, not just the
15 European reactors, but also --

16 DR. SIEBER: Rails, planes.

17 MR. LOESER: Yes, everything that uses
18 high reliability software, MIL-SPEC.

19 DR. APOSTOLAKIS: This probably is not a
20 good idea, but anyway.

21 DR. CORRADINI: I, just for clarification,
22 Jack, you said there is one case in industry where
23 they're doing it for, and I thought you said control
24 and protection?

25 DR. SIEBER: The Oconee project is pretty

NEAL R. GROSS

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

1 big.

2 DR. CORRADINI: But that's including
3 reactor protection laws.

4 MR. LOESER: And the SF.

5 DR. SIEBER: The other 30 or so projects,
6 in my opinion, have been relatively small.

7 MR. LOESER: That is correct. This is the
8 biggest one we've had.

9 DR. APOSTOLAKIS: Just to move it along.
10 We had the presentation here sometime, I don't know,
11 last year where another team within the Agency had a
12 similar problem, namely, during construction of a
13 facility, reactor, they just cannot inspect
14 everything. It takes too much work, too much effort,
15 okay?

16 MR. LOESER: Yes.

17 DR. APOSTOLAKIS: So they developed a
18 methodology, it's really a sampling methodology, but
19 a sample is not random. They use some method to risk
20 inform the process, and so on. I'm wondering whether
21 you should look at that and see whether you can get
22 any help from it.

23 MR. LOESER: Well, we actually something
24 like that. What we do is we do a reasonably thorough
25 investigation on the process they use, and then 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 sample the design outputs in our threat audit to see
2 that the process worked correctly and that
3 the --

4 DR. APOSTOLAKIS: All I'm saying is that
5 you may find the method there of approach that they
6 use helpful. That's all. I'm not saying you are not
7 doing anything.

8 MR. HILAND: This is Pat Hiland. I'm the
9 director of engineering in the Office of NRR, and let
10 me just try to add some clarification. You're
11 correct. The current application that we have in from
12 Duke on the Oconee project is significantly larger
13 than any that we've seen before.

14 We've gone back and looked at the way
15 we've done business before and it's not reasonable to
16 expect us to review the Oconee application to that
17 level. And what we've mapped out is that we're trying
18 to define what is a licensing review, what would be an
19 onsite review of the factory or the onsite test
20 information, and then, finally, what would be an
21 inspection activity. Inspection activity will likely
22 be by the regional inspectors after the amendment is
23 approved.

24 We have an example in the steam generator
25 replacements. You know those amendment requests to

1 replace steam generators, I've never done one, but I
2 believe they're approved far in advance of the actual
3 work on site, and those who have been at a site when
4 a generator replacement is ongoing, that's a lot of
5 work and we have a defined inspection program that's
6 about 850 hours. So it's a sample inspection. You
7 can't be there all the time to do that. That's what
8 we're doing in the Oconee place.

9 We have given an initial estimate of how
10 much effort and how long that effort's going to take.
11 We're talking with the licensee, and they gave us what
12 their desires were, and we're different. We're off by
13 about four or five months today, so we have to go back
14 to see if we can improve that schedule by adding more
15 resources if that's the correct approach, or the
16 licensee moving up some of their activities as the
17 factory accepts its tests.

18 You know, currently, they're scheduled to
19 get the results in January of '09. Will that support
20 our review to meet their schedule? Maybe, maybe not.
21 Don't know. So I'm trying to answer the question in
22 broad terms.

23 DR. APOSTOLAKIS: The question, I'm not
24 doubting that you have a plan and inspection and so
25 on. I'm not saying that. All I'm saying is there's

1 another group within the Agency that has a similar
2 problem. They appear to have developed a methodology
3 for selecting the sample in a reasonable way, and all
4 I'm saying is look at it. If you find something that
5 is helpful to you, use it. I never doubted that you
6 can had an approach already.

7 I don't remember who was doing that, but
8 we wrote a letter. So through the letter we can --

9 MR. HILAND: I'll work with Girija and
10 find out. We'll get that.

11 DR. APOSTOLAKIS: Yes, so it would be very
12 easy.

13 MR. LOESER: So much for the easy
14 presentation.

15 (Laughter.)

16 DR. APOSTOLAKIS: We are behind schedule.

17 MR. LOESER: Anyway, what we basically do
18 is we look at what the licensee or the vendor plans to
19 do and how this will be done. This is by reviewing
20 the plans and procedures. Was it actually done? And
21 this is at the vendor audit. And then what were the
22 results? And this is looking at the design outputs
23 and the final test procedure.

24 This is considerable amount of
25 documentation and the industry decided that this

NEAL R. GROSS

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

1 amount of documentation not be presented to the staff
2 and put on the docket; in particular, they were
3 worried that once it's on the docket, any changes they
4 make to their configuration management plan would need
5 to be reviewed. We've reassured them that this is not
6 the case. It would be done on 50.59. They would only
7 be re-reviewed if the change was significant enough to
8 change the determination that we had made that it was
9 adequate.

10 TWG 6 actually had four problem
11 statements, four issues. One is the level of detail
12 necessary in the review of the licensing actions. Two
13 is the applicability of this guidance for operating
14 reactors. Three was the clear licensing protocols for
15 the review. And four was clear guidance on cyber
16 security issues for I&C. The fourth one we really
17 didn't look at. This is left for the cyber group.

18 In order to do this we needed to deliver
19 a specific clarification on what documents needed to
20 be delivered to the staff, at what phase in the review
21 process it was needed, which of these documents needed
22 to be on the docket and which would be sent off the
23 docket, and which documents don't need to be docketed
24 or sent to the staff at all but only available onsite
25 during the site visit.

NEAL R. GROSS

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

1 We considered the inputs and we basically
2 provided such a list. We're still working on refining
3 this list. This list right now encompasses the most
4 complex possible amendment, so licensees or the staff
5 would delete from the list rather than trying to add
6 things to it.

7 This does not modify or supercede existing
8 regulations, with one exception. That is the site
9 activities of maintenance operation and training would
10 be left to the region to review. We don't consider
11 that a licensing issue, so that would be --

12 DR. APOSTOLAKIS: Can an ISG change the
13 regulation?

14 MR. LOESER: No.

15 DR. APOSTOLAKIS: No. It's just guidance?

16 MR. LOESER: Yes.

17 DR. APOSTOLAKIS: You cannot introduce new
18 requirements, can you?

19 DR. SIEBER: You can.

20 MR. LOESER: You're right. It changes the
21 guidance. It changes no regulation.

22 DR. APOSTOLAKIS: You cannot impose
23 requirements through an ISG?

24 MR. LOESER: That's correct.

25 DR. APOSTOLAKIS: It's a softer version of

NEAL R. GROSS

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

1 a regulatory guide. Is that true?

2 MR. LOESER: Well, we're hoping to turn it
3 into a regulatory guide eventually.

4 DR. BLEY: Less of a review process than
5 a regulatory guide, is that right, the review and
6 approval process?

7 DR. APOSTOLAKIS: Exactly.

8 MR. BAILEY: Well, and you can make a less
9 significant change during. You cannot deviate --

10 DR. BLEY: More flexible.

11 MR. LOESER: I mean we're doing things
12 like considering revising the standard review plan to
13 account for some of these. We're writing a new
14 inspection procedure for the regions to use when
15 they're looking at the portion that is now being
16 assigned. Things of that nature. But none of this
17 goes to changing regulation or legal requirements at
18 all. All those are still in place.

19 DR. APOSTOLAKIS: Very good.

20 MR. LOESER: So we have provided the ISG,
21 which besides the explanation, also has a table 1 that
22 shows all the documents that need to be reviewed and
23 shows at what time during the review process or the
24 design process they need to be reviewed. We also have
25 a second set of tables that show for reviews of lesser

1 complexity. That is, if they're using a platform that
2 has already been reviewed, we only then would have to
3 look at plant specific documentation. Or if the
4 platform has been modified at little but not totally,
5 we'd only need to look at the changes and only to the
6 degree necessary to realize that this doesn't change
7 our original concept.

8 And we're still working on refining these
9 tables unless we have continuous dialogue with the
10 various licensees and the licensee members of the
11 working groups.

12 DR. APOSTOLAKIS: So this is going to be
13 issued when?

14 MR. LOESER: Sometime this year. We're
15 getting fairly close. We're hoping to have it in a
16 couple of months. But depending on how much we refine
17 this, I can't guarantee right now.

18 DR. APOSTOLAKIS: Any questions, comments?

19 DR. SIEBER: I guess I would reiterate the
20 fact that the Oconee modification is fortuitous
21 because it's big enough to help develop the licensee's
22 and the industry's approach and the staff's approach
23 to this and I would advise or recommend that you take
24 advantage of this opportunity to think about the
25 review you're doing in terms of regulations that you

NEAL R. GROSS

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

1 need to do future review.

2 MR. LOESER: Yes. We are certainly doing
3 this. We are using Oconee as a potential test case.
4 If we have any new insight, we will try it out there.
5 We're in the process of doing this and, at the moment,
6 we're in the early stages of the review. I believe we
7 have just sent out the acceptance letter for the
8 review. So we don't have enough experience yet to be
9 able to report results from the Oconee review.

10 DR. SIEBER: Yes. You're probably going
11 to be writing regulations before you're done with that
12 review. On the other hand, as things evolve during
13 the review process to the extent that you can work
14 them into the guidance documents, I think that would
15 be helpful.

16 MR. BAILEY: That is our plan. Our plan
17 is to refine the staff guidance based on what we find
18 in Oconee.

19 DR. SIEBER: Okay. Thank you.

20 DR. APOSTOLAKIS: Okay. Let's move on.
21 Hope this time we go quickly.

22 CHAIRMAN SHACK: The noncontroversial one.

23 DR. APOSTOLAKIS: Any questions before we
24 start this time?

25 (Laughter.)

NEAL R. GROSS

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

1 DR. APOSTOLAKIS: Mr. Kelly is the
2 presenter.

3 MR. KELLY: Yes.

4 DR. APOSTOLAKIS: Very good.

5 MR. KELLY: Good morning. I'm Glenn
6 Kelly. I'm with NRO. I'm a senior reliability and
7 risk analyst.

8 I'm going to talk to you today about the
9 review of digital I&C systems and the guidance that
10 we're providing to the NRC analysts on how for new
11 reactors we should review the digital I&C system PRAs.

12 Next slide, please.

13 The problem statement that we had was that
14 existing guidance doesn't provide sufficient clarity
15 to be used current, and I want to emphasize the word
16 current, methods to properly evaluate digital I&C
17 systems. So we're asked to provide guidance to make
18 it easier for the staff reviewers and part for
19 industry to see what they should be doing for new
20 reactors. We've been asked to consider common-cause
21 failure modeling uncertainty analysis of digital I&C
22 systems.

23 In looking at this I just wanted to remind
24 the committee that 10 CFR 50.42 requires that new
25 reactor designs submitted under Part 52 must have

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

1 PRAs. The PRAs would be design and plant specific and
2 they would include models of digital I&C systems.
3 They only need to show, though, that under Part 52
4 basically that they meet the safety goals. There's no
5 requirement for much more than that.

6 Our short term action, then, was to
7 develop this interim guidance. We've done that. And
8 just to bring the committee aware of some of the
9 issues that we were dealing with, the risks
10 assessments, we have a lack of consensus on them, how
11 to model digital I&C systems, and we have issues
12 associated with the robustness of the data for digital
13 I&C systems. And as you've heard before, digital I&C
14 systems are constantly being improved, and, in turn,
15 that makes it hard to get data that says we've had so
16 many years of experience with this particular
17 software, whatever, and it shows X, you know. What
18 happens is that the software changes so fast that,
19 before you know it, you're onto a whole new version,
20 and, therefore, you can't say, well, okay, I've got
21 ten years' experience with this at 20 plants and this
22 what I've learned from them. So we're working with
23 that.

24 In particular, what we were looking at
25 here was for new reactors for determining the 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 basic guidance about our analysts would do these
2 reviews. The guidance that's in the ISG is not about
3 how you make risk-informed decisions involving digital
4 I&C systems. That's going to be addressed in later
5 ISGs, but we're not dealing with that here.

6 Next slide, please.

7 The content of the ISG, basically, we've
8 outlined various attributes and risk insights that
9 we're hoping we'll be able to derive out of the
10 information that gets provided by the utility. The
11 risk insights that we feel will be most robust and
12 useful will be those that are at a fairly high level.
13 And one of the reasons for that is that we have very
14 little detail information at this point on digital I&C
15 systems.

16 As a matter of fact, much of information
17 that would be needed to do a very detailed PRA review
18 might not be available until the PRA that is going to
19 be performed one year prior to fuel up. So at that
20 point they'll actually already have this COL and we'd
21 be potentially then reviewing something at that point
22 to give us information as to whether or not they've
23 met the DAC associated with the digital I&C system.

24 We've provided guidance to the PRA
25 reviewers for situations where we're going to have a

NEAL R. GROSS

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

1 more limited review, for situations where we're going
2 to have a more detailed review. And, again, part of
3 that has to do with as we go through the various
4 stages of it, a design certification, or a COL
5 application, or even potentially down the road that
6 one year prior to fuel load.

7 We have very, very different levels of
8 information about what's in a digital I&C system.
9 We've provided an appendix to the ISG that has
10 captured a number of the insights that have come out
11 of the ABWR PRA review and the AP-1000 PRA review.
12 And this is just to give the reviewers some
13 information on the type of things that they might be
14 seeing or could expect to be able to develop or have
15 the applicant develop out of their risk assessment.

16 Next slide, please.

17 The subcommittee was kind enough to
18 provide us with a lot of interesting comments during
19 the meeting that we had on the 20th.

20 DR. APOSTOLAKIS: Did you say kind?

21 (Laughter.)

22 MR. KELLY: It was a very interesting
23 time.

24 DR. APOSTOLAKIS: That's an
25 understatement.

1 MR. KELLY: What we've done in taking
2 these comments, and, again, these are some of the key
3 comments that we got from the subcommittee,
4 originally, we had on performing an uncertainty
5 analysis, we discussed specific guidance on types of
6 sensitivity studies that we might expect a licensee to
7 submit to us. It was felt that we were too specific
8 about this. That a licensee might come to believe
9 that this was all they needed to do was to do these
10 particular ones, or that what, in essence, we were
11 doing is creating an NRC approved methodology for this
12 is how you perform uncertainty analysis.

13 So what we did is we kind of backed it up
14 and made it a higher level guidance saying we would
15 like you to perform sensitivity studies. We think
16 it's important and what we're going to do is we're
17 going to list some of the areas that in the guide
18 today are the most contentious or the most worrisome
19 for us, or that we feel have the greatest uncertainty.
20 and with the expectation that some of these will end
21 up being exercise when they perform their sensitivity
22 studies.

23 It was also pointed out to us that some of
24 the guidance, as I mentioned earlier, we broke our
25 guidance into less detailed/more detailed guidance 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 the review. The subcommittee felt that some of the
2 guidance in the more detailed review really belonged
3 up in the less detailed review, and, in particular,
4 the subcommittee showed strong interest in having more
5 information on performing how the failure modes and
6 effects analysis was performed, and, in particular,
7 the process because on a less detailed review, you
8 would not have enough time to actually go into how
9 they performed the FMEA, but you can look at the
10 process that they used for developing that FMEA. And
11 then if you need to, you can go into the details at
12 some later time. So we've modified that.

13 We also simplified the guidance on common-
14 cause failure analysis, in part because, as George
15 pointed out, if you don't really know how to model
16 common-cause failure analysis, it's tough to tell them
17 to do it right. So what we did is we basically said,
18 we'd like you to address common-cause failure analysis
19 and tell us basically what are your assumptions, what's
20 the basis for why you did that, and we can look at
21 that see how well it captures the expectations today
22 of how one might express common-cause failure.

23 Now, one of the things I think is very
24 clear here is the average PRA reviewer is not going to
25 have lot of knowledge about digital I&C systems,

NEAL R. GROSS

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

1 certainly in coming to the working on this TWG. I
2 gained a lot of knowledge about digital I&C systems,
3 and given how we've streamlined our review process, it
4 would be very difficult for every reviewer to come in
5 and get up to the same level of knowledge at least
6 that I've gotten to.

7 So our expectation is that the PRA
8 reviewers will be very heavily coordinating their
9 review with the digital I&C reviewer because that's
10 where the real expertise and insights into the system
11 itself belie in the review process.

12 Next slide, please.

13 So our path forward right now is I'm in
14 the process of revising the ISG to take into account
15 the subcommittee's comments and some other comments
16 that we've gotten, and we're hoping in the next month
17 or so to get the ISG out in final form.

18 And that finishes my presentation.

19 DR. APOSTOLAKIS: Good job. I would like
20 to make a few comments on this.

21 First of all, I think this is a good
22 example of a very useful and productive interactions
23 between the subcommittee and the staff. It was not
24 really contentious. I mean these are hard issues. We
25 expressed some views, the staff expressed views. 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 not sure. I don't think we really disagreed on
2 anything and I'm very pleased that the staff, as Glenn
3 said, is rewriting the ISG to reflect some of the
4 conclusions, so to speak, of our interaction.

5 This is a very hard problem. Just to
6 elaborate a little bit. There were I believe 14 steps
7 for the standard review in there to be supplemented by
8 10 steps, and these include both failure mode
9 evaluation, or the identification of failure modes and
10 probabilities. And this issue of sensitivity studies
11 on the probabilities was something that was discussed
12 a lot.

13 As Glenn said, first of all, we don't want
14 to give the impression to anybody that these
15 probabilities are somehow meaningful and we want to do
16 sensitivity studies to see what happens because my
17 personal view is they're not meaningful. And I went
18 back to AP-1000 and looked at the data they have there
19 and all you can find is the common-cause failures of
20 a number of digital systems. The rate is $1.2 \cdot 10^{-6}$,
21 but you find no evidence supporting arguments why that
22 is so.

23 And so if you take that number, then you
24 say, I'll multiply by ten and see what happens, so
25 100, and, of course, the issue of sensitivity studies

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 itself is not well defined. I mean where do you stop?
2 Do you multiply by 1,000? Do you go all the way until
3 you have a probability of failure rate of 3.

4 (Laughter.)

5 DR. CORRADINI: That would be unique.

6 DR. APOSTOLAKIS: And we sort of objected
7 to that. The staff did not object to our objection.
8 And it all comes down, as I said earlier, to the issue
9 of the question: do we really understand how these
10 things can fail?

11 I don't think that the state of the art
12 right now is such to say, yes, we have a fairly good
13 understanding. We don't. So the focus really should
14 be on that, and not only on this particular ISG, but
15 also in future activities of the staff, we have to
16 make sure we have a better understanding, we improve
17 our understanding of failure modes. So this was the
18 main subject of discussion and it was very good
19 interaction, very good interaction.

20 DR. STETKAR: I wanted to ask a question.
21 This is kind of in preparation for the upcoming
22 subcommittee meeting.

23 There's a lot of discussion of PRA of
24 digital I&C systems, and in kind of a simple sense one
25 can separate that into the models and the

NEAL R. GROSS

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

1 quantification of those models for the hardware, the
2 microprocessors and so forth, and the associated
3 software recognizing that the line between those two
4 may not be as clear as I've defined. But for the
5 purpose of this discussion let me do that.

6 In your opinion, where are the larger
7 challenges these days, or the largest challenges in
8 the risk assessment of the digital I&C? You mentioned
9 that there isn't very much experience; there isn't
10 very much guidance for this fuzzy thing we call
11 digital I&C. Are you more concerned in the software
12 area or are you more concerned in the modeling of the
13 hardware itself?

14 MR. KELLY: I believe that today the
15 majority of the concern is in the software. The
16 software has some very, very unique challenges. The
17 type of challenges that you run into is that you
18 timing issues about when something fails. You can
19 create loops. You can have dependencies on things
20 that have happened before or things that may happen in
21 the future.

22 None of those things that I just mentioned
23 are well handled by our traditional event tree, fault
24 trees that most PRA analysts at nuclear power plants
25 routinely work with. I spent the last two days 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 through looking at a draft report on dynamic methods
2 and my own personal opinion about that is that it's
3 not clear to me that the dynamic methods offer a
4 solution to doing a good job in a model. There are
5 just a number of issues associated with dynamic
6 modeling.

7 So I just think in general at this point
8 it's going to be very difficult to model the effect
9 that a digital I&C system might have. And one of the
10 major things that's associated with it, I mean the
11 reality is that if the systems have -- if the hardware
12 has a reasonable reliability and the if the software
13 has a reasonable reliability, if we're just talking
14 about single failures of components and things like
15 that, that's really not going to be an issue. The way
16 they've designed the systems, it's not going to cause
17 you to go to core damage. It's not going to cause a
18 lot of big problems.

19 The problem is really going to come with
20 the common-cause failure and how far does the common-
21 cause failure propagate. What's the probability that
22 the frequency with which you actually get these
23 common-cause failures, there are issues with how you
24 even handle something like that because the common-
25 cause failure itself potentially resides in the

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

1 software for all time. It's there or it isn't there.
2 And so treating that is a random variable as some
3 issues associated with that.

4 But even if you can get around that, then
5 generally what you're talking about is you have some
6 causative event, some event that's going to run you
7 through a different loop of your software that you had
8 before, give you different inputs that you had before
9 that's all of a sudden is going to give you this
10 common-cause failure.

11 Now, assuming that the common-cause
12 failure exists in the software, is the initiating
13 event that could maybe, and this is where my knowledge
14 gets a little fuzzy, is this something that can
15 simultaneously lock up the computer screens and affect
16 the ESF? Exactly how far can this thing go? What
17 kind of failures can I really end up getting? I don't
18 think we really understand those very clearly. So we
19 have a few uncertainties. Let's put it that way.

20 DR. STETKAR: Thanks. We're running short
21 on time.

22 MR. KELLY: I'm sorry.

23 DR. STETKAR: No. Thanks for your
24 insights because part of what we're looking at in the
25 subcommittee and broader in the committee are the

1 applicability of PRA methods to handle digital I&C
2 problems and I wanted to be sure that when we're
3 looking at that very, very broad problem that we're
4 focusing our attention in the areas where we think we
5 have the greater lack of understanding and lack of
6 knowledge, in other words, that, if indeed, the
7 software is the larger concern and the area where our
8 current experience and methods may be lacking, that we
9 should focus more in that area rather than how one
10 models a chip, or a solder connection on a print
11 circuit board, or wires between CPUs, or things like
12 that.

13 MR. KELLY: I think it's very important
14 that we very carefully define what it is that we need
15 to understand, determine, and then work towards that
16 goal.

17 DR. STETKAR: Thanks.

18 DR. APOSTOLAKIS: I think next week on the
19 17th there is a subcommittee meeting on one effort to
20 say something about the risk. So a lot of these
21 issues will come up again.

22 Any other comments, questions? Thank you,
23 Glenn.

24 The next one is operating experience.

25 MR. WATERMAN: I'm Mike Waterman. I'm

NEAL R. GROSS

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

1 with the Office of Research in the division of
2 engineering, and I'm here today to talk about our
3 review of operational experience and classification of
4 systems. And all of this arose out of a presentation
5 we did I think last year, or something like that,
6 where we were talking about developing diversity
7 strategies that a licensee could use to facilitate
8 more rapid approval of submitted systems, and
9 strategies that could reasonably address most of the
10 common-cause failures that occur.

11 I believe it was Dr. Apostolakis pointed
12 out that if we're going to develop diversity
13 strategies, we probably ought to know what kind of
14 failures the strategies are to address, and so,
15 therefore, we ought to go out and take a look at what
16 kind of failures have occurred not only in the nuclear
17 industry, but in other industries. We had actually
18 already started a project to do that and the ACRS'
19 recommendation just reinforced that goal.

20 Additionally, it was recommended that we
21 not only consider what kind of failures had occurred
22 when we're developing diversity strategies, but what
23 kind of systems are these diversity strategies going
24 to fit into. A particular strategy might be great for
25 a reactor protection system, but it may not be so good

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 for engineered safety features actuation system. So,
2 therefore, we should go out and do an inventory of
3 what kind of systems were out there, what kind of
4 digital systems were going to be implemented, what
5 kind of systems were already in existence, and
6 consider those when we were developing the diversity
7 strategies so we had strategies that would cover a
8 gamut of things.

9 Next slide, please.

10 And so that's essentially what we've been
11 doing. And the idea is as we come up with the
12 diversity strategies, which have been developed in
13 draft form by the Oak Ridge National Laboratory under
14 the research, that we can start using that failure
15 criteria to assess how good those strategies are.

16 Next slide, please.

17 Some of the things we've discovered in
18 looking around the world are that our concerns with
19 the possibility of software common-cause failure are
20 valid. We've seen lots of failures. We've seen
21 things such as the Aryan problem with the French Aryan
22 thing. Switching system 7 failure telecommunications.
23 There was a software error apparently in the northeast
24 grid blackout that occurred a few years ago. Ad
25 infinitum.

NEAL R. GROSS

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

1 What we have found, most of the failure
2 data that we've looked at is the failure to report a
3 very high level system reset, software failed. Those
4 kind of failure reports. You know, software,
5 something happened to the system and the plane started
6 losing altitude and we shut off the automatic pilot
7 and turned it back on; everything worked fine. That's
8 typically the level of detail we've been getting.

9 Now, that's not a very good level of
10 detail for actually developing a diversity strategy
11 where you're considered, you know, should be use
12 timing.

13 DR. SIEBER: Just shut it off.

14 MR. WATERMAN: That's scarce detail and
15 causes of failures is making the collection of the
16 data fairly interesting. One of the recommendations
17 that we got out of our last subcommittee meeting is
18 that instead of just looking at safety related
19 systems, we ought to really be looking at systems
20 that, if you will, are at a software integrity level
21 3 level instead of just at the integrity level 4.

22 Now, integrity level 4 and 3, when we were
23 writing IEEE 1012 -- well, I was on the working group
24 for IEEE 1012. When we were writing that standard, we
25 introduced the idea of software integrity level so we

1 could, if you will, parse out how much level of detail
2 you put into a particular verification and validation
3 project.

4 And integrity level 4 were systems where
5 if the systems failed lots of people died, businesses
6 went out of business, financial institutions lost lots
7 of money, those kind of really serious events, and
8 integrity level 3 systems were maybe only one person
9 dies or there's serious injuries, and business loses
10 money, but they don't go out of business, and things
11 like that, and Dr. Stetkar pointed out that feedwater
12 systems, for example, at a nuclear power plant, are
13 not safety systems. We don't regulate those.

14 But when they fail, the company loses a
15 lot of money, and, consequently, when they put in a
16 digital feedwater system, they want it to be very high
17 quality. That's an availability issue, not really
18 safety issue because the design basis of the plant can
19 handle that, but it's an availability. If the plant
20 shuts down, the licensee loses lots of money, and so
21 they put a lot of effort into that, so we should be
22 taking a look at those systems, too, because they have
23 good quality. So when they fail, we ought to be
24 considering that failure data.

25 As far as the root cause analysis, you get

NEAL R. GROSS

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

1 into this obsolescence thing. People are putting in
2 digital systems because analog systems are becoming
3 obsolete. Boy, you talk about obsolescence occurring
4 fast. You look at digital systems and see how fast
5 they become obsolescent.

6 And so for root cause analysis, it's
7 really nice to have somebody around who's familiar
8 with a system to such a point that when a system fails
9 they've got years of experience. They can say, yes,
10 that component fails all the time; that's what causes
11 it. When you've got these new digital systems coming
12 in, where's the base of expertise? It's certainly not
13 year and year of expertise on a 286 because nobody
14 uses an Intel 286 any more.

15 And so the new systems coming in for doing
16 root cause analysis is a whole new field. As a matter
17 of fact, IEEE had considered doing a standard on root
18 cause analysis through the nuclear power engineering
19 committee just to define here's how you do root cause
20 analysis. And they're not doing that now because it's
21 a very complicated problem.

22 Next slide.

23 DR. BLEY: Mike?

24 MR. WATERMAN: Yes.

25 DR. BLEY: In going through this data,

NEAL R. GROSS

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

1 especially the common-cause failure stuff, have you
2 been able to generalize some categories, functional
3 categories of causes for the common-cause failures
4 that probably would apply across all these different
5 specific systems?

6 MR. WATERMAN: Well, you could do the high
7 level categorization, three classes of failure, right?
8 You have your failures in design and specification
9 where the main expertise, possibly, wasn't
10 incorporated into coming up with the right specs and
11 the right requirements. And then you've got the
12 translation failures where, no matter how good the
13 spec is, no matter how good the design is, when it
14 comes to implementing it, somebody screwed up, you
15 know, typing a Zero instead of an O, and a variable
16 name for example, or something like that, or not doing
17 verification validation not finding the errors that
18 were incorporated by the coder or something like that.

19 And then you have that last class, the
20 operation error. You've got a system that's fault
21 free, if you will, but nothing is fool proof because
22 fools are so ingenious, and a CPU card is slid in on
23 hot mode and none of the memory locations have been
24 initialized to plant conditions for example, like the
25 kind that's a system failure that we saw just recently

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 here.

2 So those three classes of failures there,
3 you could subdivide it down into failures in deriving
4 a design out of specification, failures in life cycle
5 process if you will where verification validation
6 could have been better, and things like that. But we
7 haven't got enough data right now that we could
8 actually pin it down and say, ah, timing is a big
9 issue, for example, in software or order of execution
10 is a big issue. We're still working on that.

11 That kind of data would be terrific to
12 have because that's what you need to actually develop
13 a diversity strategy.

14 DR. BLEY: I think until you can get that
15 kind of functional level ordering, it's --

16 MR. WATERMAN: But that doesn't mean we
17 can't come up with diversity strategies right now, and
18 we have come up with three different diversity
19 strategies mostly focused around design, a design that
20 incorporates completely different technologies, analog
21 and digital for example. That kind of diversity.

22 Or I think the second strategy is a design
23 that incorporates digital technology for example, but
24 the technology itself is radically different within
25 the technology, for example microprocessor versus 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 field programmable gate array, something like that.
2 And then you've the third strategy where you're using
3 microprocessors for example, but you're using
4 different manufacturers of microprocessors, for
5 example Intel versus AMD, for example risk reduced
6 instruction set computer versus a complex instruction
7 set computer.

8 DR. SIEBER: That brings up a problem that
9 I think you're going to face in the future. If you
10 look at a power plant that was built to last 40 years,
11 maybe 60 years, these digital systems are not going to
12 have that kind of life time, and the initial failures
13 are going to be this processor failed, that module
14 failed, and you're going to go out to buy it and you
15 aren't going to be able to buy it, and so there's
16 going to be a substitution; and it's going to be done
17 in a hurry and the compatibility and your ability to
18 go through and do flow testing for open loops and all
19 that kind of stuff is the plant's availability is
20 going to pressure you to do that pretty fast, and I
21 think you're going to be in this business a lot more
22 than you think you are because things are going to
23 change that fast.

24 MR. WATERMAN: And licensees have
25 attempted to address that by, for example, purchasing

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 enough microprocessors, Intel 286s for example, to
2 last 20 years. The problem with that is that a few
3 years down the road when they go to the website to
4 find out what new problems have come up, they find out
5 Intel no longer supports that processor and they're
6 not longer updating the information. And so you've
7 got all the spare parts, but you really don't know
8 what the performance is years down the road.

9 And the other thing is is I've seen the
10 case where a designer has said we're going to use the
11 286 chip, even though faster chips are available,
12 because we know the 286, we've been using it for
13 years, and, therefore, we're going to do it with the
14 286. And then they implement the 286 and the
15 configuration has never been implemented in before,
16 for example master slave microprocessors.

17 DR. SIEBER: And the development by the
18 manufacturers has stopped so you're dead in the water
19 with that.

20 DR. APOSTOLAKIS: Coming back to the issue
21 of categorizations, let's listen, please. Our
22 consultant brought to my attention that there has been
23 some literature where they try to create classes of
24 failures of the processor, for example early response,
25 late response, no response. I think that kind 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. categorization would go along with what Dennis said.
2. I guess you agree?

3. MR. WATERMAN: Absolutely.

4. DR. APOSTOLAKIS: Okay.

5. DR. STETKAR: The only thing I'd warn
6. about that, and I think it's a good idea because it's
7. good to have classes to throw things into, just don't
8. make them too rigid initially. I remember in the
9. early days of risk assessment when we started looking
10. at events, the idea was to have a classification
11. scheme first and then force fit everything into the
12. boxes you had defined, and sometimes that doesn't work
13. so well.

14. DR. APOSTOLAKIS: No, no. But in terms
15. of giving some broad view to the --

16. DR. STETKAR: Right, right.

17. DR. APOSTOLAKIS: -- looking for, I think
18. that would be a useful thing.

19. DR. STETKAR: I guess what I'm saying is
20. don't codify the classification scheme and force all
21. of the experience to fit the --

22. DR. APOSTOLAKIS: Right. Okay, Mike.
23. What else do you have to say?

24. MR. WATERMAN: Next slide, please. Isn't
25. it interesting that it's my fault we're behind

NEAL R. GROSS

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

1 schedule.

2 (Laughter.)

3 MR. WATERMAN: We're also doing the
4 classification where the path forward is, obviously,
5 we're going to continue together with failure
6 information. The type of failure is really important
7 because you tend to think of failure, oh, just quit
8 operating. You know, it doesn't work as well any
9 more. Sometimes failures have the downstream effect
10 and the failure may be the system continues to operate
11 but it's just a little misleading.

12 You know, if you think about Three Mile
13 Island was not a failure of a PORV or a feedwater
14 system, it was the operator's interpretation of what
15 to do after it failed, right? The operator was
16 misled, so that's a class of failures right there in
17 the digital system, and it's just like, is the failure
18 subtle enough that the operator is misled and how they
19 are to respond.

20 As you can see off of our path forward,
21 we're working on the draft strategies now. It's not
22 ready for prime time. I may be working with the
23 contractor a little bit to refine those strategies.

24 We'll continue to develop our inventory of
25 new and existing digital systems so we can fit 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 strategies in and see how well they work, and that's
2 it.

3 DR. APOSTOLAKIS: Thank you.

4 MR. BAILEY: That's it. Anything else for
5 the staff?

6 MR. HILAND: Before we leave the NRC's
7 presentation, could I make one additional comment?

8 DR. APOSTOLAKIS: Sure.

9 MR. HILAND: Regarding the dialogue we had
10 on the current licensing review for the Duke
11 submittal, and I'm just going to parrot what I said to
12 the Commission on Monday regarding that submittal is
13 the licensee has chosen not to follow IEEE 1012 and
14 that's an IEEE standard we've endorsed by our
15 regulatory guides. It deals with V&V and so that's a
16 challenge that the staff will have.

17 In addition, there are several other
18 regulatory guides that endorse IEEE standards
19 involving software QA documentation, and our initial
20 look in our acceptance review, they've taken a lot of
21 exceptions. And so when we were talking about the
22 length of time and the amount of effort, as you know,
23 a licensee doesn't have to follow a regulatory guide.
24 That's only one acceptable method and so we're going
25 to focus on those activities very early in our 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 to make sure if there's a red flag that has to up,
2 it'll go up early.

3 But that's just a head up.

4 DR. STETKAR: Just I'm curious. Is that
5 because of the particular platform that they're using
6 and where it's coming from, or is it the decision of
7 the licensee? Only because the licensee's personal,
8 only because of the experience from that particular
9 platform in applications in Europe for example.

10 MR. KEMPER: It seems to be rooted in
11 that. It's basic. It's a particular vendor that
12 we're dealing with which is a European-based vendor.

13 DR. STETKAR: But I was just curious
14 because there is a lot of experience in Europe --

15 MR. KEMPER: Right.

16 DR. STETKAR: -- with that platform.

17 DR. APOSTOLAKIS: Now, when a licensee
18 uses an item list, you must have reviewed that
19 standard, right?

20 MR. KEMPER: Yes, typically we endorse
21 those.

22 DR. APOSTOLAKIS: Because -- that the
23 Agency has not reviewed?

24 MR. KEMPER: They can, they can. They
25 certainly can, they can submit that. We 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 evaluate that. We would evaluate the merits of the
2 plant form itself based on that standard.

3 For example, we got an application from
4 Wolf Creek that used an aviation standard, DO218 I
5 think it is, to qualify their FEGA application. Well,
6 of course, we don't endorse that. So the first
7 question we asked was how does that comply or comport
8 to Reg Guide 1. -- excuse me, IEEE 74.32 because
9 that's the primary document that we would use to
10 approve a computer-based system. And they did that.
11 And since then we understand what they did and we've
12 moved down the process and things are going along
13 quite well with that application quite frankly.

14 DR. APOSTOLAKIS: Are you happy with the
15 IEEE standards?

16 MR. KEMPER: Well, I am.

17 DR. STETKAR: It's a matter of time and
18 effort.

19 DR. APOSTOLAKIS: It seems to me that
20 somebody decided that you should never be allowed to
21 use one standard. They always refer you to another
22 one, and the other one refers you to another one, and
23 then you complete the cycle and come back to the
24 original standard.

25 DR. SIEBER: Endless loop.

1 DR. APOSTOLAKIS: Endless loop.

2 MR. KEMPER: This is true.

3 DR. APOSTOLAKIS: Speaking of failure
4 modes.

5 (Laughter.)

6 DR. APOSTOLAKIS: So if you guys are
7 happy, we're happy.

8 MR. KEMPER: Good to hear, thank you.

9 DR. APOSTOLAKIS: Okay. So the next is,
10 what, industry comments. Please, go ahead.

11 MR. CLEFTON: Good morning. I'm Gordon
12 Clefton. I'm with NEI. The subcommittee asked us to
13 bring a presentation of our evaluation research on
14 operating experience that the industry's been doing.

15 Just as a lead-in to that, I'd like to
16 point out that I'm the lead of the shadow organization
17 that Jack referred to earlier that I got seven TWG
18 industry people that support the NRC. We've got
19 probably 150 to 175 people ranging from operators to
20 senior vice presidents assisting us to make sure that
21 we speak as one voice and have a feeling together of
22 how we can make the industry successful in the
23 implementation of application of digital I&C.

24 We really looked at the fact that that's
25 the future of the nuclear industry. We need it for

NEAL R. GROSS

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

1 .obsolescence, we need it for futures available, and
2 we're doing everything we can to assist in the
3 approval of the packages that we submit.

4 Need to go on to a couple of slides here
5 today.

6 Just quick moments to talk about our
7 objectives and, as you can see here, our shadow
8 organization matches what the NRC is doing. We're
9 looking for safety focus applications. We're looking
10 for stable, predictable, timely licensing process and
11 guidance. That's significant right now in the fact
12 that the regulatory risk associated with submitting
13 applications is threatening the submittal of
14 applications.

15 We've talked about the Duke Oconee
16 package. The industry is watching that one very
17 closely.

18 We have a need for continuing level of
19 coordination, cooperation between the NRC and the
20 industry, and we're looking for consistency in the
21 processes. We've got a management structure that's in
22 place that identifies the issues. We're moving them
23 to resolution in a disciplined manner. It's been
24 identified earlier. With this we think we can get
25 realistic guidance.

NEAL 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. APOSTOLAKIS: You spoke of the
2 regulatory activities. Surely you're not implying
3 that there are delays that are not justified on the
4 part of the staff? I mean the industry has complained
5 in the past that the staff is not moving quickly
6 enough, and so on. It seems to me that the staff is
7 dealing with very, very hard problems here, so you
8 probably acknowledge that.

9 MR. CLEFTON: Absolutely.

10 DR. APOSTOLAKIS: And are you doing
11 anything, in fact, to help this effort? In other
12 words, they have a project or projects on how to risk
13 inform the process. Do you have similar projects and
14 do they deal with defense in depth and diversity
15 issues? Do you have your parallel projects so
16 eventually we will have some intellectual meeting of
17 minds? Or are you just sitting back and waiting to
18 see what the staff will do?

19 MR. CLEFTON: No. We're absolutely
20 involved in producing projects, looking at
21 applications. Remember, we have digital in the plant.
22 The digital that's coming to the NRC for approval now
23 are those that would not screen out with 5059 process
24 saying that the plant was adequate to make decisions
25 of implementation.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 We've had digital feedwater systems for
2 many years that have been working successfully in the
3 power plant. We've got secondary aspects and such
4 that are out there that are practical in use already.

5 VICE-CHAIR BONACA: You know, one thing
6 that seems to be important from the presentation is
7 the proper classification characterization of failures
8 so that you build. I mean you're the only one who can
9 build a database.

10 MR. CLEFTON: That's true.

11 VICE-CHAIR BONACA: Because you have the
12 experience and it seems to be a critical element to me
13 if we cannot understand the other modes and the
14 effects, there is going to be very little progress.
15 And, again, I mean you can support that?

16 MR. CLEFTON: Yes. That's our
17 presentation today. We've brought the experts of Ray
18 and Bruce from the industry to speak to it. We'll get
19 to that with analysis in a moment.

20 VICE-CHAIR BONACA: But it's almost like,
21 how do you implement within an organization procedures
22 for sure that when issues arise they are properly
23 characterized, evaluated so there isn't just a blip
24 there that says something malfunctioned and that's it.

25 DR. APOSTOLAKIS: Yes.

NEAL R. GROSS

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

1 MR. CLEFTON: That's correct.

2 MR. TOROK: There's another part to your
3 question though. I think in regard to the industry
4 activities supporting a number of these ISGs. We
5 provided a number of white papers on specific issues.
6 We're continuing to work on more. The one we're
7 talking about today happens to involve operating
8 experience, but there are others in the areas of
9 defense in depth and diversity, in human factors,
10 cyber security, and risks, that's right, in the PRA
11 area. There have been white papers submitted and more
12 in progress.

13 DR. APOSTOLAKIS: Are we getting those
14 Girija, the committee?

15 MR. SHUKLA: Yes.

16 DR. APOSTOLAKIS: Is the committee getting
17 those white papers?

18 DR. SIEBER: No.

19 DR. APOSTOLAKIS: Okay.

20 MR. TOROK: Have you seen, for example,
21 when a common-cause failure applicability?

22 DR. APOSTOLAKIS: I think I saw it, yes.
23 I see so many documents.

24 MR. TOROK: So you're seeing some of
25 these.

1 DR. APOSTOLAKIS: That's good. But as
2 long as when you speak make it clear that we all have
3 a common problem and we're trying to understand it.

4 MR. TOROK: Yes, absolutely.

5 DR. APOSTOLAKIS: Rather than say the
6 regulatory instability and all that stuff.

7 MR. TOROK: That's a good point.

8 MR. CLEFTON: We're sharing the concerns
9 that the NRC has and resource capability of
10 handling --

11 DR. APOSTOLAKIS: Good.

12 MR. CLEFTON: -- so that they're aware and
13 we are that we can't expect a detailed design review
14 expect regulatory assurance and that's a very
15 difficult decision for a reviewer to make is how much
16 is enough is management pressure for schedule and
17 such, so we're working with the industry to try and
18 help the NRC to put our packages in order that they
19 can be reviewed the best that's possible and that
20 comes from good guidance. It's for the submitter and
21 for the reviewer. But the rules are the same as what
22 the NRC has.

23 We can go on to the next slide and talk in
24 conclusions.

25 What we've got is the project plan, which

NEAL R. GROSS

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

1 Duke Oconee is RPS, ESPS, the system that's in there
2 right now and the pilot project. We expect this to
3 validate the ISGs that are written and available to
4 us. This is of highest importance to us. We're
5 working on this. It's very significant in the
6 industry applications.

7 Duke's is pressed by time, as we talked
8 earlier, that they're looking at a 2009 installation
9 into unit 1, then unit 3, then unit 2. So they've got
10 several years of application. As you all know, we've
11 worked outages very carefully for months and months in
12 advance. These have to be approved so we've got a
13 thumbs up, go ahead with it far enough in advance to
14 implement.

15 That's why the package went in on the 31st
16 of January this year. We're working with the NRC to
17 try and refine differences in schedule where we can
18 progress on both sides effectively. The emphasis,
19 again, is on good strong guidance, stable,
20 predictable, and timely that's realistic, that we can
21 use.

22 What I'd like to do today is introduce Ray
23 Torok and Bruce Geddes. Bruce is from --

24 DR. APOSTOLAKIS: Before you do that, I'm
25 sure you addressed this to some people. You are

NEAL R. GROSS

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

1 heading a group, the shadow group?

2 MR. CLEFTON: Yes, sir. I have seven TWGs
3 that match the NRC's TWGs.

4 DR. APOSTOLAKIS: And you are representing
5 the industry, not NEI?

6 MR. CLEFTON: That's correct.

7 DR. APOSTOLAKIS: You are industry?

8 MR. CLEFTON: We are industry. Industry
9 are us.

10 DR. APOSTOLAKIS: Okay. You are working
11 with EPRI and NEI and so on?

12 MR. CLEFTON: INPO.

13 DR. APOSTOLAKIS: Yes, and INPO. But your
14 group consists primarily of industry group?

15 MR. CLEFTON: It's industry and vendors
16 and operators and managers.

17 DR. APOSTOLAKIS: Okay.

18 MR. CLEFTON: It's a combined interest.

19 DR. APOSTOLAKIS: Thank you.

20 DR. BLEY: I think you folks told us at
21 the subcommittee that your groups have been working
22 very closely --

23 MR. CLEFTON: Absolutely.

24 DR. BLEY: -- so that you've actually had
25 input into these ISGs on the way?

NEAL R. GROSS

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

1 MR. CLEFTON: And that's an ongoing
2 situation. We've got meetings working probably three
3 to five times a month with the different TWGs so that
4 can interface on the assistance of the industry that
5 we've got out there and make sure that the new plant
6 vendors are aware of what we're creating, and, of
7 course, the existing --

8 DR. BLEY: And you will be commenting
9 formally on the ISGs as well, is that right? Is that
10 something on the schedule today?

11 MR. CLEFTON: That's not on the schedule.

12 DR. BLEY: Okay.

13 DR. APOSTOLAKIS: Who's funding this
14 activity?

15 MR. CLEFTON: Each of the industry
16 participants are funding it separately. There's no
17 separate cash involved on it. The EPRI has their own
18 financial for some of their topical reports that come
19 out, but the gathering is --

20 DR. APOSTOLAKIS: Who decides that, in a
21 particular issue you need somebody to spend some time
22 investigating and doing some what we call research,
23 then it's members of this group that are doing this or
24 you are going and say, hey, you have a record of this;
25 why don't you look at this problem?

NEAL 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. CLEFTON: We have the advantage of
2 several of the members of the group are in management
3 positions that they can bring it from their own
4 organizations with no extra costs, so we don't have a
5 budget and a funded aspect associated with it.

6 DR. APOSTOLAKIS: Okay.

7 MR. CLEFTON: The spokesmen that typically
8 come to our meetings or participate by teleconference,
9 links in, or webcasts are tip of the iceberg, if you
10 will, of resources that are available in the industry,
11 so we haven't had to fund separate resource as such.
12 We've had volunteers step forward with each of the
13 topics.

14 DR. APOSTOLAKIS: Now, does EPRI have
15 parallel efforts? I mean do you have a research
16 project some place that is trying to develop something
17 like the staff has research projects in several
18 places?

19 MR. TOROK: We certainly have a research
20 area in instrumentation and control. Right now
21 several of the activities have been tailored to
22 support the NEI effort specifically.

23 DR. APOSTOLAKIS: Right, but they are
24 activities where you go to an organization and you
25 say, here is a problem; we'd like you to tell us what

1 to do about it in two years or a year, or whatever, a
2 typical research project in other words.

3 MR. TOROK: Well, yes, we have an internal
4 advisory structure that consists of representatives
5 from the various utility members of EPRI, and they
6 have to approve what we're working on.

7 DR. APOSTOLAKIS: But this is the
8 mechanics of it. Do you actually have such projects?

9 MR. TOROK: Yes, and the one we're going
10 to talk about is one of those projects. Right?

11 MR. CLEFTON: This one has come with a
12 collection of available digital related events. It's
13 of significance because we had to go through and
14 evaluate whether they were truly digital events.

15 DR. APOSTOLAKIS: Good.

16 MR. CLEFTON: And raise from EPRI versus
17 from Southern Engineering Services and who's
18 supporting NEI and EPRI on this issue, so it's a
19 representation of coming straight from the industry,
20 the people that are out there. This represents, what
21 do we have, a three-hour presentation that's now down
22 to a few a minutes, or 30 minutes.

23 DR. APOSTOLAKIS: So this --

24 MR. TOROK: We want to apologize for
25 putting you farther behind schedule.

NEAL R. GROSS

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

1 (Laughter.)

2 DR. APOSTOLAKIS: So this is an activity
3 that parallels what Mr. Waterman presented on behalf
4 of the staff?

5 MR. CLEFTON: It's actually in
6 cooperation.

7 DR. APOSTOLAKIS: It's brother?

8 MR. TOROK: Yes. I would call them
9 complimentary, but it's certainly on the same subject.

10 DR. APOSTOLAKIS: Now why do you always
11 have 10, 20 minutes? I mean would you mind if in one
12 of the subcommittee meetings you actually come and
13 spend an hour or two?

14 MR. TOROK: We would be happy --

15 DR. APOSTOLAKIS: I mean you fly from
16 California anyway.

17 MR. TOROK: We would be happy to come and
18 spend four hours with your subcommittee.

19 DR. APOSTOLAKIS: Okay. Let's make sure
20 that next we actually review what the industry is
21 doing in more detail. We're not going to write a
22 letter on it, but it's very informative because it
23 would be useful I think for us, especially for a
24 project like this to know the details, not just we are
25 trying to do the best job in the world. We all try.

NEAL R. GROSS

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

1 Some of us succeed.

2 MR. TOROK: We would certainly appreciate
3 that opportunity. And, in fact, not just for the
4 operating experience, but for the other areas, the
5 human factors, defense in depth, diversity, and so on.

6 DR. APOSTOLAKIS: I really would like
7 that. I really would like that to spend serious time
8 because usually we reserve 15, 20 minutes at the end
9 and here is the industry to tell us, you know, they
10 are doing something. We should get into it.

11 CHAIRMAN SHACK: That's it. We'd better
12 move on.

13 DR. APOSTOLAKIS: Mr. Riley wants to say
14 something.

15 MR. RILEY: I have something real quick.

16 DR. APOSTOLAKIS: Yes.

17 MR. RILEY: This is Jim Riley, director
18 engineering NEI. I just wanted to say we'd be happy
19 to provide or spend some more time with you folks
20 talking about the various things we have ongoing with
21 digital I&C.

22 One thing that I would like to just add a
23 minute more on because I think it's pretty important.
24 Gordon talked about it. NRC did, too. That we are
25 using a pilot plant concept on this, that's Oconee.

NEAL 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 have a separate task force set up within the NEI to
2 assist Oconee in their review of the NRC RAIs and as
3 the process goes through. The whole purpose of that
4 task force is to assist in any issues that come up,
5 generic issues not plant specific, during the staff's
6 review of the license amendment request. And, also,
7 to identify any new issues that maybe we hadn't
8 recognized when we were doing the ISGs.

9 The whole point in this is to try out the
10 ISGs and see how they actually work in application
11 and, hopefully, smooth them out so it's a much better
12 product when we're done. And we're just getting
13 started on that, but I think that's very important.
14 And I know we're working, the staff's well aware of
15 this, I think we're all working together on it and I
16 think it should help the final product quite a bit.

17 DR. APOSTOLAKIS: At some point it would
18 be useful I think for us, for the subcommittee at
19 least, to be briefed on this effort, if you don't
20 mind?

21 MR. RILEY: Happy to do that, too.

22 DR. APOSTOLAKIS: Because the actual
23 lessons learned from a practical application is really
24 where the action is or should. Thank you very much.

25 MR. RILEY: Thank you.

1 MR. TOROK: Okay. Well, first of all,
2 we'd like to thank you for the opportunity to come
3 back and talk to you about this EPRI project that's
4 ongoing in support of the NEI working group.

5 I'm Ray Torok. I'm the EPRI project
6 manager on this. Bruce Geddes is our principal
7 investigator supporting the project. That's why we're
8 both here. Bruce will answer the tough questions.

9 We, also, we presented some of the same
10 information to the ACR subcommittee on March 20th and
11 they were also very kind to us with suggestions about
12 things where we could do a better job or add
13 clarification.

14 So we've tried to react to some of that,
15 so we do have some new material here. That's sort of
16 a warning. I just didn't want you to stop paying
17 attention, think you were going to see the same thing
18 again.

19 We're going to briefly describe what we
20 did on the project, what we think the operating
21 experience is trying to tell us, and how we arrived at
22 those conclusions. And, of course, we'll give
23 something on the conclusions and recommendations
24 coming out of it.

25 Now, this project started for us as a

1 result of an ACRS recommendation to the staff to
2 investigate operating experience and come back and use
3 the lessons learned from it to refine the guidance,
4 the regulatory guidance on defense in depth and
5 diversity. And while we were not the staff, of
6 course, we recognized that that was a good idea and we
7 had the right mechanisms in place to pursue this
8 ourselves, so we started doing it.

9 The basic idea here was that we would look
10 into various published reports with NRC and INPO.
11 From NRC that means things like licensee event
12 reports, Part 21 notifications, event notifications,
13 and I may be forgetting some of them. From INPO, of
14 course, there are operating experience reports.

15 Now all of we looked at 322 reports over
16 a period of about 20 years in both 1E and non-1E
17 systems. Now, you notice there it says digital events
18 in quotes.

19 DR. ARMIJO: Yes. How do you define that?

20 MR. TOROK: We want to clarify that a
21 little bit because that caused some confusion the last
22 time. Basically, a digital event for the purposes of
23 this is anything that was reported that involved or
24 affected an digital system. Doesn't necessarily have
25 to be a failure, might be a plant trip, might be

NEAL R. GROSS

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

1 discovering some flaw in a digital system, anything
2 that was reported was fair game. Okay.

3 DR. ARMIJO: Just on that point. Last
4 year there was a failure in a digital feedwater
5 control system at Perry.

6 MR. TOROK: Yes.

7 DR. ARMIJO: Which if you keep peeling
8 that onion you get down to maybe a transformer failed
9 or parts of it.

10 MR. TOROK: Yes.

11 DR. ARMIJO: Is that in your analysis?

12 MR. TOROK: Yes. If it was reported -- in
13 that case, yes, that one is. But we also at some
14 point differentiated between events that were really
15 digital system failures or software failures and ones
16 that were caused by other things, and Bruce is going
17 to explain that in a few minutes.

18 But that's an excellent point because
19 there are a number of definitions you'll find us using
20 that are important to understand here. And that's one
21 of them, what's the difference between what we call a
22 software event and a non-software event.

23 For this purpose, a software event is
24 where, basically, a design flaw in the software was
25 involved, that sort of thing. Another way to think of

NEAL R. GROSS

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

1 it would be a problem that would affect a digital
2 system and happened because this was a digital system,
3 as opposed to one that would have happened the say way
4 for an analog system like a power supply failure or an
5 incorrect set point that would affect analog or
6 digital the same way. So we tried to break it down
7 that way, and, again, Bruce will show you that.

8 There are a couple of other things I
9 wanted to mention though. We used some other words.
10 Defect is one of them. What's a defect?

11 A defect is just a flaw somewhere in the
12 system. For software that typically would mean what
13 would be called a software fault or a bug.

14 MR. GEDDES: But it would also include
15 procedural issues or human error.

16 MR. TOROK: So it's fairly broad term the
17 way we're using it here.

18 The word failure, something actually
19 misbehaved one way or another. Now, it's important to
20 note for software, a software failure, that needs a
21 defect plus a trigger, and I think that was mentioned
22 earlier. A trigger is a set of conditions that causes
23 the software to do the wrong thing. Now, typically,
24 in a software-based system, the kind of thing that
25 does this is an unanticipated condition, something

NEAL R. GROSS

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

1 that wasn't anticipated in the design. So that's what
2 a failure is.

3 Now, we also talked about common defects.
4 A common defect is one that occurs in multiple
5 redundancies and can affect a redundant system. And
6 we also talked about a common-cause failure. Now,
7 here you need common defects plus concurrent triggers
8 if you're talking about a software failure that can
9 become a common-cause failure. And what you find is
10 that not every common defect can lead to a common-
11 cause failure, and Bruce will explain some of that
12 later. But I wanted to make sure we were all more or
13 less clear on those terms.

14 Now, at the back of the presentation
15 there's a list of key terms. It goes into more
16 detail. I don't think we need to go through the rest
17 of it now, but it's there for your reference.

18 Another thing that I wanted to point out
19 here was that we're only looking typically at problem
20 reports here, so we're not talking about positive
21 experience. We tend to focus on what went wrong and
22 there are a number of good reasons to do that.
23 There's a lot more to learn there typically. But
24 we're ignoring a lot of successful operating
25 experience.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 Core protection calculators have been
2 operating for a long time with not very many problems.
3 There are many instances of digital feedwater control
4 systems that have done a wonderful job of doing away
5 with the analog system problems. I know of somewhere
6 during the first startup transient with the new
7 digital feedwater system, it was credited with paying
8 for itself in the first startup just by being able to
9 handle transients that they couldn't handle before,
10 that would have let the plant trip. So there's a lot
11 of those kinds of experiences out of there that we're
12 not talking about.

13 Now, in one case, one of these digital
14 platforms that people have been talking about here,
15 they have a lot of experience, not in the nuclear
16 industry, but in others, in petrochem. They have over
17 6,000 units in service for I don't know how many
18 years. They're saying their total service time is in
19 excess of 450 million hours and they've never seen a
20 failure on demand.

21 Now the problem there is if you're trying
22 to generate statistics for PRA, you don't have a lot
23 to work with. So that's one of the things that makes
24 it so difficult. Now, in this case, one of the first
25 things that comes in your head is how many demands did

NEAL 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 have and how many failures if I'm worrying about
2 statistics? It's hard to get that data especially for
3 systems like these where they're designed to be
4 extremely robust.

5 They don't fail often, and that's one of
6 the problems with generating a statistical argument,
7 which drives us to consider things in regard to design
8 features that are typically built into these systems
9 which make them robust because they're not robust by
10 accident. They're designed to be that way. So I just
11 wanted to mention that.

12 Now, for our purposes, since we're
13 primarily trying to support the defense in depth and
14 diversity issue, our focus is on actual common-cause
15 failures that can disable systems or potential common-
16 cause failures that can disable systems. Things at
17 lower levels aren't so important for the purposes of
18 this discussion, although we did look at them. So
19 that's an important point.

20 We also wanted to capture insights in
21 regard to potential corrective measures that make
22 sense, depending on what we're seeing. One of them is
23 a diversity strategy like Mike talked about. What
24 kinds of diversity would have been helpful here? Or
25 another way of looking at it is, what kinds of

NEAL R. GROSS

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

1 diversity prove to be helpful in these events? And
2 we've seen some of that because it turns out that
3 there's a lot of internal diversity built into the
4 plant systems as it is and it turns out that's a good
5 thing, which should be a surprise. They were designed
6 by smart people.

7 So in regard to insights, there's
8 diversity. What kind of diversity would have been
9 helpful? And, also, what kinds of design in defensive
10 measures are proven to be helpful here? So we're
11 trying to look at those things to capture insights.

12 I should also mention that while the focus
13 here has been on the D3, the defense in depth and
14 diversity issue, and common-cause failures, a lot of
15 the insights that we get from these events, especially
16 the non-safety ones, have a lot of value in terms of
17 lessons learned that we can factor back into the
18 utilities and the processes to improve the way they
19 handle these systems.

20 So we have another project ongoing at EPRI
21 where we're working on that. We're taking selected
22 cases from the same set of information and building it
23 into our training program on digital upgrades. So
24 that's ongoing, too. I just wanted to point that out.

25 I wanted to very briefly go through what

NEAL R. GROSS

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

1 we're seeing here. In looking at these events, we
2 were trying to look at software errors in the broader
3 context of all the causes of potential and actual
4 common-cause failures that have been reported. Now,
5 when we did that, we discovered that software is a
6 relatively minor contributor. Although there have
7 been a number of actual common-cause failures and
8 potential common-cause failures, 49 of our 322 events
9 involved actual or potential common-cause failures.
10 Of those 49, eight involved software. So software has
11 not proven to be a big -- in practice over the last 20
12 years that software is not proving a major
13 contributor.

14 The more prevalent causes of the problems
15 have been things like incorrect set points, incorrect
16 system parameters, process issues, really, which, of
17 course, would be equally problematic for analog
18 systems. If the set points are wrong in multiple
19 redundancies of an analog system, you had problems
20 same as if it's in a digital system.

21 Also, for the non-safety systems, the
22 dominant cause was really hardware issues, and there
23 are a number of important differences between safety
24 and non-safety and Bruce will get into that later.

25 So while the numbers of events and the

1 numbers of common-cause failures and potential common-
2 cause failures are not large statistically speaking,
3 the operating experience shows no indication that the
4 introduction of software in these systems has been
5 particularly problematic in terms of -- compared to
6 other factors that can degrade reliability and safety.

7 On the contrary, the operating systems
8 suggest -- it certainly doesn't prove, but it suggests
9 that whatever is being done now in terms of design
10 practices and designed in features in these digital
11 systems, whatever is being done now to ensure that
12 they're very robust in regard to failures and common-
13 cause failures seems to be doing pretty well because,
14 as I said, software has not been a major contributor.

15 DR. ABDEL-KHALIK: Doesn't that depend on
16 the level of complexity of the software though?

17 MR. TOROK: That's an excellent point.
18 And, yes, absolutely, and we'll show you a little more
19 on that. That's an excellent point.

20 Now, with that, I'd like to turn it over
21 to Bruce who's going to show you how we looked at the
22 data and drew conclusions from it.

23 MR. GEDDES: Thanks Ray.

24 We actually read, evaluated,
25 characterized, and built a database for almost 322

NEAL R. GROSS

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

1 reports. You can see down the left hand side of this
2 figure, we used this pyramid construct to separate 1E
3 from non-1E, and we've got another slide that points
4 out the fundamental differences between the two types
5 of systems out there.

6 On the 1E side we found 49 reports.
7 Breaking that down further, 27 of them reported a
8 common defect. They did not all result, of course, in
9 a common-cause failure. Twenty-two single defects
10 were report, and out of those 27 common defect
11 reports, these are software or non-software defects
12 that are common and multiple redundancies, four of
13 them are related to software.

14 The other 23 were life cycle management,
15 parameter issues, set point issues, operator error, or
16 procedures, other kinds of defects that can result in
17 a failure at the system level, and what this means is
18 a loss of safety function. We saw zero, actual
19 common-cause failures on demand.

20 We did see six reports that could have led
21 to a possible system level failure. We are calling
22 those potential CCFs. One of them is software
23 related. The other five are non-software related, in
24 other words, about the same ratio of software to
25 non-software events.

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 Of the remaining common defects, we saw
2 ten single failures, in other words triggered into one
3 channel even though the defect was common on multiple
4 channels. We saw six spurious actuations, four
5 subsystem level meaning a trip function or some other
6 function of the system, could have led to a potential
7 CCF, one subsystem level actual CCF.

8 Next slide.

9 On the non-1E side, we see bigger numbers,
10 okay, and we have some fundamental differences between
11 like a 1E and non-1E systems that tend, we believe are
12 causing these numbers to be higher. Going, again,
13 down the left hand side of this figure, 273 non-1E
14 events, 77 of which contained a common defect.

15 Sir?

16 DR. STETKAR: Probably the largest
17 difference is the fact that there is many, many, many
18 more non-1E applications --

19 MR. GEDDES: Yes.

20 DR. STETKAR: -- than digital I&C, so it's
21 not necessarily correct to imply that the failure rate
22 is higher in non-1E because it's fundamentally
23 designed differently. There's just more of them out
24 there, so you're going to see more events. So the
25 implication is that they may not be as different as

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 you might think.

2 MR. GEDDES: Well, we do have some backup
3 slides on failure modes and there's been a lot of
4 discussion. We can give you a glimpse. Time
5 permitted, we can show you some failure modes of the
6 non-1E systems and it's important. Those failure
7 modes we don't believe are necessarily translatable
8 directly to the 1E systems.

9 DR. STETKAR: I just wanted to make sure.

10 MR. GEDDES: That's a very good point, but
11 we need to make both points together because there are
12 differences.

13 DR. BLEY: Two things on that. One, have
14 you ever tried to normalize them for the number of
15 systems out there? And, two, are you preparing a
16 report on this information that we might be able to
17 get a look at when it's done?

18 MR. GEDDES: Absolutely, yes. We have a
19 white paper that's coming out in May and a final EPRI
20 technical report that's later this year.

21 MR. TOROK: But the answer to the first
22 question was no, we haven't tried to normalize. And
23 to do that is a much more difficult problem. You have
24 to go back and capture the information on all the
25 other systems and 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 MR. GEDDES: Absolutely.

2 MR. TOROK: -- moving toward.

3 DR. BLEY: That was the hard part in doing
4 mechanical systems for ten years.

5 MR. TOROK: And we started talking about
6 whether that kind of effort is feasible, but we're not
7 doing anything there right now.

8 DR. STETKAR: I was going to wait until
9 the end, but you gave me a lead in and we may never
10 get to the end anyway.

11 You mentioned you have all of the
12 classification and evaluation you had done is based on
13 332 event reports, let me call it that. You've
14 obviously done some screening of the experience to
15 identify these 322 events. Have you made efforts to
16 go back to the plants and ferret out more details in
17 terms of what actually went on? In the staff's
18 presentation they mentioned some frustration. We used
19 to see throughout the PRA business of finding an event
20 report, the pump failed and the corrective action was
21 replace pump; or software failed and we reset the
22 processor. Did you make to actually go back to those
23 322 events and flush out more information? That's the
24 first question.

25 MR. GEDDES: Only in a couple of cases and

1 I can elaborate on that.

2 DR. STETKAR: Why only in a couple of
3 case?

4 MR. GEDDES: Well, we found in the reports
5 about half of the 322 reports were licensee event
6 reports, the other half are INPO operating experience
7 reports. And what we've seen over the 20 years is the
8 quality of the reporting has improved and we do see
9 there's three specific things that we can read
10 directly, black and white, in the reports: the cause
11 of the event, the failure mode of the event, and the
12 immediate corrective actions and the corrective
13 actions to prevent recurrence.

14 Those three pieces of information are in
15 these reports and readily available, and we felt like
16 that was enough for us to do this research. Now, we
17 will go back and do some more detailed review and
18 bring out more information in the final EPRI type of
19 a report on selected events.

20 DR. STETKAR: My point is that in the risk
21 assessment experience in areas, in some of these very,
22 very difficult areas, talking about common-cause
23 failures now of hardware pieces of equipment, diesel
24 generators, pumps, valves, those types of things, fire
25 events, human error events, in many, many cases

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 simplistic categorization of both the failure mode, if
2 I'll call it that, and the cause based on very, very
3 high level summaries often does not give you the type
4 of information that you really need to understand what
5 happened.

6 Now, I'll grant you that the resources, if
7 we're talking about 100,000 events, the resources
8 required to go back and delve into more details would
9 be daunting. But we're talking about 322 events here
10 and a lot of them, because of the history of digital
11 control systems, probably have occurred in the last 10
12 to 15 years. That's where implant documentation
13 tracking systems may be much better than what is
14 reported in an INPO report or an LER.

15 The reason I bring this up is that our
16 experience from PRA is sharing the information between
17 both the industry and the regulator at the level of a
18 detailed narrative of what actually happened
19 oftentimes leads to better understanding of the
20 problems, the scope, definitions of failures, and
21 things like that rather than tabulations of numbers of
22 events categorized into different boxes with summary
23 tables of numbers.

24 MR. TOROK: Well, there's two questions
25 going on here. Let me first say that a lot of the

NEAL R. GROSS

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

1 information came from INPO databases, and, of course,
2 we, EPRI, can't release INPO information on our own to
3 NRC or anybody else. However, we have been talking to
4 INPO about this, what can we give to NRC and so on,
5 and it looks like it will be feasible to just strip
6 selected information out of the reports and then
7 provide a lot more of the details to NRC and everybody
8 else. So we're trying to do that and we will to the
9 extent that we can.

10 Now, the other question had to do with
11 distribution of what was seen, and that's a hard
12 question. Bruce has to answer.

13 MR. GEDDES: If I may, I've picked up a
14 lot of discussion points listening to you all today
15 about failure modes. What are the failure modes? How
16 does software fail? And looking at the 20 non-1E
17 software events, and I apologize for having to look
18 sideways, but maybe I could stand up.

19 CHAIRMAN SHACK: No, no. You have to stay
20 down. You can't stand up and move around.

21 MR. GEDDES: This is a simple Pareto chart
22 of 20 software events on non-1E systems and these
23 might be the 20 that we go after instead of 322.

24 The first bin is eight. Eight of those
25 events were application logic errors. In other words,

NEAL R. GROSS

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

1 in any digital you've got an operating system with
2 fundamental core functions like accessing memory and
3 operating certain transfer functions. At the upper
4 end of the architecture is the application logic, the
5 function blocks that make the system do something
6 useful. These are errors in that logic at the
7 application level.

8 The next bin is buffer overflow. Those
9 could be and probably are operating system issues.
10 They could be an application call that does something
11 inappropriate. The designers of the application
12 didn't quite understand the -- didn't maybe not
13 completely how the operating system works, but these
14 are buffer overflows.

15 The next category is inadequate
16 indications or alarms. Somebody mentioned operators
17 trying to understand and diagnose an event. In this
18 case there's three of those.

19 Inadequate human machine interface
20 operating system issues. In some architectures you've
21 got a control layer, in other words, processors that
22 interface directly with the plant, and then a layer
23 above is a human machine interface system with a
24 client serve arrangement, that could go dark and the
25 control systems keep functioning. A typical feedwater

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 control or electrohydraulic system control might have
2 that architecture, especially with a larger DCS type
3 systems. So that's a case where the HMI failed, but
4 the plant kept operating.

5 The next bin is faulty deadband function.
6 That's a operating system issue where there's a
7 function block to insert a deadband into a processor
8 control and that function block had an error in it,
9 that the code inside the function block itself was
10 incorrect.

11 The next one is a faulty communication
12 function, another operating system core function
13 issue. The next to the last one is --

14 MR. TOROK: Incorrect exit call in
15 firmware.

16 MR. GEDDES: Incorrect exit call in
17 firmware, that's another operating system issue. An
18 incorrect signal range, that's an application issue.

19 So you can see a few operating system
20 issues and a few application issues. We think these
21 are interesting. We think these begin to answer the
22 question: how does software fail and how do those
23 failure modes propagate. I would argue I think that
24 application logic errors tend to be isolated within
25 particular systems, and operating system issues can

NEAL R. GROSS

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

1 propagate across the architecture.

2 Let's go back to where we were on the --

3 DR. APOSTOLAKIS: We have six minutes.

4 DR. ARMIJO: This is the interesting part,
5 George.

6 DR. BLEY: You'll leave us those extra
7 slides?

8 MR. TOROK: Yes, yes, we will.

9 MR. GEDDES: We can be here all day. I
10 can go to the airport, find out if the FAA will let me
11 go home or not. I don't know. It's Delta, but
12 they've given us a heads up.

13 Vulnerability of CCF, we do want to get
14 this point across. Looking at 1E systems,
15 independence and sharing of resources, those are the
16 fundamental differences. The triggers of the events
17 where there's a common defect quite often rely on that
18 these kinds of fundamental design attributes between
19 1E and non-1E.

20 In a non-1E system there's quite often a
21 master slave architecture with some kind of a shared
22 resource. It could be a back plane, a network
23 segment, a power, somebody mentioned a feedwater
24 event, the power supply issue, that was the shared
25 resource.

NEAL 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 some case even those shared resources
2 are redundant, but they might have diode connections,
3 and if those aren't configured properly or tested or
4 maintained properly, or they just fail, that can lead
5 to an event. And that's not necessarily a fault of
6 the digital system, but it does get involved in the
7 event and you don't see those fundamental design
8 attributes.

9 Independence is maintained in 1E systems
10 by regulation and that's a very, very important point.
11 To try to transfer those non-1E failure modes into 1E
12 systems, you have to transcend. You have to take into
13 account these fundamental design attributes and
14 understand the triggers that lead to events. That's
15 a very key takeaway here.

16 DR. STETKAR: However, I know in at least
17 one of the new reactor designs that we'll be looking
18 at for licensing in the United States you will see
19 safety-related 1E systems with that type of diode
20 backup sharing of things, so that for that particular
21 type of design this experience might be relevant.
22 That's the only point of not necessarily --

23 MR. GEDDES: I understand. It's not --

24 DR. STETKAR: -- separating between 1E and
25 non-1E.

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 DR. APOSTOLAKIS: How do you define
2 functional complexity?

3 MR. GEDDES: This is application level
4 complexity.

5 DR. APOSTOLAKIS: Is it a quantitative
6 metric?

7 MR. GEDDES: No, qualitative.

8 MR. TOROK: What it refers to really is
9 that in the 1E side, the system is typically just
10 looking at some input-censored data --

11 MR. GEDDES: Bistable functions versus
12 closed loop events control algorithms for feedwater --

13 MR. TOROK: It's just a trip. It's on and
14 off and that's all it is. Whereas, on the other side,
15 you've got feedback control, closed feedback and so
16 on.

17 MR. GEDDES: I think it's important for
18 the community to understand that 1E systems aren't
19 always quiescent, dormant, waiting for an event.
20 They're constantly scanning process values, comparing
21 them to a set point and writing in a zero or a 1 on a
22 millisecond level, constantly. They do the same thing
23 over and over whether there's a demand or not. When
24 there is a demand, it writes a 1 instead of a zero to
25 the reactor trip breakers. That's a very important

NEAL R. GROSS

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

(202) 234-4433

www.nealrgross.com

1 point.

2 DR. SIEBER: Let me ask this question. If
3 you show us this chart ten years from now, what will
4 change? For example, in ten years will there be
5 shared resources for 1E systems?

6 MR. GEDDES: No.

7 DR. SIEBER: Will you have functional
8 complexity, maybe become high for 1E systems? How is
9 this going to change and what's going to prevent it
10 from changing?

11 MR. GEDDES: I think the 1E column is a
12 function of regulation, and the non-1E column is a
13 function of plant reliability and availability, and
14 we're learning. You notice formal software quality
15 assurance methods varies under -- but it's improving.

16 There's nothing like a reactor trip to be
17 a learning opportunity for an I&C engineer. And
18 that's what's happening in the non-1E column. We are
19 improving dramatically on the non-1E side and in ten
20 years I expect event free operation.

21 DR. SIEBER: Well, a lot of the trips of
22 the plants are pretty events, you know. It's too hot,
23 you trip it. Flux is too high, you trip it, and so
24 forth. As opposed to control systems particularly --

25 CHAIRMAN SHACK: Jack, we had better let

NEAL R. GROSS

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

1 them finish.

2 DR. SIEBER: -- integrated control systems
3 where it's altogether different.

4 MR. TOROK: We would be happy to come back
5 later.

6 DR. APOSTOLAKIS: Yes, I think you would
7 do that. Tell us --

8 MR. TOROK: There's a point down -- we
9 need the red box here.

10 MR. GEDDES: I think we've covered that.

11 MR. TOROK: The 1E systems are much better
12 protected for a bunch of reasons.

13 DR. APOSTOLAKIS: Good.

14 MR. TOROK: Now we're there, right. Same
15 thing we said before, software has not been
16 particularly problematic compared to the other
17 contributors to common-cause failure which suggests
18 that the designers and users of these types of
19 equipment have learned how to do pretty well. The 1E
20 and non-1E is still apples and kumquats. It's tough
21 to compare and we tried to explain why, although there
22 are a lot of good lessons learned from both.

23 Recommendation wise, we agree with Mike.
24 Let's keep looking at things, at information from
25 whatever sources we have, and let's start thinking

NEAL 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 factoring this back into the D3 guidance as
2 suggested earlier.

3 Now, I was just going to point to this.
4 We've got some other things we saw which were kind of
5 interesting, like there are many cases where, in doing
6 corrective actions for a non-software-related issue,
7 a hardware failure perhaps, added features were put in
8 in software to protect against that from happening
9 again, which is really nice. They're using software
10 for what it's good at. So that was encouraging.

11 We also saw events that confirmed the
12 effectiveness of certain kinds of diversity, in this
13 case signal diversity and functional diversity. For
14 example, reactor protection systems have lots of
15 different signals. They can all start trips. That's
16 a good thing. We don't want to do away with that.

17 On the other hand, we saw no events where
18 using platform diversity and redundant trains of a
19 system seemed to be the right thing to fix the
20 problem. Because the problems weren't coming from the
21 platforms, they were coming the application code, set
22 points and requirements, and things like that, not
23 from the base platforms.

24 I mentioned the last one already. So
25 we're 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 DR. ARMIJO: This is not my area, so it
2 may be a dumb question. These operating system
3 errors, what do you do to fix them or how do you test
4 these systems in advance to be sure these errors are
5 not there?

6 MR. TOROK: That's a good question.
7 That's where I mentioned so-called defensive measures
8 here. There's a difference between a good operating
9 system or a good platform and a bad one. Now, 15
10 years ago, I'd say we didn't know that much about how
11 to figure out which were the good ones and which were
12 the bad ones. We know a lot more about it now.

13 And I'll give you a couple of easy
14 examples.

15 MR. GEDDES: Based on non-safety system
16 experience.

17 DR. ARMIJO: Right.

18 MR. TOROK: Yes. For example, everyone's
19 heard of the Y2K problem. Well, that happens when
20 operating systems try to track dates and they tangled
21 up over that. So if you're evaluating a system before
22 you put it into a critical application, safety or
23 non-safety, one of the things you want to do is look
24 inside the box and make sure it's not using dates, or
25 if it is, it's doing it very carefully.

NEAL R. GROSS

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

1 MR. GEDDES: Or turn that feature off.

2 MR. TOROK: Yes. Now, another example
3 might be in a well-designed system for critical
4 applications. What the operating system does, it's
5 functions don't change at all during a plant
6 transient. It just does the same thing over and over
7 again. It reads data; it ships data someplace else.
8 It can't tell that a transient's going on.

9 The reason that's important is because you
10 can have all the bugs you want in that operating
11 system and a plant transient can't trigger them. So
12 it eliminates the operating system as a contributor to
13 common-cause failure. So you're looking for those
14 kinds of design features when you evaluate these
15 systems before you before you put them.

16 And there are many other things. We call
17 them defensive measures. And from our standpoint
18 that's one of my soap boxes I guess. I'd say these
19 systems are reliable, well, in part because they have
20 good development processes behind them, but maybe more
21 importantly because they have good designs with lots
22 of the right kinds of designed-in defensive measures.
23 And so we're working more on methods to credit that.

24 DR. APOSTOLAKIS: I think future meetings
25 have to be structured better so we have more time to

NEAL R. GROSS

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

1 go into the interesting stuff. But let's start with
2 the subcommittee meetings where you will have a
3 stronger presence.

4 I'd like to thank you, gentlemen, and also
5 the staff for very informative presentations today,
6 and back to you, Mr. Chairman, on time.

7 (Laughter.)

8 MR. BAILEY: Let's take a ten minute break
9 and then we'll try to catch up on some of that time
10 that we've lost.

11 (Whereupon, the foregoing matter
12 went off the record at 11:07 a.m.)

13

14

15

16

17

18

19

20

21

22

23

24

25

CERTIFICATE

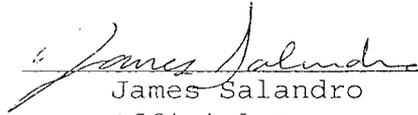
This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission in the matter of:

Name of Proceeding: Advisory Committee on
Reactor Safeguards

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.


James Salandro
Official Reporter
Neal R. Gross & Co., Inc.

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

(202) 234-4433

www.nealrgross.com



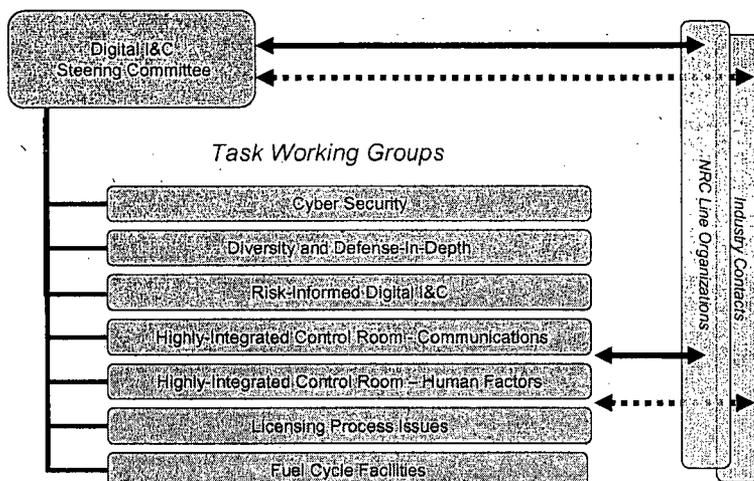
DIGITAL INSTRUMENTATION AND CONTROL Steering Committee Review

Advisory Committee on Reactor Safeguards
April 11, 2008

John Grobe, Chairman
Digital Instrumentation and Control Steering Committee



DI&C STEERING COMMITTEE PROJECT STRUCTURE





DI&C STEERING COMMITTEE

- **Oversee and Provide Direction to 7 DI&C Task Working Groups**
 - **Activities Since October 2007**
 - **18 Public Task Working Group Meetings**
 - **3 Public Steering Committee Meetings**
 - **1 New Task Working Group Established**
 - **Fuel Cycle Facilities**
 - **1 Interim Staff Guidance Issued: Cyber Security**
 - **1 Interim Staff Guidance near completion: Probabilistic Risk Assessments**
 - **Developing Interim Staff Guidance on Licensing Process**

ACRS Presentation - April 11, 2008

Slide 3 of 29



DI&C STEERING COMMITTEE

- **Activities Since October 2007**
 - **March 14, 2008, Project Plan Revision Issued**
 - **17 Long Term Actions Identified to Retire ISGs**
 - **4 Industry Reports Received**
 - **Minimum Inventory of Human-System Interfaces**
 - **Computerized Procedures Design & Implementation Guidance for Procedures, Associated Automation and Soft Controls**
 - **Manual Operator Actions**
 - **Common Cause Failure Applicability**
 - **March 20, 2008 meeting with ACRS Digital I&C Sub-Committee**

ACRS Presentation - April 11, 2008

Slide 4 of 29



DI&C STEERING COMMITTEE

- **Remaining Interim Staff Guidance Documents**
 - 2008: Licensing Process
 - 2008: Manual Operator Actions
 - 2008: Fuel Cycle Facilities
 - 2009: Licensing Process that Incorporates Cyber Security
- **Industry Feedback**
 - Accept Industry Feedback
 - Revise ISGs If Applicable
 - Incorporate into Regulatory Infrastructure

ACRS Presentation - April 11, 2008

Slide 5 of 29



DI&C STEERING COMMITTEE

- **Retire Interim Staff Guidance Documents**
 - **Project Plan Includes 17 Long Term Actions**
 - Rulemaking, Standard Review Plan Revisions, Issuance of NUREGS and Regulatory Guides
 - Develop Tracking Methodology
 - **Standard Agency Processes including formal ACRS reviews**

ACRS Presentation - April 11, 2008

Slide 6 of 29

DIGITAL INSTRUMENTATION AND CONTROL Review of Cyber Security Interim Staff Guidance

**Mario Gareri, Division of Engineering,
Office of New Reactors**

CYBER SECURITY BACKGROUND

- RG 1.152 Rev 2, "Criteria For Use Of Computers In Safety Systems Of Nuclear Power Plants" addresses cyber security only as it relates to safety systems
- NEI 04-04 Rev 1 "Cyber Security Program for Power Reactors" addresses cyber security in general from a programmatic approach.



CYBER SECURITY BACKGROUND

- Task Working Group (TWG) was established to address industry concerns of possible conflicts between RG 1.152 Rev 2 and NEI 04-04 Rev 1.
- Analysis revealed some gaps and some overlaps but no inconsistencies/conflicts. Rather, the two documents are complementary.

ACRS Presentation - April 11, 2008

Slide 9 of 29



CYBER SECURITY BACKGROUND

- Industry committed to revise NEI 04-04 Rev 1 to better incorporate cyber security guidance for safety-related systems so that it could be used in lieu of RG 1.152 Rev 2.
- A cross-correlation table was developed to demonstrate how the topical elements within RG 1.152 Rev 2 map to the provisions in draft NEI 04-04 Rev 2.
- ISG issued December 31, 2007.

ACRS Presentation - April 11, 2008

Slide 10 of 29

- ISG clarifies the NRC staff's guidance with regard to implementation of cyber security requirements for nuclear power plant safety systems.
- The ISG includes a table correlating NEI guidance with the RG to facilitate licensing process.
- Either the RG or the NEI document in conjunction with table may be used.

- ISG rollover to cyber security DG 5022
- Remaining long term actions to be conducted through established agency process.
 - Issuance of new rule 10 CFR 73.54 (proposed rule 73.55(m))
 - Regulatory Guide to support proposed rule (DG 5022)
 - Revisions to Chapter 13 of Standard Review Plan (SRP)



DIGITAL INSTRUMENTATION AND CONTROL Review of Licensing Process Draft Interim Staff Guidance

Paul Loeser, Division of Engineering,
Office of Nuclear Reactor Regulation

ACRS Presentation - April 11, 2008

Slide 13 of 29



LICENSING PROCESS LICENSING & DOCUMENTATION

- SRP Chapter 7 provides guidance to the NRC staff.
- Digital I&C systems are unique:
 - Dependent on testing to verify that design outputs meet system requirements
 - Also dependent on a well defined design lifecycle and a high quality design process.
 - It is not practical for the staff to perform Independent V&V or an independent design review
 - These processes take too long, and require more personnel than are available.
- The staff reviews "the process" used to design, code, test, and implement digital safety systems and assesses:
 - What will be done? (Plans)
 - How will it be done? (Procedures)
 - Was this done correctly? (Vendor Audit)
 - What is the result of this effort? (Design Outputs)

ACRS Presentation - April 11, 2008

Slide 14 of 29



LICENSING PROCESS PROBLEM STATEMENTS

- The review of the design process results in a considerable amount of documentation that must be reviewed by the staff. All this documentation should be produced IAW industry standards & the Reg Guides that endorse the standards. These documents are all part of a high quality design process, and are not specifically created for the staff review.
- Industry desires these documents not to be formally submitted on the docket. Industry is concerned that once docketed, any future change would require re-review. NRC has stated any future change would be processed via 10 CFR 50.59, and only re-reviewed if required by 50.59
- TWG #6 Problem Statements contain 4 issues:
 - Problem 1 Level of Detail: Adequate guidance on the level of detail in licensing actions for operating reactors necessary to begin and complete the regulatory reviews.
 - Problem 2 Applicability: Clear guidance for operating reactors regarding the applicability of Chapter 7 of the Standard Review Plan (NUREG-0800) to digital instrumentation and control upgrades.
 - Problem 3 Clear Process Protocols: Clear licensing process protocols for developing the application and NRC review of digital technology licensing actions.
 - Problem 4 Clear Guidance: Clear guidance on licensing criteria for cyber security in DI&C safety systems needs to be developed.

ACRS Presentation - April 11, 2008

Slide 15 of 29



LICENSING PROCESS INDUSTRY REQUEST

- In order to address these problem statements, industry and vendors have requested specific clarification as to:
 - What documentation needs to be delivered to the staff for review.
 - At which phase in the review this documentation is needed.
 - Which documentation needs to be on the docket.
 - Which documentation does not need to be docketed, but needs to be available for staff review during the audit.

ACRS Presentation - April 11, 2008

Slide 16 of 29



LICENSING PROCESS SCOPE OF ISG

- The staff has considered input from the industry and is drafting an ISG that clarifies what documentation is required and when, as well as guidance on the scope & content of what should be in the LAR to address the regulatory requirements.
- This Interim Staff Guidance is applicable to all digital I & C amendment requests.
 - The ISG builds on lessons learned during review of previously approved digital platforms.
- ISG will encompass the most complex amendment request (Combined RPS and ESFAS upgrade).
- Not all documents identified in this ISG may be applicable to upgrades to digital system which are less complex or perform a single function.

ACRS Presentation - April 11, 2008

Slide 17 of 29



LICENSING PROCESS BASIS APPROACH

- These guidelines will not modify or supersede existing regulatory requirements or guidance with one exception: the current approach excludes staff review of lifecycle process that are not licensing issues, but are operations/maintenance issues.
- The staff assumes that modification planning has been completed by the time that a LAR is submitted.
 - All planning documentation will be available at the time of the submittal.
- Some of the results of the life cycle tasks, such as final design, procedures, results of testing, and final configuration may not yet be completed at the time of submittal, and therefore can be submitted later. These documents are needed prior to the SER completion.
- ISG will specifically address the information needed for acceptance review. The staff needs to see a clear path to the acceptance and review of the license amendment request.
 - Sufficient information needs to be submitted with the LAR to show that the licensee is using a high quality design process.

ACRS Presentation - April 11, 2008

Slide 18 of 29



LICENSING PROCESS DOCUMENTATION REQUIREMENTS

- TWG #6 determined the documentation required for review by consolidating the documentation required by the SRP
- Table 1 lists documents that must be reviewed. Column one identifies the most applicable SRP sections, Column two lists the requirements, standards, regulatory guides for this document, Column three describe how these requirements are met or referenced in the body of the LAR submittal, and Column 4 through 7 show at which stage of the review the documents are expected to be submitted.
- The staff does not re-review documentation which has already been approved.
 - If a Topical Report review or pervious LAR review has already approved some portion of a vendor or licensee methodology, there is no need to approve it again.
- The second set of tables are examples of sets of documents associated with different review complexities.

ACRS Presentation - April 11, 2008

Slide 19 of 29



DIGITAL INSTRUMENTATION AND CONTROL Review of New Reactor DI&C PRAs Draft Interim Staff Guidance

Glenn B. Kelly, Division of Safety Systems & Risk Assessment,
Office of New Reactors

ACRS Presentation - April 11, 2008

Slide 20 of 29

- **Problem Statement 1:**
Existing guidance does not provide sufficient clarity on how to use current methods to properly evaluate DI&C systems in PRAs for DC or COL under Part 52. The issue includes addressing CCF modeling and uncertainty analysis associated with DI&C systems.
- **Short-term Action:** Develop interim guidance for review of new reactor DI&C PRAs.
- **Other Problem Statements will Address Risk Informed Decision Making**

- Outlines various attributes and risk insights to help a reviewer identify, at a high level, any potential risk-significant problems in a DI&C implementation
- Provides guidelines for DI&C PRA review for situations where either limited or detailed review is required
- Appendix A provides risk insights obtained from previous reviews of ABWR and AP-1000 DI&C risk assessments

- Revised review guidance on uncertainty analysis by removing specific guidance on types of sensitivity studies.
- Moved up review guidance for identification of DI&C failure modes and their effects. Provided additional clarification.
- Simplified review guidance for CCF analysis of DI&C systems

- The staff is currently rewriting the ISG.
- The staff plans to issue the final ISG in the near future.

DIGITAL INSTRUMENTATION AND CONTROL Review of Operational Experience and Classification of Digital Systems

**Michael E. Waterman, Division of Engineering,
Office of Nuclear Regulatory Research**

OpE BACKGROUND

- Evaluate OpE to obtain insights regarding potential failure modes
- Develop an inventory and classification of DI&C in nuclear power plants
- Use assessments in development of D3 strategies

- Concerns with Software CCF are Valid
- Failures reported at high level
 - “Software failed”, “System reset”
 - Scarce details on cause of failures
 - Design or function errors
 - Development errors
 - Operator errors
- Root cause analysis methods must be refined

- Classification
 - Complexity
 - Inter-connectivity
 - Digital system importance
- Inventory
 - System reviews required to implement

- Obtain more detailed information from OpE reviews
- Develop an inventory of existing and new digital systems
 - Structure to align with the system classification method
- Identify D3 strategies consistent with OpE and system classification

Digital Instrument & Controls Industry View

April 11, 2008

Gordon Clefton
Senior Project Manager



Topics

- Objective
- Goals
- Conclusions



Objective

- **Safety-focused application of digital technology**
 - Current operating plants
 - Design certification
 - New plants
 - New fuel facilities
- **Stable, predictable, and timely licensing process with realistic guidance**
- **Enhance plant safety, availability, and reliability**

The logo for the Nuclear Energy Institute (NEI), featuring the letters "NEI" in a bold, sans-serif font with a stylized graphic element to the left.

3

Goals

- **Short term - Interim Staff Guidance (ISG)**
 - Technically sound
 - Practical to apply
 - Appropriate detail of regulatory evaluations/reviews
- **Long term - Final staff guidance**
 - Incorporate ISG content into final regulatory guidance
 - Assure consistency with applicable industry codes and standards
 - Endorse related, detailed industry guidance

The logo for the Nuclear Energy Institute (NEI), featuring the letters "NEI" in a bold, sans-serif font with a stylized graphic element to the left.

4

Conclusions

Project Plan

- Continue management oversight / coordination

Pilot Project

- Validate Licensing Process ISGs
 - Highest importance and significance
- Demonstrate effective and timely regulatory process for licensing digital upgrades

Guidance

- Continue to refine and enhance regulatory guidance, as necessary
- Develop a stable, predictable, and timely licensing process with realistic guidance

NEI

5

Acronyms

▪ ATWS	Anticipated Transient Without Scram
▪ BTP	Branch Technical Position
▪ D-3	Diversity & Defense-in-Depth
▪ DAS	Diverse Actuation System
▪ DI&C	Digital Instrumentation and Control
▪ ESPS	Engineered Safeguards Protective System
▪ ISG	Interim Staff Guidance
▪ ITAAC	Inspections, Test, Analyses, and Acceptance Criteria
▪ LAR	License Amendment Request
▪ NEI	Nuclear Energy Institute
▪ RPS	Reactor Protective System
▪ TWG	Task Working Group

NEI

6



EPRI | ELECTRIC POWER
RESEARCH INSTITUTE

Industry Review of Operational Experience

Advisory Committee on Reactor Safeguards
April 11, 2008

Ray Torok
EPRI

Bruce Geddes
Southern Engineering Services

Contents

- Project description
- What does the operating experience tell us?
- Event evaluations
- Results

Industry OE Review – Project Description

Project genesis - May 18, 2007 ACRS recommendation:

- Use operating experience insights to refine guidance on defense-in-depth and diversity for digital I&C

Basic Approach - Study NRC and INPO operating experience reports

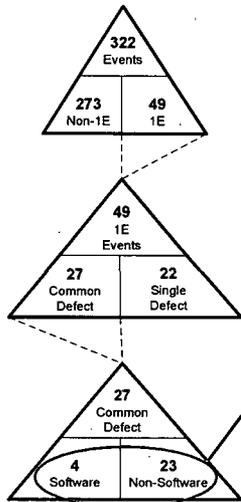
- Found 322 “digital events” from 1987 to 2007 (1E & Non-1E)
- Look for actual and potential common-cause failures (CCFs)
- Capture insights on effective corrective measures

Related EPRI Project – Develop case studies, lessons learned and training materials based on selected OE reports

What is the OE Telling Us?

- There were no actual CCF events that disabled a safety function
- Actual and potential CCF events were dominated by non-software issues, e.g.,
 - Lifecycle management and human performance errors (e.g., incorrect setpoints)
 - Hardware failures (non-1E)
- OE suggests that current methods are effective in keeping software a minor contributor to CCF
 - Use of software codes and standards
 - Design and process characteristics that preclude or limit CCFs (“defensive measures” and diversity attributes)

1E Common Defects



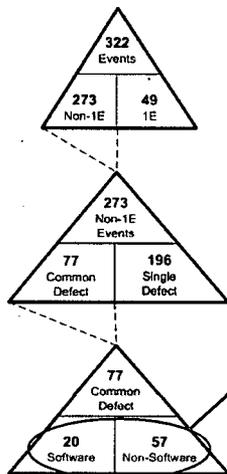
System-Level Effects:

- ❖ 0 (Zero) Actual CCFs
- ❖ 6 Potential CCFs
 - 1 Software Related
 - 5 Non-Software Related

Remaining Common Defects:

- ❖ 10 Single Failures
- ❖ 6 Spurious Actuations
- ❖ 4 Subsystem Level Potential CCFs
- ❖ 1 Subsystem Level Actual CCF

Non-1E Common Defects



System Level Effects:

- ❖ 33 Actual CCFs
 - 7 Software Related
 - 26 Non-Software Related
- ❖ 5 Potential CCFs
 - 0 Software Related
 - 5 Non-Software Related

Remaining Common Defects:

- ❖ 10 Single Failures
- ❖ 12 Spurious Actuations
- ❖ 6 Subsystem Level Potential CCFs
- ❖ 11 Subsystem Level Actual CCFs

1E vs. Non-1E Vulnerability to CCF

Attribute	1E Systems	Non-1E Systems
Redundancy	Independent Channels	Master/Slave
Shared Resources	Never	Almost Always
Formal SQA* Methods	Always	Varies (Improving)
Functional Complexity	Low	High
System Interactions	Low	High

1E systems are inherently better protected against CCF
Both 1E & Non-1E reports reveal valuable insights
Direct comparison of 1E & Non-1E events is difficult

*Software Quality Assurance

© 2008 Electric Power Research Institute, Inc. All rights reserved.

7

EPRI | ELECTRIC POWER
RESEARCH INSTITUTE

Results

Conclusions

- **Software has been no more problematic than other CCF contributors**
 - Current methods have been effective in keeping software a minor contributor to potential 1E CCFs
- **Difficult to combine 1E and non-1E experience**

Recommendations

- **Encourage additional OE investigations**
 - Other countries and industries (confirm U.S. results)
 - Analyze for risk significance and other insights
- **Refine D3 guidance**
 - Endorse and credit methods that have proven effective in protecting against software CCFs

© 2008 Electric Power Research Institute, Inc. All rights reserved.

8

EPRI | ELECTRIC POWER
RESEARCH INSTITUTE

Additional Insights

- Software changes were commonly used as corrective actions for non-software problems
- Saw events that confirmed effectiveness of signal and functional diversity in protecting against CCF
- Saw no events that indicated platform diversity would be effective in improving CCF protection
- Saw several cases where design changes were made to preclude or mitigate certain failure modes (added defensive measures)

Key Terms - Industry Review of Operational Experience

- **Defect** – A deficiency in characteristic, documentation or procedure. In software often referred to as "fault" or "bug."
- **Common defect** –
 - Safety Systems - A defect that affects multiple redundancies, for example a software fault that exists in all divisions of a redundant safety system.
 - Non-safety systems – Also includes defects in shared resources, for example a power supply that feeds multiple non-safety process controllers.
- **Software event** – An event involving design defects introduced in the software development process (not, for example, incorrect setpoints or flawed requirements)
- **Failure** – Degraded or terminated ability of a functional unit to perform a required function. A software failure results when a software defect is activated by certain triggering conditions.
- **Potential CCF** – A defect common to multiple redundancies that can result in an actual CCF in the presence of concurrent triggers.
- **Actual CCF** – A malfunction on demand that results in an incorrect response or loss of function across multiple redundancies at the same time.
- **Digital event** – Any plant occurrence that involved or affected a digital system and was reported in the databases that were searched.
- **Trigger** – A plant condition or specific set of inputs that activate a defect; in digital systems this is typically an unanticipated, unexpected, or untested condition.

Acronyms

• 1E	Safety system
• BTP	Branch Technical Position
• CCF	Common Cause Failure
• D-3	Diversity & Defense-in-Depth
• DAS	Diverse Actuation System
• DI&C	Digital Instrumentation and Control
• EPRI	Electric Power Research Institute
• INPO	Institute of Nuclear Power Operations
• ISG	Interim Staff Guidance
• LAR	License Amendment Request
• NEI	Nuclear Energy Institute
• Non-1E	Non-safety system
• OE	Operating Experience
• SQA	Software Quality Assurance
• TWG	Task Working Group

Non-1E Software Failure Modes

