

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

Title: ACRS Digital I&CS Subcommittee

Docket Number: n/a

Location: Rockville, MD

Date: 6/22/11

Work Order No.: NRC-965

Pages 1-349

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

DISCLAIMER

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

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

WEDNESDAY

JUNE 22, 2011

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

NEAL R. GROSS

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

1 SUBCOMMITTEE MEMBERS PRESENT:

2 CHARLES H. BROWN, Chairman

3 DENNIS C. BLEY

4 MICHAEL CORRADINI

5 JOY REMPE

6 MICHAEL T. RYAN

7 JOHN D. SIEBER

8 JOHN W. STETKAR

9

10 NRC STAFF PRESENT:

11 CHRISTINA ANTONESCU, Designated Federal

12 Official

13 RUSSELL SYDNOR

14 PAUL REBSTOCK

15 LUIS BETANCOURT

16 SUSHIL BIRLA

17 ALAN KURITZKY

18 KARL STURZEBECKER

19 DEREK HALVORSON

20 DAN SANTOS

21 STUART RICHARDS

22 MILTON CONCEPCION

23

I-N-D-E-X

I	
Opening Remarks -- C. Brown, ACRS.	4
II	
Overview and Research Accomplishments of FY2010 to FY2014 Digital Research Plan -- R. Sydnor, RES/DE	6
III	
NUREG-I/A-0254- Suitability of Fault Modes and Effects Analysis for Regulatory Assurance of Complex Logic in DI&C Systems -- L. Betancourt, RES/DE -- S. Birla, RES/DE59
Break	
III Continued.	113
IV	
Expert Clinic and Research Information Letter (RIL) 1001: Software-Related Uncertainties in the Assurance of Digital Safety Systems -- S. Birla, RES/DE	136
Lunch	
IV	
Expert Clinic and Research Information Letter (RIL) 1001: Software-Related Uncertainties in the Assurance of Digital Safety Systems (Continued) -- S. Birla, RES/DE	167
Break	
V Learning from Digital Operating Experience K. Sturzebecher, RES/DE	224
VI	
Research Whitepaper on Redundancy and Independence among Safety Channels - P. Rebstock, RES/DE.	280
VII	
Digital I&C Knowledge Management and Standards Harmonization -- M. Concepcion, RES/DE	332
Adjournment	359

NEAL R. GROSS

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

P R O C E E D I N G S

8:32 a.m.

1
2
3 CHAIR BROWN: The meeting will now come
4 to order. This is a meeting of the Digital
5 Instrumentation and Control Systems Subcommittee. I
6 am Charles Brown, Chairman of the Subcommittee.

7 ACRS members in attendance are Jack
8 Sieber, John Stetkar, Dennis Bley, Joy Rempe;
9 Christina Antonescu of the ACRS staff is the
10 Designated Federal Official for this meeting.

11 The primary purpose of this meeting is
12 to discuss accomplishments of the 2010-2014 Digital
13 Research Plan which are of interest to the ACRS,
14 with emphasis on answering the following questions:
15 what are the research accomplishments on the DI&C
16 plan since the last subcommittee meeting; two, how
17 are you intending to use the research findings that
18 you have done or got; the user offices for NRR, NRO,
19 NSIR, et cetera; and three, what are your future
20 plans?

21 Also, the staff will discuss NUREG --
22 what is the number?

23 MS. ANTONESCU: There is no number --
24 it's, um --

25 CHAIR BROWN: Okay, IA-xxxx: Identifying

NEAL R. GROSS

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

1 and Analyzing Fault Modes Attributable to Complex
2 Logic and Digital I&C systems; RIL-1001, Software-
3 Related Uncertainties and the Assurance of Digital
4 Safety Systems; expert clinic findings; research
5 White Paper on redundancy and independence among
6 safety channels and other DI&C research activities.

7 The Subcommittee will gather
8 information, analyze relevant issues and facts, and
9 formulate proposed positions and actions as
10 appropriate for deliberation by the full committee.

11 The rules for participation in today's
12 meeting have been announced as part of the notice of
13 this meeting previously published in the Federal
14 Register on June 13th, 2011.

15 We have received no written comments or
16 requests for time to make oral statements from
17 members of the public regarding today's meeting.
18 Also, we have no requests for a bridge phone line
19 listening to the discussions.

20 A transcript of the meeting is being
21 kept and will be made available as stated in the
22 Federal Register notice. Therefore we request that
23 participants in this meeting use the microphones
24 located throughout the meeting room when addressing
25 the Subcommittee.

NEAL R. GROSS

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

1 The participants should first identify
2 themselves and speak with sufficient clarity and
3 volume so that they may be readily heard. We will
4 now proceed with the meeting.

5 I call upon Mr. Russell Sydnor, DI&C
6 Branch Chief in the Division of Engineering, Office
7 of Nuclear Regulatory Research, to provide an
8 overview on research accomplishments of the FY 2010-
9 14 Digital Research Plan.

10 MR. SYDNOR: Thank you, Charlie.

11 CHAIR BROWN: Proceed.

12 MR. SYDNOR: Good morning. I am Russell
13 Sydnor. I work in the Office of Research, Digital
14 I&C Branch. With this morning to support and
15 participate in the presentations, my supervisor Stu
16 Richards, who is the deputy division director of the
17 Division of Engineering in the Office of Research
18 and our other presenters, Mr. Luis Betancourt, Mr.
19 Karl Sturzebecher, Mr. Milton Concepcion, Mr. Paul
20 Rebstock and Dr. Sushil Birla who is the senior
21 technical adviser for the Division of Engineering
22 for digital I&C in the Office of Research.

23 Our purpose today and objectives: our
24 primary purpose in scheduling this meeting was to
25 talk about some specific research topics that are of

NEAL R. GROSS

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

1 interest to the ACRS because their origin and some
2 of the work relate back to previous ACRS meetings
3 and SRMs, especially focusing in the area of digital
4 failures -- digital failure mode investigations.

5 So that was our original purpose in
6 scheduling the meeting. Coincidentally, timing is --
7 falls under the time frame when ACRS is trying to
8 formulate their biennial review of research overall
9 and so we were requested to try to support that.

10 And so hopefully we can answer the
11 questions you need to have answered to draw
12 conclusions about that. So input to the biennial
13 review was an auxiliary purpose today.

14 And that will primarily be covered in my
15 overview. The specific presentations today are going
16 to cover more specific topics. Now, in this topics
17 you will also get the flavor of what we are doing
18 and why we are doing it and where we are going.

19 CHAIR BROWN: Now those topics are part
20 of your all's overall research plans and --

21 MR. SYDNOR: Yes, and I'll --

22 CHAIR BROWN: I make that point, they
23 are pieces of the pie.

24 MR. SYDNOR: Yes, and I will try to
25 focus that for you of where they're at, where they

NEAL R. GROSS

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

1 fit into the plan.

2 CHAIR BROWN: Okay. Thank you.

3 MR. SYDNOR: Again, part of the reason
4 for scheduling it, the second bullet is what we hope
5 to gain from the meeting today and we really want to
6 discuss some of these issues because they are far
7 from resolved, research is still in progress, we are
8 looking for your input and feedback on not only the
9 technical issues but if you have suggestions on
10 areas that -- gaps or areas that we need to refocus
11 or reapply our thinking, that's what we are for, to
12 obtain that feedback.

13 And finally we are not requesting any
14 specific letter because this is more or less an
15 interim report at this point in time.

16 So just an overview of the current
17 research plan, which we are supporting. This was a
18 major update to the previous plan. The ACRS reviewed
19 the new plan in late 2009 and issued a letter in
20 October of 2009.

21 Subsequent to that we obtained program
22 offices, as you were stating, NRR, NRO, NSIR,
23 concurred in the plan by February 2010 and then we
24 issued the current plan.

25 And I believe we actually have some

1 handouts in the back room if anyone would like a
2 copy of the current plan.

3 So the current plan is made up of five
4 major topic areas. The biggest one with the most
5 research activity is safety aspects of digital
6 systems, which has a number of different topics
7 including the failure mode investigation, a number
8 of which we will be talking about today.

9 Another major area is security, which is
10 pretty self-descriptive. That is a topic where we
11 looked at cybr security and some other security --
12 plant security related issues, which -- and I will
13 actually give an overview of that since we don't ha
14 specific topics on the agenda for that area today.

15 Likewise for advanced nuclear power
16 concepts, I will cover that briefly. A lot of it you
17 have already heard via presentations from NNGP and
18 HTGR so I am just going to kind of relate how that
19 fits and where we are at in our specific research.

20 And kind of a new area we added, it's --
21 to this plan, but an important area, is knowledge
22 management, where we are doing a lot of activities
23 with updating regulatory guidance, international
24 collaboration, standards harmonization, things like
25 that, and our last topic on the agenda today will

NEAL R. GROSS

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

1 talk to some of those.

2 Also in that area is important work we
3 are doing in operational assessment, and we do have
4 a specific presentation on that, and I think you
5 will be surprised at how broad we are looking that
6 area, and some success we have had in getting
7 information from a wide range of sources.

8 And then, the final area which I will
9 just cover very briefly just for completeness, is we
10 did have a few projects that we added to this plan
11 that were specifically reviewed.

12 They projects never started in the
13 previous plan, but were -- when the program offices
14 looked at them they said we are not ready to drop
15 those yet, but make them low priority but keep them
16 in this plan.

17 We have -- currently, and I believe
18 actually the Office of Research provided a matrix of
19 projects to the ACRS as part of their biennial
20 review effort -- but in my branch in that matrix,
21 there are at least 27 individual recert projects.

22 There's actually more than that in there
23 but some of them are just budget placeholders for
24 things like our budgeting of the Halden research
25 project.

NEAL R. GROSS

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

1 But there are 27 individual research
2 projects that we currently have, that we are either
3 working, completing or planning to start in that
4 listing.

5 And of those 27, actually seven of them
6 are still where we are still resolving work that was
7 started on the 05-09 plan.

8 One thing I thought it was, to give you
9 the proper context of where we are at, is talk a
10 little bit about the transition we have been going
11 through from the previous plan to the current plan.

12 Last year and this year are really a
13 transition period, and an example of that is what I
14 just previously mentioned on the previous slide, the
15 projects from the previous plan that are still
16 wrapping up or completing, or that we thought were
17 important enough to actually incorporate in the new
18 plan.

19 And so I wanted to just talk about that
20 transition a little bit. The old plan -- because
21 rather than five topic areas, consisted of seven
22 research programs. They actually mapped pretty well
23 through the current five we are doing. There was
24 some combination.

25 In 21 of those 29 research projects that

1 came out of those seven research programs,
2 significant research projects -- either we have
3 completed the work, published reg guides, published
4 NUREGs or still are in the process of finalizing
5 work from that plan.

6 The work that was in progress, we
7 continue to completion. Research that wasn't
8 initiated, we had reviewed that with the program
9 offices, part of the update of eight areas there, 21
10 -- 29 minus 21 of the eight areas that were not
11 dealt with in the previous plan, or actually
12 probably more a matter of resources, they just --
13 they were lower priority and never started.

14 Five of those the other offices deemed
15 as not requiring further effort, either because the
16 user -- the usefulness of those projects did not
17 bear fruit, or just other priorities had overtaken
18 them. But three of the topics did actually --- we
19 did roll into the new plan.

20 The old plan -- slightly different from
21 the new plan in that it was more specific. It was
22 really geared toward specific regulatory guidance
23 improvements, development of new methods like the
24 PRA work, software assurance, software quality
25 assurance, testing methods for software assurance,

NEAL R. GROSS

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

1 things like that, and I will talk about some
2 specific examples of those.

3 And it also, to a great extent, had a
4 number of topics looking at regulatory implications
5 of new technology, which is part of our role I think
6 especially in my area, in the digital I&C area.

7 The other thing I wanted to mention
8 because it impacted how that plan was finishing up
9 in the 07-09 time frame, was that at least three
10 areas in the plan supported a digital I&C project
11 and ISG development.

12 Examples are diversity and defense in
13 depth, communications -- ISG-4 communications, we
14 were doing work in those areas -- and of course the
15 PRA work.

16 So all three of those we had ongoing
17 research, but the research was also somewhat
18 tailored to support those ISG developments. So in
19 that case, we kind of made a quick leap from ongoing
20 research discussions to actual guidance via the
21 ISGs, which the committee reviewed all of those, so
22 we don't need to rehash any of that today. But it's
23 important -- I wanted to make you aware of that.

24 I have provided a handout, a three-page
25 handout that lists all of our research products. I

NEAL R. GROSS

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

1 won't say all, ninety-some percent of them, because
2 there's some smaller ones that I didn't bother
3 putting in there, from the last three to four years.

4 And I just -- on this slide I just
5 highlighted some of the, to kind of give you a
6 flavor, that a lot of those are completing --
7 because of the time frame -- they are completing
8 work that was in the previous plan, but they are
9 also -- there's some new products from the new plan
10 and some products that are still in progress, which
11 I will -- my later slides will give you some more
12 detail on that.

13 These are -- this is some specific
14 examples of work and in some cases, the Committee
15 has actually looked at -- looked at some of these,
16 the diversity and defense in depth study, which
17 served as -- you know, a couple of purposes, as a
18 technical basis for ISG-3 but there is also a
19 potential there incorporating that in a future
20 update of BTP 7-19.

21 We have discussed putting that
22 methodology in our guidance. I am aware that some
23 licensees have used it as a model, or used it as
24 part of their discussions with NRO or NRR as part of
25 their license applications for digital upgrades or

NEAL R. GROSS

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

1 new reactors.

2 CHAIR BROWN: Was that the one that had
3 -- you are talking about 7007, right?

4 MR. SYDNOR: Right, the first one there.

5 CHAIR BROWN: Was that the one that had
6 the mathematical construct that you could end up
7 getting a weighting, or a --

8 MR. SYDNOR: Yes.

9 CHAIR BROWN: ranking. Okay I remember
10 that presentation.

11 MR. SYDNOR: But that work also has a
12 lot of good discussion about diversity principles
13 and how you apply them that I think is -- it's for
14 anybody who is trying to determine if they have
15 adequate diversity it's a good source of
16 information. It gives you more detail of the actual
17 principles.

18 The use of the tool, the licensing
19 offices, we have not had a chance to vet that tool
20 so the current update of BTP 7-19 does not include
21 using that tool but we are still discussing
22 potential future uses of it.

23 But the work is -- the NUREG is a
24 perfectly good source of information and like I say,
25 I am aware that we have done some trial uses of ut

NEAL R. GROSS

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

1 in licensing applications.

2 The second one is -- we recently issued
3 is a study of the best practices for the design and
4 use of field-programmable gate arrays in digital
5 safety systems and we have been asked to -- it
6 provides an excellent technical basis along with
7 some other work that is going on in the outside,
8 both by EPRI and internationally with an IEC
9 standard that's under development.

10 And we are looking at developing a
11 future reg guide that supports that type of
12 technology, provides more guidance to the staff on
13 reviewing that type of technology.

14 CHAIR BROWN: Was that review with the
15 Committee?

16 MR. SYDNOR: The Committee has not
17 looked at that. It's a pretty straightforward
18 compilation of best practice, design practices for
19 FPGA work, and like I say there's a number of --
20 EPRI has done a couple of reports too that are more
21 geared toward the utility side of it than the
22 regulatory side.

23 Ours had a more regulatory perspective,
24 and then internationally, there's an IEC standard
25 under development that we are using, you know, our

NEAL R. GROSS

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

1 knowledge that we have gained here to influence that
2 standard, and hopefully we may even be able to
3 endorse that standard as part of our reg guide.

4 MEMBER SIEBER: Do you think that that's
5 a distinct possibility, that you will endorse that?

6 MR. SYDNOR: I think it's a possibility.
7 I am not ready to use the word distinct yet. We are
8 trying to influence it. We have provided input to
9 the draft, and we are collaborating with the lead
10 for the IEC standards, Jean Gassino from IRSN.

11 MEMBER SIEBER: Okay, it seems to me
12 that the international community has done quite a
13 bit of work and has some novel ideas and will have
14 an influence on what we do, particularly with future
15 reactors, what we do here.

16 MR. SYDNOR: Yes, in Milton's
17 presentation, which hopefully we will get to at the
18 end of the day, it talks about a lot of our
19 collaborations.

20 MEMBER SIEBER: Okay, yes, I will look
21 forward to that. Thank you.

22 MR. SYDNOR: The next one, large-scale
23 validation of a methodology for assessing software
24 quality is a new work. The publication -- it's in
25 the Office of Publications right now, so it's been

NEAL R. GROSS

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

1 reviewed and concurred by the program offices.

2 This was out of the old plan in the
3 software assurance area. It was an exploration of
4 the potential to use software metrics as a part of
5 software assurance, and it's got -- I think it's a
6 useful study because it really has a good discussion
7 about the pluses and minuses of the various methods
8 and how well they could support the regulatory
9 process.

10 More work would have to be done from
11 that to determine if we would ever -- ever use it,
12 but I think it's a useful product should a vendor or
13 an an applicant try to use software metrics, because
14 it discusses about 12 different methods and actually
15 they were actually used on a demonstration system.

16 MEMBER SIEBER: You could have a whole
17 range of quality and accuracy within a given rating
18 range of a lot of the systems, it seems to me,
19 because they don't actually address all the intimate
20 details of the coding.

21 MR. SYDNOR: One thing I'll mention, as
22 we discuss, or as you review the handout at your own
23 leisure later, if there's topics that you might have
24 a future interest in hearing about, a presentation,
25 certainly just Christina will collect those and she

NEAL R. GROSS

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

1 will discuss that with me, because I am sure we will
2 be back.

3 And a final product that really
4 overlapped the old plan and the new plan -- you are
5 more than familiar with the new Reg Guide 5.71; we
6 were integrally involved with developing that cyber
7 security guidance in support of 10 CFR 73.54.

8 From the new plan there's a couple of
9 new products and I'm not going to discuss those in
10 any detail because we have detailed presentations on
11 them there, but I just listed them there for your
12 benefit, and I will just refer you to the handout
13 because the handout has a lot of detail, additional
14 letter reports, reg guides that we have produced in
15 the last several years.

16 CHAIR BROWN: Could you go back for just
17 a second -- just -- you are talking about this
18 handout where we have -- the 27 you sent out to us,
19 it's for all the items --

20 MR. SYDNOR: I provided an additional
21 handout --

22 CHAIR BROWN: This is just the matrix --

23 MR. SYDNOR: The matrix is the --

24 CHAIR BROWN: (Inaudible, two speakers)
25 reflected in there.

NEAL R. GROSS

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

1 MR. SYDNOR: the 27 projects that --

2 CHAIR BROWN: Yes, okay.

3 MR. SYDNOR: I'm not going to --because
4 we want to get onto one of the other parts for one
5 of the other members we may come back to this and
6 revisit some of the stuff in it later, and we may
7 answer some of your questions as we go along.

8 CHAIR BROWN: That works also.

9 MR. SYDNOR: I hope. So again, here's a
10 research program. The highlighted areas that we are
11 going to talk about -- the topics today come out of
12 those topic areas and they are probably -- two of
13 the larger areas that we are working on are
14 generating most of our new work and so I am -- the
15 things that are going to be talked about in the
16 other presentations I'm not going to cover as part
17 of my overview.

18 There are some research projects in the
19 safety aspects that I will cover briefly because
20 they are not covered in the following presentations,
21 but I wanted to give just a real brief overview of
22 the other areas, mainly for -- to support your
23 biennial review effort.

24 So in the safety aspects of digital
25 systems, some of the other work that's under way

NEAL R. GROSS

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

1 that won't be discussed, a lot of it you have
2 already heard -- the digital system PRA work we have
3 dedicated a whole meeting to, just a few weeks ago,
4 so I know you are -- Mr. Brown was not able to be at
5 that but the other members were, and heard that
6 presentation by Mr. Alan Kuritzky, who is here today

7 And so that's already been well
8 discussed so I'm not going to cover it, but that is
9 a major topic of ours that we are collaborating with
10 the other division on.

11 Another research project in that area --
12 - that topic area is fault injection test
13 methodology development, which we have been working
14 with the University of Virginia for a number of
15 years to develop a methodology.

16 The original thinking was that we might
17 be able to use this methodology as part of our
18 assurance program. Whether we could do that or not
19 still needs to be determined.

20 What we did in that, we actually
21 physically tested two different platforms: the AREVA
22 Teleperm platform; and the Invensys Tricon platform,
23 and University of Virginia ran their fault testing
24 methodology on those platforms and the documentation
25 of all that work is -- they are drafting a NUREG/CR

NEAL R. GROSS

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

1 for publication, and that may be one that you'd have
2 some future interest in having a discussion on.

3 How we actually may use that in our
4 regulatory process is probably a future decision
5 after we -- after the program offices have more time
6 to take a look at that.

7 MEMBER BLEY: Can you say anything
8 briefly about the results? Were there things that
9 were uncovered that way that were hard to discover
10 in other review modes?

11 MR. SYDNOR: Well I don't know how
12 familiar people are with the methodology but
13 essentially they use an emulator to emulate binary
14 faults right into the processor and see how the
15 system responds to those.

16 Now they don't use a random method to do
17 that. They have a methodology where they select a
18 fault injection profile and that would be the
19 interesting part I think of their work, is they have
20 developed that methodology by looking at these two
21 systems, and I'm not smart enough to describe them
22 in two sentences.

23 But it's an organized methodology where
24 they look at the design of the system and look at
25 the purpose of the system and tailor their fault

NEAL R. GROSS

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

1 injection campaign based on that.

2 And we actually had mock-ups. They
3 weren't full-scale systems, but they simulated a
4 multi-channel system operation and then we used
5 outputs out of a TRACE model to run into the Digital
6 Protection System that was set up to simulate a real
7 basic Reactor Protection System, and then inject
8 faults as it was at its most crucial standpoint of,
9 you know, generating a trip, or needing to generate
10 a trip, and then they looked at the results of that.

11 So it's quite an extensive campaign.
12 Generally, the systems performed pretty well. It's
13 not like they didn't have issues. We did make a
14 point of inviting both the vendors to detailed
15 presentations of what we found.

16 So we shared that testing information
17 with the vendors for their benefit, because it was a
18 collaborative research agreement with them. In one
19 case one of the vendors actually loaned us the
20 equipment free of charge, so that was pretty
21 generous of them.

22 And they were very interested in the
23 methodology because they thought they had done some
24 fault-tolerance testing themselves, but they had
25 used a different technique than this.

NEAL R. GROSS

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

1 CHAIR BROWN: Did -- let me ask a
2 question on that, because that was one of the
3 interesting items in the -- obviously one of the
4 items of interest as to how do you test that stuff
5 for failures and faults.

6 And when you talked about -- that's
7 platform testing, but when you talk about the
8 emulators, was it single data output emulators for
9 the -- I mean, most of the platforms you get, you've
10 got multiple sets of data coming in.

11 You have got a number of reports, you've
12 got multiple sets of data representing a plant
13 configuration. So one of the issues, I know that,
14 you know, test program I participated in, we worried
15 about, was interactions of combinations of sets of
16 data from multiple sources and how they could
17 possibly muck up the processing and have stuff not
18 come out the way you'd like it to be.

19 And that's complicated because you
20 almost have to have a plant model of the plant you
21 are going to apply the system to, and then run it in
22 terms of a real-time model.

23 Detectors are out of it. I mean, you are
24 just doing this as a digital simulation, and so you
25 have got all those inputs coming in at the same

NEAL R. GROSS

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

1 time, and then varying them -- and you've got, what,
2 hundreds of millions of combination of bits and
3 bytes, so you have to make some judgements.

4 I take it from your comment, that this
5 was not that extensive?

6 MR. SYDNOR: Yes, let me just try to
7 characterize that for you. These by no means were a
8 full-scale mock-up. Channel, channel-and-a-half
9 arrangement, or two-channel arrangement to try to
10 simulate, you know, some logic and ability to
11 generate an actual trip output, which were generally
12 -- for the mock-ups were just alarms, obviously.

13 And so we did -- and the inputs were
14 just really minimal, one or two parameters. You've
15 got to remember, our purpose here was to test the
16 methodology, not to actually test the systems.

17 So the information we learned on the
18 systems out of it, which was some -- of substantial
19 interest to the vendors, we couldn't claim that was
20 full-scope system testing because it was primarily
21 looking at the methodology, trying to refine the
22 methodology and actually get it to the point where
23 the University of Virginia could maybe even market
24 the methodology.

25 And I actually think they are pretty

1 close to being able to do that and this could be
2 something that vendors would want to use as part of
3 a developmental program.

4 Our ultimate use in regulatory
5 assurance, probably not as obvious yet, to me
6 anyway, because it's more of a developmental tool.
7 So it wasn't that full-scale testing, it was --

8 CHAIR BROWN: And I wasn't really -- I
9 mean, more of along a single channel, I mean a
10 single channel -- every channel gets a set of
11 pressures, temperatures, flows, levels, etcetera, in
12 various pieces of other commands, type commands that
13 may be coming in.

14 So I was thinking more of the single-
15 channel type routine but with multiple parameters
16 and then varying those parameters within some
17 construct that replicates, you know, plant-type
18 conditions that you would have. That's not as
19 complicated as a full-scale, you know trying to
20 emulate or mock-up an entire nuclear power plant
21 which is extremely complex.

22 MR. SYDNOR: We did -- the researchers
23 were not experts in -- they were more experts in
24 digital systems and not so much in plant models or -
25 - but they did utilize some of our expertise in the

NEAL R. GROSS

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

1 other -- in other divisions in the Office to look at
2 the TRACE model, which generates a plant-level
3 response and generates parameters.

4 And so they used that to generate
5 parameters that were inputs to this, but it wasn't
6 that sophisticated. It wasn't, certainly, you know,
7 12 or 15 inputs that you might in an operating
8 reactor.

9 CHAIR BROWN: Okay, thank you.

10 MR. SYDNOR: So anyway, those top two --
11 those are two of the other research projects under
12 safety aspects that we're still pursuing, and then
13 at the bottom under new research projects, there's
14 some new projects.

15 The first bullet there, we are a little
16 further along and actually formulating a Statement
17 of Work and working -- trying to figure out who can
18 support us, whether DOE or commercial and things
19 like that, where we are going to look at developing
20 regulatory guidance for safety assessment of tool-
21 automated processes which the agency has already
22 been confronted with applicants that want to credit
23 automated tools as part of their software
24 development.

25 And diagnostics and prognostics is

NEAL R. GROSS

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

1 actually -- has been around for a while but this is
2 -- there's potential for new uses of these
3 techniques in digital systems where they would
4 actually be credited as part of surveillances,
5 formal tech spec surveillances.

6 So the goal of this work is to look at
7 the implications of those type of techniques and
8 equipment on digital systems and on safety assurance
9 digital systems, and you know, how we could also --
10 what regulatory structure, guidance we might need to
11 have in place to approve those, should we actually
12 get an application.

13 I am aware that at least one of the new
14 reactors has approached NRO with some interest in
15 doing that --

16 CHAIR BROWN: Let me --

17 MR. SYDNOR: and it's only a logical
18 step --

19 CHAIR BROWN: I just wanted to try to
20 understand since I'm -- came out of a different
21 world relatively, when you talk about tech spec-type
22 stuff.

23 We used to have -- weekly you'd go
24 through into a weekly set of manual trip point
25 calibration checks and then there would be another,

NEAL R. GROSS

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

1 more extensive set of checks that you did quarterly
2 and a more extensive check that you did semi-
3 annually etcetera, etcetera, etcetera.

4 MR. SYDNOR: Actually, the commercial
5 fleet is very similar to that.

6 CHAIR BROWN: Okay, well that -- I
7 figured, since we -- they kind of grew out of what
8 we did initially, probably the case. But I mean it
9 seems like a logical extrapolation, if you end up
10 with diagnostics it's going to run through that
11 entire sequence and take the man out of it and you
12 get it done more frequently, it seems to be a
13 logical path to me, I mean, but I gather that really
14 hasn't been taken to its conclusion so far in the
15 commercial world.

16 MR. SYDNOR: But the commercial world,
17 just as there's been delays in upgrading for
18 digital, there's also been delays in using these
19 techniques. Now, they are used on, as part of
20 maintenance diagnostics and things like that, they
21 have separate systems.

22 It turns out my -- Mr. Paul Rebstock is
23 my project manager, and Paul, did you have something
24 you wanted to say in that regard?

25 MR. REBSTOCK: Yes, I am Paul Rebstock.

1 Is this mic on? I am Paul Rebstock. I am the
2 technical lead and project manager on that project.
3 There's -- the way we have got it divided up is a
4 little bit unusual. There's actually three separate
5 areas.

6 There's what you were talking about,
7 which is what I would refer to as on-line
8 monitoring, where the computer watches the plants
9 and looks for strange things that tell it that maybe
10 something is coming out of calibration; there's
11 another aspect, where the computer is watching over
12 itself, doing digital diagnostics of its own self;
13 and the third aspect is watching over things like
14 motor-operated valves and mechanical equipment and
15 looking for bearing wear and that kind of stuff.

16 The on-line monitoring is a project that
17 was already completed a few years ago, and that was
18 looking toward the possibility of extending the
19 physical calibration interval to up to eight years
20 by saying that you have to test one channel each
21 year rather than all four channels each year, each
22 refueling outage, and a two-year refueling outage
23 would give you eight years between channel tests,
24 unless the on-line monitoring program detected some
25 kind of an anomaly in which case you'd have to go in

NEAL R. GROSS

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

1 and check it more often.

2 That NUREG has already been issued and
3 published some time ago. This project that we are
4 looking at now looks at the other two: the
5 mechanical equipment monitoring; and the monitoring
6 of the digital system itself.

7 All three of those together would
8 ultimately be integrated into a plant as a
9 comprehensive testing program. But as far as the
10 project scoping is concerned, I just wanted to make
11 it clear where the scope boundaries are.

12 So what you are saying is true, but
13 that's in the other research project, okay?

14 CHAIR BROWN: okay, yes, well I was
15 referring to actually both, both the monitoring as
16 well as the on-line, periodic, calibration testing.
17 I mean you can do that with these if you have got
18 set of reference standards that are built into the
19 equipment.

20 MR. REBSTOCK: Right.

21 CHAIR BROWN: And then they, every
22 minute, whatever the interval you want, you can
23 connect those in, check to see that you get the
24 proper response from it -- any particular
25 temperature instance, whatever, and you really do

NEAL R. GROSS

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

1 reduce the time necessary for folks to go back and
2 operate switches or disconnect things and put in
3 calibration standards, if you have quality reference
4 devices.

5 MR. REBSTOCK: Right. Right. Well
6 there's a learning period involved, where the system
7 learns how the plant behaves. There are advantages,
8 I mean, it reduces -- besides reducing cost, it also
9 reduces risk exposure and that kind of stuff.

10 CHAIR BROWN: Well, we did not try to
11 make it learn how the plant behaves. We just used
12 fixed -- we tried to make sure the temperature,
13 pressure and other type devices were working
14 properly, that all the systems to monitor those were
15 working properly. Obviously the detectors
16 themselves, you have to do something else with, if
17 you -- if you can -- kind of hard to test a pressure
18 detector unless you do something with pressure --
19 the input.

20 So anyway, I understand what you are
21 talking about. Thank you.

22 MR. REBSTOCK: Okay, sure, thanks.

23 MR. SYDNOR: So we're -- in those two
24 areas, we are close to initiating new research
25 projects to complete work in those, and the bottom

NEAL R. GROSS

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

1 two -- defining scope -- but these are a couple of
2 projects that are in our research brand that have
3 more to do with developing models, models for
4 digital I&C systems, and a plant-wide model for
5 multiple networked digital systems, and quite
6 frankly we are still trying to understand how we
7 might use these, in what context and so it would be
8 easy to -- and actually some previous work was done
9 in -- exploratory work several years ago -- in
10 developing a computerized model of a digital system
11 that was actually based on an old B&W Star control
12 system.

13 But -- and it worked but its usefulness
14 was -- is something we took a look at. We didn't
15 really determine it was that useful to us.

16 So in those two, we have them in place,
17 we really haven't started work because we really --
18 before we start work we need to understand the
19 ultimate use of these in order to do a better job
20 developing the models.

21 So that's just a quick status of other
22 things that are in that topic area, the safety
23 aspects, and again, the stuff on fire modes and
24 other areas, you will hear in detail later.

25 CHAIR BROWN: Yes, on that diagnostic,

NEAL R. GROSS

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

1 the one you talked about is -- when we get to the
2 end, somewhere could you identify which of those
3 projects that discussion falls under?

4 I mean -- I couldn't -- some of these
5 were kind of generic titles, so that the explanation
6 is crisp. Okay? Later.

7 MR. SYDNOR: Another area that is not
8 specifically on the agenda today, but just to give -
9 - for completeness -- in the advanced nuclear power
10 concepts topic area, our research there is primarily
11 geared towards supporting the NGNP/HTGR research
12 plan, which again, the ACRS reviewed in May of this
13 year.

14 We are actually a small part of that
15 plan overall, but the goal of our research is to
16 identify unique I&C aspects of these -- the proposed
17 designs with -- looking toward -- do we have the
18 regulatory knowledge and guidance to review those
19 unique aspects.

20 The stuff that is going to be similar in
21 design to what we are seeing in new reactors will be
22 perfectly capable, so this is really geared toward
23 identifying and looking at the exceptions, because
24 of the high temperature environments and things like
25 that, unique protective trips that these HTGR

NEAL R. GROSS

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

1 designs may use.

2 We have started these projects. Oak
3 Ridge National Labs is supporting us in these. We
4 actually have our first interim report of results
5 scheduled next week with NRO, almost a whole-day
6 presentation on the nature of these designs and how
7 they differ from -- in -- specific to the I&C areas.

8 So our next steps there are to
9 incorporate NRO feedback and then publish the
10 results. And if we determine we need guidance
11 improvements, we will work with that -- work with
12 NRO to support them in that too.

13 Security aspects, the topic areas there,
14 again they are not on the agenda today, but actually
15 we have done a lot of work in this area over the
16 last four, five years.

17 This is -- the Committee is probably not
18 aware that we have actually done hands-on digital
19 platform cyber vulnerability assessments. We had
20 Sandia Lab, through collaborative research
21 agreements with either a utility or the vendors
22 themselves. We obtained the equipment for the three
23 generic platforms that are approved via topical
24 reports for use by utilities: Westinghouse Common Q;
25 AREVA Teleperm; and Invensys Tricon platforms.

NEAL R. GROSS

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

1 And we actually did -- had Sandia
2 perform their -- their methodology. They have a
3 red-team methodology where they can, for lack of a
4 better word, attack a system or simulate a cyber
5 attack.

6 Obviously, these, again are limited
7 mock-ups, so we are not actually simulating a full
8 installation in a plant where a plant has other
9 layers of protection.

10 So the approach was an inside-out
11 approach where we just attacked the system to
12 determine what vulnerability it might have, should
13 someone be able to get to it.

14 And so those findings are available.
15 They are listed -- they are security-related OOU,
16 since in some cases they provide a roadmap for bad
17 guys, so we don't want that released to the public.
18 They actually get down in quite a bit of detail of
19 what you can do with these systems.

20 We have also done some studies --
21 actually these are still in progress -- where we are
22 looking at network security --

23 CHAIR BROWN: Before you go on -- excuse
24 me, before you go onto that. Are there any reports?

25 MR. SYDNOR: They are listed in the

NEAL R. GROSS

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

1 informational handout. They are in ADAMS, but they
2 are on the non-public side of ADAMS.

3 CHAIR BROWN: This one. It's in this
4 list --

5 MR. SYDNOR: Three-page -- they are
6 under the topic areas --

7 CHAIR BROWN: That's the listing you
8 have put down here?

9 MR. SYDNOR: Yes, so I believe you have
10 access to those. Is that true Christina?

11 MS. ANTONESCU: Yes.

12 MR. SYDNOR: So they should have access
13 to those. Now they are security-related OUO.

14 CHAIR BROWN: Yes, one of the -- I
15 guess, two things. I guess I'd like to at least see
16 one of them, just to see the scope. I don't know if
17 you all are interested or not, but --

18 UNIDENTIFIED SPEAKER: In that I am.

19 MEMBER SIEBER: I'm curious.

20 CHAIR BROWN: in terms of the results
21 and how they did that. Just pick one --

22 MR. SYDNOR: The most recent one we have
23 finished, actually Jeanne Dion is my project manager
24 for those, she is here today, and we have given
25 detailed presentations to the program offices on the

NEAL R. GROSS

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

1 results of those.

2 Again, because they are collaborative
3 research, we also shared the results with the
4 vendors, who were very interested in what we were
5 able to find.

6 Now these were -- again, not 100 percent
7 -- we were --

8 CHAIR BROWN: No, just looking -- we're
9 just looking for what type of results you got and
10 what type of input you did -- I am not particularly
11 interested in the Common Q because of its more wide
12 application in several projects which we have had in
13 new projects.

14 MR. SYDNOR: Common Q is an interesting
15 one because we actually did that under a
16 collaborative agreement with a utility that had a
17 mock-up of a Common Q installation in their training
18 facility that they allowed us access to.

19 So Sandia came there and ran their
20 exercise in the training facility, and the other one
21 would be the AREVA Teleperm one and I know that's
22 recent, so -- You can pull those for --

23 CHAIR BROWN: If she has difficulty, I'm
24 just -- if you would help her find them if we can't
25 --

NEAL R. GROSS

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

1 MEMBER REMPE: You should be able to
2 find them.

3 MS. ANTONESCU: Yes, it's fine. We have
4 the ADAMS number.

5 CHAIR BROWN: You do. Okay. That works
6 then. Yes Jack?

7 MEMBER SIEBER: Just so I don't
8 misunderstand what you are saying, but I look at
9 cyber security as an ongoing thing, every day
10 there's people throughout the country, including my
11 son, who does that for a living, and there are
12 people out there thinking, trying to figure out how
13 to ruin your system, and you've got to be thinking
14 how to keep them from doing it.

15 Do you have something in place that does
16 that in the whole system? And I presume you, or at
17 least you imply that a plant control system is not
18 connected to the outside world in any way, so there
19 are limited pathways these things can get in.

20 But what do you do about the day-to-day
21 kinds of thing?

22 MR. SYDNOR: We believe -- I'll say we,
23 it's more than I believe -- that the new Regulatory
24 Guide 5.71 -- if a utility establishes a good
25 program under 5.71, they will establish the layers

NEAL R. GROSS

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

1 of protection and the ongoing monitoring for
2 intrusion detection and the ongoing monitoring for
3 the changing environment, because it's never -- it's
4 never stable. It changes daily.

5 And so -- and I'm speaking for the
6 program office here -- but NSIR, through the Cyber
7 Assessment Team, has put in place monitoring where
8 we monitor cyber information that may be of interest
9 to, or the utilities need to be aware of, and that
10 information is transmitted to the utility.

11 MEMBER SIEBER: So that network is set
12 up now, because that's one of the features of the
13 industrial systems, there is a network out there
14 where all these people communicate, and an intrusion
15 someplace will reach all these IT managers within a
16 couple of hours.

17 MR. SYDNOR: DHS, the Department of
18 Homeland Security, runs one of the primary sources,
19 if we get information like that, the US CERT, which
20 looks at control systems, and a good example, as
21 everybody remembers, the Stuxnet virus and you know,
22 the information that was transmitted for that, and
23 actually I believe the NRC did a transmittal to the
24 utilities talking about the implications of that,
25 for example -- that's a good example.

NEAL R. GROSS

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

1 Like I say, we have informed the other
2 offices of our findings here. We are looking at more
3 -- you know, what additional communications could we
4 do. Could we make this information generic enough,
5 or in fact transmit an Information Notice-type
6 communication via secured communication channels to
7 the utilities and make them aware of some of these
8 findings.

9 MEMBER BLEY: Russ, in your list of
10 documents on security, two of them are NUREG/CRs
11 that are in internal review. Those are not available
12 yet?

13 MR. SYDNOR: No, they are still under --
14 we had pretty significant comments from the program
15 offices, more from a licensing use aspect and one
16 issue we are having in this area -- since we are
17 doing a biennial review I'll air some dirty laundry
18 -- these projects were started with the intent of
19 developing -- supporting the development of the
20 regulatory guidance, and then the rulemaking came
21 out and we needed to develop regulatory guidance.

22 And so ultimately we ended up falling
23 back on NIST standards for that, which are good
24 standards, in my opinion probably the best you are
25 going to find, and if you set up the program for the

NEAL R. GROSS

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

1 reg guide, I think you can have a secure facility.

2 So -- but this work kind of changed as
3 its original intent was to help us develop
4 regulatory guidance. We ended up learning a lot from
5 it.

6 But ultimately, we didn't use it
7 directly to support -- develop that reg guide. We
8 ended up basing most of the reg guide on the NIST
9 standards.

10 MEMBER BLEY: Okay, but at least you had
11 the knowledge of what you are dealing with.

12 MR. SYDNOR: It's the knowledge and we
13 are still trying to figure out how to share that
14 learning more.

15 CHAIR BROWN: One more before we leave
16 this. It's always an exciting subject. You said --
17 you commented that you made these presentations to
18 the program office. I presume that's NRR, NRO --

19 MR. SYDNOR: And NSIR.

20 CHAIR BROWN: and NSIR, with the results
21 of your reviews for the vulnerabilities of these
22 platforms, at least within the scope with which you
23 were able to do it.

24 Obviously the purpose is to have these
25 things be used. Are you aware of any plans they have

NEAL R. GROSS

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

1 or utilization of those results to -- that resulted
2 in their actions backing their evaluations of the
3 projects or the platforms that are in service now?

4 MR. SYDNOR: Well certainly one of those
5 -- I have to be careful how I say this. We didn't
6 credit our research as part of the licensing of the
7 Oconee platform. But some of our work was done at
8 NRR's request in their licensing review of that
9 platform. But the research is not formally credited
10 in the SER.

11 CHAIR BROWN: So you are not really
12 aware of any -- that's a specific example of what
13 you are --

14 CHAIR BROWN: Yes well Oconee came to
15 mind since that's the one that's in service right
16 now.

17 MR. SYDNOR: Or being put in service.

18 CHAIR BROWN: But I mean there's two
19 other projects in it under the NRO world where the
20 platforms are -- two or three of them, three of them
21 as a matter of fact -- where these platforms are
22 being used and the equipment's not even been
23 designed yet and the licensing has not been
24 completed.

25 And so I guess what -- it would be

1 interesting to see, it would be nice to see if this
2 information had been utilized, and there were
3 considerable discussions on these projects relative
4 to the cyber security aspects of it.

5 And I guess it would be interesting to
6 see how that information is being used, or not used.

7 MR. SYDNOR: I can say that the
8 reviewers of those platforms in NRR, NRO, were part
9 of our information exchange and so the knowledge
10 they gained about these systems and how they can
11 behave, I'm confident are being factored into their
12 review and thinking.

13 Again, these are collaborative research
14 projects with the vendors, so I mean -- and in, I
15 think in all three cases they are, I'll say dated
16 versions of the platforms. I know that at least two
17 out of the three vendors are you know, looking at
18 updated versions.

19 And certainly in new reactors, it's
20 probably going to be different software and
21 potentially even different hardware, because they
22 are going through updated to those different
23 platforms.

24 CHAIR BROWN: Okay, let me try this
25 again. Would you be able to provide us or me with at

1 least a short summary of, by talking with them about
2 some things they did, I mean the Common Q platform
3 is in process right now, in two projects, the AREVA
4 platform is in another project, so they are not
5 closed out relatively from that standpoint.

6 And the fundamental concern comes down
7 to when you look at the way these platforms are
8 being used, they are sending data everywhere and Reg
9 Guide 5.71 establishes a set of zones or whatever
10 you want to call it, protective walls, through
11 which, theoretically nothing -- if you do it right -
12 - nothing should get through.

13 There's always the concern with the
14 information being sent out to other parts of the
15 plant, under some sort of == like if you have got a
16 problem you have got to go up to the Technical
17 Support Center, the Emergency Operations Facility,
18 what's the validity of their data, how good is their
19 data. Is it being compromised? How could it be
20 compromised, etcetera, etcetera?

21 So there is some interest to make sure
22 communications between the main control room and the
23 other facilities are based on the same -- they are
24 all working from the same sheet of music in terms of
25 data that they are making -- from which they are

NEAL R. GROSS

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

1 making -- or drawing conclusions or making
2 decisions.

3 So one of the interests here is to try
4 to see, you know, is the limited, you know -- admit
5 these were limited studies, and weren't, you know
6 full-bore and you can only do what you have got, but
7 you would like to see some of that being applied in
8 terms of how it's being passed on, such that the
9 applicants have some constraints on them in terms of
10 how they are laying out these systems all the way
11 through all the zones.

12 So anyway, I'd just -- that would be
13 useful, if I -- if we could get not a big, whole lot
14 of it, but just some of it.

15 I mean most of the conversations we've
16 had so far is that that's being put off until after
17 the license is issued and relative to architectures
18 that are put in place and things like that, in order
19 to support the ability to have a security
20 communications setup on the platform -- with the
21 platforms.

22 MR. SYDNOR: Well, as the Committee is
23 well aware, I mean there's been a number of
24 discussions about how much review of cyber security
25 occurs during --

1 CHAIR BROWN: I don't want to get back
2 into that one.

3 MR. SYDNOR: Okay.

4 CHAIR BROWN: We've been there and done
5 that and we have got other venues for that. Yes,
6 Jack.

7 MEMBER SIEBER: On a slightly different
8 subject, could you describe very briefly what you
9 plan to do in the solar storm impact study?

10 MR. SYDNOR: Oh yes, I didn't get to
11 that yet. And so the second topic area on this slide
12 was added to the research plan actually partially by
13 request of a previous Chairman of the Commission,
14 and was initially just primarily looking at the
15 impact -- revisiting the impact of electromagnetic
16 pulse because of the installation of more digital
17 equipment in nuclear power plants. It's something he
18 personally requested.

19 The scope of that was expanded to look
20 at high radio frequency threats also and so we had
21 Sandia do a study of that. There was actually a
22 NUREG published in 1983 and I think I may have put
23 the number of that on my handout. Hopefully I did.

24 It's an old NUREG but it studied EMP
25 effects on nuclear plants at that period of time,

NEAL R. GROSS

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

1 concluded that because of the rugged construction of
2 the buildings, concrete structures and things like
3 that, they would survive the EMP and could achieve
4 safe shutdown.

5 That's not -- nobody is going to say the
6 grid's going to survive because the grid is
7 susceptible to EMP events. Those are well-published
8 studies on that.

9 So we revisited that, had Sandia -- and
10 Sandia actually did that old NUREG too -- they
11 updated their models, we visited a couple of new
12 plants, took a look at installation of digital
13 equipments in the plants, and they documented the
14 results of their study to us. Again, this is -- not
15 because of the EMP, but because of more the high
16 radio frequency threats, implications in there -- is
17 security-related OOU, and made that -- made the
18 results of that study available to NSIR to determine
19 if we needed to do something new or different
20 because of our findings there.

21 And actually, Sandia's conclusion was
22 that even with digital systems, where they were
23 installed in the plant, they were shielded well
24 enough that they were likely to survive and the
25 plants would still be able to achieve safe shutdown.

NEAL R. GROSS

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

1 MEMBER SIEBER: Yes, but not all digital
2 systems are inside plant buildings.

3 MR. SYDNOR: No, this is -- we did --
4 the grid, like I said, the impact of these things on
5 --

6 MEMBER SIEBER: You've got the grid,
7 you've got transmitters all over on tanks and
8 equipment, switchyard stuff, which, you know,
9 station blackouts now have gathered attention
10 recently, since --

11 MR. SYDNOR: This mainly looked at
12 internal impacts.

13 MEMBER SIEBER: Okay, but all that other
14 --

15 MR. SYDNOR: And so there's limitations
16 on the study.

17 MEMBER SIEBER: rest of it is important
18 too.

19 MR. SYDNOR: The biggest limitation is
20 off-site power I would say.

21 MEMBER SIEBER: Right, well, that's what
22 we think so far, right. That's the obvious one.

23 MR. SYDNOR: We also had them take a
24 look at -- use the analysis they did in the EMP
25 study as a basis for taking a look at

NEAL R. GROSS

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

1 geomagnetic-induced currents, and what sort of wave
2 forms they might produce internal to the plants.

3 And so that's -- they used their
4 modeling from the EMP to make some assumptions about
5 how closely those electromagnetic wave forms might
6 align, and their impact on the plant and documented
7 that study.

8 Both of those reports are available too,
9 and the ADAMS numbers are listed. We --

10 MEMBER SIEBER: Are they restricted?

11 MR. SYDNOR: Yes.

12 MEMBER SIEBER: Thank you.

13 MR. SYDNOR: Non-public, yes. Primarily
14 because of -- there are some threat implications in
15 the H -- it's not my business at all. We let NSIR
16 make those determinations.

17 And so really this was exploratory
18 research to determine if there was a -- you know,
19 regulatory impacts, primarily, is there something
20 else we need to be doing in regulatory space.

21 A lot of this information is actually
22 publicly available. Our studies are not, but I mean
23 a lot of the implications of EMP, geomagnetic, we
24 know there's been failures of distribution systems
25 due to geomagnetic storms. There was actually just a

NEAL R. GROSS

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

1 big article yesterday about the potential for
2 damaged communication systems and electric grids due
3 to major solar storms.

4 MEMBER SIEBER: Yes, I drove through it.
5 The light don't work, traffic lights.

6 CHAIR BROWN: Well, vacuum tubes and
7 magnets work much better than solid-state devices
8 do, unfortunately. But shielding is a big issue, I
9 mean that's what we did with the Navy side of it.
10 You've got all that steel around it so you make sure
11 all your points of entry are very, you know, very
12 well shielded, and that -- but these are more open
13 plants relatively.

14 So it was interesting when you made the
15 comment that Sandia concluded that there was enough
16 shielding around the plants, which are concrete and
17 reinforced --

18 MR. SYDNOR: It has to do with the way
19 the waves are actually transmitted into the plant.

20 CHAIR BROWN: Yes. I gather that. I'm
21 not -- I don't pretend to be an electromagnetic
22 expert from that standpoint.

23 MEMBER SIEBER: It is one thing to come
24 to a judgement. It's another thing to prove it
25 significantly.

NEAL R. GROSS

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

1 CHAIR BROWN: Well, go off to Solomon
2 Island, it's as good a way to test this stuff, if
3 you want to.

4 MR. SYDNOR: One of the reasons we
5 picked Sandia to help us with this study is they --
6 for DOD they actually do offensive and defensive
7 capabilities so they have a lot of knowledge about
8 how digital systems behave.

9 CHAIR BROWN: Are you done Jack?

10 MEMBER SIEBER: Yes.

11 CHAIR BROWN: Okay.

12 MR. SYDNOR: And then finally -- I am
13 on track here -- I'm really not going to talk about
14 these unless -- these are some of the older projects
15 that we rolled into the new plan that given the
16 resources, we will eventually get to them. We have
17 not started anything actively on them yet.

18 There actually was a fair amount of work
19 done in the past on the first topic there, including
20 development of Reg Guide 1.180, but there's still
21 some outstanding improvements there that we are
22 looking at, and the last issue may have more
23 emphasis given Japanese events

24 CHAIR BROWN: Okay.

25 MR. SYDNOR: So overall the research

NEAL R. GROSS

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

1 program is targeted to, as you can see, either
2 answering specific regulatory questions -- a good
3 example develop a reg guide for cyber security;
4 improve regulatory guidance -- I'd say the majority
5 of our work is looking at improvements to our
6 current processes or changes we should make due to
7 changes in technology.

8 And a new area that we are spending more
9 time on and you will hear more about it later, is
10 knowledge management, how to keep our regulatory
11 structure up to date and maybe look at some
12 efficiencies there too.

13 From an assessment standpoint my
14 personal assessment is that we need improved
15 interface with program offices. Too often in the
16 past, we started work without adequate involvement
17 of the user offices in the statements of work and we
18 are trying to change that now.

19 We get them involved up front and we
20 want them involved for interim review and feedback
21 and finally, review of research results.

22 Too often what we have done in the past
23 is have them review the results and they bring them
24 -- this is not the rock I asked for type situation.
25 So those are some of the improvements we are trying

NEAL R. GROSS

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

1 to drive.

2 MEMBER BLEY: How are they responding?

3 MR. SYDNOR: Very well. I mean they
4 obviously have time limitations so we have to work
5 around those, but I have found as we engage in them,
6 we get a lot of good feedback and obviously tailor
7 the work to support them better.

8 Actually that's all --

9 MEMBER BLEY: I know you have a very
10 broad program and you are driven by user needs, but
11 have you looked out further to see what are the
12 areas you might need to be looking at in a few
13 years, where needs might arise and can you tell us
14 anything about those?

15 MR. SYDNOR: Actually, I could. Briefly,
16 one topic area, one project that we have in our
17 knowledge management area is called emerging
18 technologies. Milton will cover that a little bit
19 later.

20 And so every so often we do a study of
21 emerging technologies and use that as a feedback
22 mechanism. But I would say even our other work, when
23 you hear discussions later today about our
24 collaborative -- how we have expanded our
25 collaboration worldwide, you know I think we have

NEAL R. GROSS

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

1 lots of chances -- opportunities for those type of
2 inputs.

3 Okay, thank you.

4 CHAIR BROWN: One question before we
5 transition. We are not going to through the acronyms
6 are we?

7 MR. SYDNOR: No. I didn't put a
8 questions slide. Unless you want to?

9 MEMBER BLEY: We are not going to go
10 through --

11 (Laughter)

12 CHAIR BROWN: No, we are not going to go
13 through the acronyms. All right. We'll want to come
14 back to this later, after we go through the next
15 presentations an up through noon anyway.

16 But the matrix that you all provided did
17 a little bit -- I went through the plan that we had
18 and it was -- it was a little bit difficult to map
19 the items in the matrix, which is a good matrix, to
20 some of the specific areas in the plan.

21 So I am not too sure how much I need of
22 that, but at least I'd like to have that at our
23 fingertips, particularly for this biennial report,
24 if I get the appropriate questions here.

25 MR. SYDNOR: The matrix is -- that's

NEAL R. GROSS

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

1 because the matrix is generated out of the budget
2 system which really doesn't align with --

3 CHAIR BROWN: I'm familiar with the
4 technique, yes, I've used it myself in the old days.
5 So if you could provide some type of a little
6 mapping at some point, about how does this connect
7 back into some of the items in the -- specifically
8 written in the overall plan.

9 MR. SYDNOR: That's something I could
10 provide you in a follow-up too now that --

11 CHAIR BROWN: Yes, that's what I am --

12 MR. SYDNOR: I understand your issue.

13 CHAIR BROWN: Yes. Yes, not right now.

14 This would be a follow-up, at post-meeting, type
15 stuff, just so I have a clue as to how this goes to
16 that and how they connect.

17 MR. SYDNOR: Yes that's probably
18 something I could get to Christina within a week or
19 --

20 CHAIR BROWN: Okay, and if I get some
21 other questions as I am going, I will -- I will feed
22 those back via Christina also.

23 MR. SYDNOR: Very good.

24 CHAIR BROWN: Any other questions? Jack?
25 John? Joy?

NEAL R. GROSS

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

1 MEMBER REMPE: I have one.

2 CHAIR BROWN: Yes go ahead.

3 MEMBER REMPE: Several times you have
4 talked about, you have borrowed equipment event from
5 vendors and you've tested it, and presented the
6 results. Are there some concrete examples where you
7 saw changes that the vendor has made because of your
8 interactions with them?

9 MR. SYDNOR: Specifically, in the case
10 of AREVA -- Jeanne will keep me straight that I
11 don't mis-speak. We met with them. They were very
12 interested in the results of the testing and they
13 are looking at -- again, they are doing updates to
14 their equipment so they are looking at, do the
15 updates take away the concern.

16 CHAIR BROWN: Does that answer your
17 question Joy?

18 MEMBER SIEBER: Yes sir.

19 CHAIR BROWN: So okay, they'll at least
20 start paying attention to it, we hope. All right.

21 MR. SYDNOR: I'll go a little further on
22 that one. We are also following up with them to
23 nudge them a little bit, informally.

24 These weren't licensing activities. In
25 fact, like, I'll say it again, they were

NEAL R. GROSS

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

1 collaborative research agreements. So vendors have
2 been very cooperative and very interested in the
3 results of the work. So these are not formal
4 licensing or inspection activities, so there's --

5 CHAIR BROWN: Yes, but her point's
6 correct, I mean if you go off and you run a bunch of
7 tests on somebody's equipment you'd like to see that
8 oh gee, they found a few problems. We are going to
9 go fix those. That's kind of what you're looking at.

10 MEMBER REMPE: Yes.

11 CHAIR BROWN: That's kind of the
12 layman's statement for those of us who are
13 challenged somewhat. So all right, I guess we are
14 ready to move on to the next setup, which is the
15 failure modes and effects analysis, excuse me, fault
16 modes and effects analysis.

17 You might explain to us why you changed
18 failure modes and effects stuff to fault modes.
19 That's an interesting thought. I've never ever --
20 faults are things that happen and stay there and
21 then get blown up because something --

22 MR. BETANCOURT: Good morning. My name
23 is Luis Betancourt. I am from the Office of
24 Research, Division of Engineering, and I am the
25 project manager for this project.

NEAL R. GROSS

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

1 Alongside here with me is Dr. Sushil
2 Birla who is also the technical adviser for the
3 DI&C, also for the office of research.

4 So today we are going to be talking
5 about the NUREG International Agreement Report 0254,
6 suitability of fault modes and effects analysis for
7 regulatory assurance of complex logic in digital
8 instrumentation control system.

9 The question that you have, why did
10 change fault modes instead of failures modes is
11 going to be addressed in second slide so I would
12 like to refer that question later on.

13 So a little bit on the agenda today.
14 First I'm going to be talking about a little bit of
15 the background, some of the ACRS' concerns about
16 failure modes analysis, along with how is the
17 NUREG/IA doing on the process.

18 Then after that I'm going to be talking
19 about some of the research method which is
20 analytical. I'm first going to be talking about some
21 of the characteristics between hardwired systems and
22 Complex Logic-intensive systems as far as some of
23 the issues and limitations.

24 And then after that I'm going to be
25 showing you what are some of the preliminary reports

NEAL R. GROSS

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

1 that we have found. And finally what I'm going to be
2 doing about it and some of the questions that we
3 have from some of the results and we are going to be
4 doing about that.

5 So the first thing that I would like to
6 do is basically show a little bit of the history of
7 the ACRS events already past three years.

8 As you may recall, the stakeholders'
9 quest to risk-inform the licensing review that was
10 considered actually in ISG-03. Also -- that is also
11 documented in NUREG CR that is on the BNL. Also Alan
12 Kuritzky talked about them on the previous ACRS
13 presentation.

14 Back then there was no expectations
15 basically that in certain quarters the likelihood of
16 software fault leading to a safety function failure
17 would have been so low that common-cause failure was
18 actually not significant, and the approach to risk
19 estimation at that time basically sought to build on
20 the FMEA results. And that's basically this over
21 here.

22 So during the review, ISG-03 was in the
23 ACRS meeting, is a second letter, basically the ACRS
24 emphasized the importance of identifying failure
25 modes, and also to help the reviewers also to reveal

NEAL R. GROSS

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

1 the common-cause failures analysis, which led to the
2 SRM, which I'm going to be talking about on the
3 later slides.

4 Also in the review on ISG-06 that was
5 done back in 2010, the ACRS also in recommendation
6 number four, they ask to look on the suitability of
7 software failure fault analysis to identify some
8 critical software failures modes.

9 CHAIR BROWN: That was back at the --
10 that was our last research plan review.

11 MR. BETANCOURT: Exactly.

12 CHAIR BROWN: Okay.

13 MR. BETANCOURT: Also, which led to the
14 NRC --

15 MR. BIRLA: Despite 76, the letter was
16 not as a result of the research plan review. It was
17 a result of the ISG-06 review.

18 CHAIR BROWN: Oh, okay. Right. Thank you
19 for fixing, correcting.

20 MR. BIRLA: Our work that Luis is
21 reporting on, was launched much earlier, responding
22 to the SRM which he is going to talk about.

23 CHAIR BROWN: I'm just remembering a
24 thought, and I -- that I vaguely remembered back in
25 the research plan where we talked about failure

NEAL R. GROSS

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

1 modes and effects analysis. I don't know whether we
2 explicitly talked about it from that standpoint. But
3 my brain is old so it doesn't work so well all the
4 times. You can go on.

5 MR. BETANCOURT: Okay.

6 CHAIR BROWN: Thank you.

7 MR. BETANCOURT: Also, all of these
8 concerns were actually incorporated into the 2010-
9 2014 research plan which actually Russ Sydnor will
10 talk about that.

11 Today we are going to be talking about
12 some of these results and some of the steps that we
13 have on this long road into that direction.

14 So in July 2008, we basically -- we had
15 the SRM that was basically what -- that I talked
16 about before, was part of the recommendations of the
17 ACRS meeting that we should report the progress in
18 identifying and analyzing the I&C failure modes.

1 The reports that you see here today that
2 are the green ones are the ones that we are going to
3 be talking about today. The yellow one is basically
4 something that we are currently working on, which is
5 the second Research Information Letter.

6 The first one is basically the
7 presentation that Sushil is going to be leading

NEAL R. GROSS

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

1 today and the NUREG/IA is the work that we actually
2 performed with the French Institute of Radiological
3 Protection and Nuclear Safety that was actually
4 performed -- we started working with them in 2010
5 and it was actually -- we are going to be addressing
6 this today.

7 CHAIR BROWN: What does RIL mean?

8 MR. BETANCOURT: Research Information
9 Letter.

10 CHAIR BROWN: Oh, okay. Thank you.

11 MR. BETANCOURT: You're welcome. And the
12 second part of the SRM is basically to discuss the
13 feasibility to apply thermal analysis to
14 quantification research associated with digital I&C.

15 This is also being addressed by the
16 Sandia folks with BNL that Alan Kuritzky presented
17 in the last presentation from the last ACRS meeting,
18 and the third RIL decision is going to be strictly
19 narrow and to the boundary of the SRM. These are all
20 the projects that we are envisioning in order to
21 close the SRM.

22 MEMBER SIEBER: There is a difference
23 between faults and failures. One is an instantaneous
24 thing that may disappear. The other one is something
25 like a broken wire or a burnt-out resistor that is

NEAL R. GROSS

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

1 there and you can go and find it with the
2 appropriate diagnostic tools.

3 Do you cover both faults and failures,
4 or just one, either faults or failures, in your
5 analysis?

6 MR. BIRLA: This work is focused on
7 software or other forms of implementation of logic,
8 we primarily think in terms of software, and --

9 MEMBER SIEBER: Okay, so that -- that
10 would be a fair --

11 MR. BIRLA: Well, this is the
12 contention, and he is coming to it so --

13 MEMBER SIEBER: Okay. I should be quiet
14 and pay attention.

15 MR. BETANCOURT: Basically I would like
16 to start talking about, before going into the
17 discussion of the report, what do we mean about
18 software FMEA.

19 CHAIR BROWN: Before you go onto that,
20 if you could backtrack to the previous slide again?

21 MR. BETANCOURT: To this one?

22 CHAIR BROWN: The two yellow jobs you
23 are showing there, are those -- you said those are
24 not done or those in the --

25 MR. BETANCOURT: That's a work in

NEAL R. GROSS

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

1 progress right now.

2 CHAIR BROWN: Work in progress?

3 MR. BETANCOURT: Yes.

4 CHAIR BROWN: And --

5 MR. BETANCOURT: Ah, okay, that was
6 actually part of the NRC expert clinic.

7 CHAIR BROWN: The what?

8 MR. BETANCOURT: The NRC expert clinic
9 that Sushil is going to be talking about later
10 today. We actually have the result which is going to
11 be in two reports.

12 The first one is the one that Sushil is
13 going to be presenting, which basically builds on
14 the sources of uncertainty and software.

15 The second one is going to be building
16 on the first one, basically now that we identify the
17 source of uncertainty, what are you doing about
18 identification of failure modes and effects
19 analysis.

20 The final one is basically -- the third
21 RIL is basically it addresses on risk quantification
22 of these failure modes in the presence of these
23 uncertainties. I don't know if that clarify a little
24 bit your question on that.

25 CHAIR BROWN: I'll think about it.

NEAL R. GROSS

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

1 (Laughter.)

2 MR. BETANCOURT: Do you want to saying
3 about that or --

4 MR. BIRLA: Yes, we can pick that up
5 later when I give my presentation.

6 CHAIR BROWN: Okay.

7 MR. BETANCOURT: Okay. So basically we
8 did a little review on 28 publicly available
9 publications that we have found on the suitability
10 of software failure modes and effects analysis.

11 What we have found is basically that
12 this software FMEA has been useful and effective in
13 identifying and mitigating potential hazards to
14 discover consequences of some hardware malfunction,
15 and also to identify some requirements to mitigate
16 the effect of thorough software under specific
17 conditions.

18 What we have found is that some of the
19 experts, they actually justify the use of software
20 from very early in the use of the development cycle
21 that will be implemented in the hazard analysis and
22 the hazard analysis, and we haven't found anything
23 or claimed to justify the use of software FMEA for
24 safety assurance.

25 What we have found is basically two

1 types of software FMEA. The first one that you see
2 on the board is the system level software FMEA, and
3 they are usually performed when you have the
4 software level design, when you got top-level design
5 documents but you haven't any source codes yet.

6 It basically examines the structure and
7 the basic protection of the design. It looks at the
8 software architecture and at the same time it looks
9 for safety characteristics, in other words basically
10 you got the design for protection mechanisms, you
11 got the basis of a partitioning, who is going to go
12 run what, who's going to go who.

13 The second one that you see below is a
14 detailed level software FMEA. That one is basically
15 implemented in the design at the level of variables
16 and coded algorithms.

17 The problem with that -- and also that
18 one has been used for identify unexpected paths
19 which is limited to the design documentation, which
20 could actually adverse to the effect on safety.

21 What we have found is basically most
22 people are using system level software FMEA and it's
23 because basically on this -- on the benefit and the
24 cost ratio, when you have a system level FMEA, you
25 can get 90 percent of the benefit out of the 10

NEAL R. GROSS

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

1 percent cost.

2 When you got the detailed level FMEA
3 it's more rigorous and more labor intensive so you
4 have 10 percent benefit out of the 90 percent of the
5 effort.

6 People --

7 CHAIR BROWN: Stop right there for a
8 second. So your conclusion out of this -- I'm just
9 trying to draw something from my simple mind here --
10 is that the system level software, at least within
11 the construct in which you all look at it, gives you
12 the biggest bang for the buck.

13 MR. BETANCOURT: Yes.

14 CHAIR BROWN: Is that fair? And then the
15 detailed level is you get some trinkets out of it
16 but it's not as useful?

17 MR. BETANCOURT: Exactly.

18 CHAIR BROWN: And by system, I still
19 don't understand the difference between system level
20 FMEA based on your comments, as opposed to detailed
21 level, unless I missed something.

22 Detailed level to me is bits and bytes.
23 System level is algorithms, partitioning,
24 subroutines, global variables, global cache or as
25 opposed to partitioning stuff so that you don't have

NEAL R. GROSS

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

1 global variables which are getting, you know --
2 which can contaminate every channel with something,
3 if they are -- depending on how they're used.

4 So I'm trying to get a feel. Dennis, go
5 ahead.

6 MEMBER BLEY: Before you answer Charlie,
7 I'd like yo to put in a little perspective for me.
8 If I look at a hardware system and do an FMEA, I
9 look at every component and I say, what are all the
10 ways in which this can fail? That's the failure
11 modes.

12 And then I say, in each of those failure
13 modes, how does it affect the system in which it
14 resides? Usually it's just a point-wise failure but
15 you like to think of how that could cascade.

16 So how do you take that concept and
17 apply it to your systems? What are the pieces you
18 are looking at in either kind of an FMEA, what are
19 the ways in which you are looking for failure, and
20 how do you look at the effects from it?

21 So I assume there's an analog back to
22 the mechanical system somehow. If not, just tell me
23 what you are doing in a way we can understand it in
24 these two kinds of FMEAs.

25 MR. BIRLA: So let's back-track a couple

NEAL R. GROSS

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

1 of steps. What he's reporting is what we have found
2 in collecting information from others. In this
3 particular case he is quoting an expert who's
4 published about 15 years ago a paper on software
5 FMEA.

6 When we interviewed the individual, it
7 came out that really there are two levels -- this is
8 where the two levels come from. So to come back to
9 Chairman Brown's question on what do you mean by
10 system level, let me explain that, in that context.

11 So it is actually not a software FMEA.
12 It's a system FMEA examining the effect on the
13 output of the system if something goes wrong with
14 the software.

15 NASA does that at the conceptual level
16 when they have a concept, even before they have a
17 design, to do an overall conceptual architecture and
18 then iterate from there on.

19 And then the expert's view -- the expert
20 that he cites here and that corroborated with the
21 NASA experts that we interviewed later on -- is that
22 that's where they derive a lot of value.

23 MEMBER BLEY: Okay. Before you leave
24 that one, let me try to parrot back what I think you
25 are saying and deal with my hardware thing at the

NEAL R. GROSS

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

1 same time. Hardware side, we could look at a
2 component or we could look at subcomponents with --
3 inside it, sort of analogous to this, but we look at
4 one thing and say how can this fail.

5 I think what you are telling me is the
6 system level FMEA, we come in with somehow a
7 predetermined list of here are the ways my software
8 can fail, these are the software failure modes.

9 I look at my system and say which of
10 these failure modes can affect my system and how can
11 I affect the system? That's not it.

12 MR. BIRLA: No.

13 MEMBER BLEY: So what do you --

14 MR. BIRLA: So again, we are reporting
15 what he heard. This is --

16 MEMBER BLEY: I know, but --

17 MR. BIRLA: What they are saying is that
18 even though the paper has been published as
19 software FMEA, what they are actually doing is an
20 overall system level effect analysis, effect of
21 software failing for whatever cause.

22 MEMBER BLEY: Well, that's what I tried
23 to say to you. I come in and I say, I must know how
24 software fails somehow, so I look at my system and
25 say how can each of these possible failure modes in

NEAL R. GROSS

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

1 my software affect my system, but you said that's
2 not -- that's not it.

3 MR. BIRLA: They don't even have a --

4 MEMBER BLEY: That's what I thought I
5 heard you just repeat back to me so I am confused.

6 MR. BIRLA: If something goes wrong with
7 software --

8 MEMBER BLEY: Or something we don't know
9 about, just something, an amorphous something goes
10 wrong.

11 MR. BIRLA: So this is at a very early
12 stage in the lifecycle.

13 MEMBER BLEY: But I'm looking at a
14 conceptual design of a hardware system.

15 MR. BIRLA: Not a hardware system, a
16 total system.

17 MEMBER BLEY: A total system that
18 includes hardware and software. So it could be a
19 feedwater system, perhaps, that includes the control
20 systems that drive it and the hardware that actually
21 opens and closes valves. Could be.

22 MR. BIRLA: Could be, yes.

23 MEMBER BLEY: Okay, so go ahead. We've
24 got this system that includes everything. Now what
25 do they do?

NEAL R. GROSS

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

1 MR. BIRLA: So if the effect is
2 undesirable.

3 MEMBER BLEY: But the effect of what?
4 That's why I'm having trouble. The effect of what?

5 MEMBER STETKAR: Theoretical discussions
6 of theoretical concepts don't fail in the real
7 world, so what I think Dennis is trying to get and
8 what I've been trying to understand reading all of
9 this is what do people really do?

10 If you've read all of these research
11 papers, what have they done in the context of a
12 real, integrated system? You said NASA uses it.

13 MR. BIRLA: Yes.

14 MEMBER STETKAR: I think you other
15 references is that FAA uses it, chemical processes -
16 - what do they really do if these are the two
17 different concepts?

18 So if we take an integrated system, as
19 Dennis has said, a digital feedwater control system
20 where the inputs are levels and flows, and the
21 output moves a valve, like this, and in between
22 you've got some software kind of stuff, what do
23 these software experts do with either that system,
24 or the software kind of stuff -- can you explain it
25 in those simple terms, in that system?

NEAL R. GROSS

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

1 MR. BIRLA: So if the effect is
2 something undesirable --

3 MEMBER STETKAR: Okay, the valve goes
4 open too much. That's the undesirable thing.

5 MR. BIRLA: Or even at a system level,
6 that you have a loss of the safety function let us
7 say --

8 MEMBER STETKAR: No, no, no, no, though,
9 the valve goes open too much. I want to hold you to
10 specifics. That's an undesirable thing because I
11 know then what will happen.

12 You can't just say -- you know, it is
13 undesirable that I dropped that but it really
14 doesn't have any implication on anything. So just
15 saying something is undesirable means everything
16 must always work absolutely perfectly, every second,
17 for the entire life of the universe.

18 MR. BIRLA: No. No.

19 MEMBER STETKAR: Okay, well, then you
20 have to define what undesirable is.

21 MR. BIRLA: Yes, so the criticality of
22 the effect is analyzed and --

23 MEMBER STETKAR: Okay.

24 MR. BIRLA: That's why --

25 MEMBER STETKAR: The valve went open too

NEAL R. GROSS

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

1 far.

2 MR. BIRLA: Okay, and I mentioned the
3 loss of a safety function just to give you an
4 example of what they would do if it is that
5 critical.

6 So in the case of NASA, it's a mission.
7 If there's a loss of mission, then you look at the
8 dependency on the software, and either you have an
9 alternate path, assuming that it is going to fail,
10 or you prove that it can't, and most of the time it
11 is not possible to prove that it can't, so they
12 develop an alternative path.

13 MEMBER BLEY: I am still having real
14 trouble. If I'm NASA, and I've worked with NASA,
15 loss of mission is a big general thing. It's like
16 loss of the power plant. Either it fell out of the
17 sky or you killed everybody who was up there. It's
18 one of those two things.

19 MR. BIRLA: Or it could be one of the
20 scientific missions.

21 MEMBER BLEY: But do they just -- do
22 they just hypothesize, well, I've got this system
23 and I'm worried about loss of mission and maybe
24 something in the software could cause that, so is
25 that my analysis?

NEAL R. GROSS

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

1 How do I determine that something in the
2 software could have affected loss of mission? To do
3 that it would have had to have affected something at
4 a lower level, as well.

5 And then how do I prove that thing
6 couldn't have happened if I don't even know how it
7 happened, or what the -- it's called a failure modes
8 and effects analysis. How do I identify a failure
9 mode and how do they identify the effect and why is
10 it useful, and I think you said why do you get 90
11 percent out of the first level?

12 So nothing you've said, either of you,
13 tells me how they identify a failure mode or how
14 they identify an effect of the failure mode, and how
15 they try to remove that from the system.

16 It's got to come down to something more
17 concrete than just those global statements or you
18 can't do the analysis.

19 MR. BIRLA: So the analysis is more
20 focused on the criticality of the effect, and
21 subsequent engineering is driven by that.

22 MEMBER STETKAR: Okay.

23 MR. BIRLA: So one possibility -- and
24 this is a very common possibility -- is that if the
25 effect is serious, like loss of mission or loss of a

NEAL R. GROSS

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

1 safety function, then find an alternative path that
2 doesn't depend on --

3 MEMBER STETKAR: But I didn't hear a
4 path that got me to the critical loss of mission
5 thing.

6 MEMBER STETKAR: Let me take it back to
7 my simple valve. The valve goes open. The entire
8 universe is destroyed. Okay, so it's not -- by
9 definition.

10 It's a simple valve, but if it goes open
11 the universe is destroyed. Now, how does this
12 process identify what types of failure modes may
13 cause that valve to go open?

14 We have identified -- we have identified
15 a failure. We have identified that it's a pretty --

16 MEMBER BLEY: Critical.

17 MEMBER STETKAR: critical failure. What
18 does this process do in that context? That's the
19 context.

20 MR. BIRLA: So, in that context, if it
21 is -- the main thing on the software side is the
22 dependency. If it is dependent on software, either
23 you'd be able to prove that the failure cannot occur
24 because of software -- that means the software is
25 going to function as intended.

NEAL R. GROSS

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

1 And if you cannot establish that, then
2 have an alternative to that software. The
3 alternative could be a compromised mission, a safe
4 state or a path that does not depend on software,
5 like a hardware-based solution.

6 MEMBER STETKAR: In this example then,
7 the alternative to the software costs all the
8 resources in the universe. It's impossible to create
9 a valid alternative. How do they determine the
10 viability of the software before they make the
11 determination that I need an alternative, or an
12 alternative is impossible and therefore I can't have
13 this valve?

14 MR. BIRLA: Yes, at that early lifecycle
15 stage, they are not determining the viability. They
16 are determining whether it is possible to establish
17 that the software will function as intended.

18 And if it something very simple, you can
19 go that route, but most of the time, the route is --
20 have an alternative, not software-based solution to
21 fall back on.

22 So in our case it is the diverse
23 actuation system.

24 CHAIR BROWN: It is interesting that you
25 say that. Now I had this discussion 28 years, when

NEAL R. GROSS

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

1 we were first trying to put this stuff into naval
2 nuclear programs.

3 And one of our proposals was we are
4 going to do a hazard analysis on the software.
5 Question we ask is how are you going to do the
6 hazard analysis -- John's question and Dennis'
7 question.

8 What are the metrics and what do you do?
9 We got a non-answer back, similar, fuzzy answer
10 similar to what we are getting right now. And this
11 is not a criticism, this is just a statement of
12 fact.

13 And you made an observation there that
14 if you can't conclude, you then -- you do something
15 else to mitigate that, but how you get there --
16 since we couldn't come to that conclusion as to how
17 you would do a software hazard analysis, we said we
18 are just going to assume the software breaks, in
19 whatever mode software can break, in whatever mode
20 the system can break, and we are going to put in a
21 second backup that will work, and therefore we are
22 not going to work on that one because it's too hard.

23 And I'm not saying we shouldn't think
24 about it, and work on it, it's just that you've --
25 we just spent 15 minutes showing how difficult it is

NEAL R. GROSS

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

1 just to define that system level versus the
2 detailed, because it -- and this is just based on
3 experience right now of about dozens and dozens of
4 systems, almost everything that somebody
5 contributed, and I'll say -- I say almost because
6 I'm sure there's something that I missed -- that was
7 attributed to a software failure was fundamentally -
8 - that it was designed wrong.

9 You asked us if the software did what
10 you told it to do and it -- what it's supposed to do
11 and the data came in and said oh okay, well I'm
12 going to take this -- actually you don't want me to
13 take but that's what you told me to do and I am
14 going to do it.

15 And those were classically not defined
16 as software failures. They were defined as design
17 failures. People did not lay out the actions that
18 needed to be taken.

19 Now, I am not saying that's completely
20 true in all circumstances because probably not, but
21 -- go ahead John, I --

22 MEMBER STETKAR: Dennis's time is
23 limited and I know we need to get through the
24 presentation --

25 MEMBER BLEY: Okay, we have got a little

NEAL R. GROSS

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

1 bit of time.

2 MEMBER STETKAR: There is an analogy --
3 again, 30 years ago -- a couple of analogies. Number
4 one, in hardware failures, we are all comfortable in
5 2011 saying I have a valve, and the valve has four
6 failure modes that I am interested: it can fail to
7 open; it can fail to close; it can open spuriously;
8 or it can close spuriously.

9 Thirty years ago, when we were first
10 starting doing risk assessments, people wasted
11 an inordinate amount of money, time, resources,
12 because they did not understand the concept of
13 failure modes: failure to open; failure to close;
14 opened spuriously; closed spuriously.

15 They were concerned about the fact that
16 my God, you have to enumerate, identify, quantify
17 the entire universe of possible failure causes. How
18 come that valve didn't open?

19 Well, it could not open because there
20 was a little piece of grit on the valve stem. Well
21 how likely is it that you could get the piece of
22 grit and where might it come from? Is it blown in by
23 the wind? Was it left there when somebody
24 manufactured the thing? Did somebody put it in there
25 because of maintenance?

NEAL R. GROSS

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

1 An innumerable amount -- this is an
2 intractable problem. You can't determine how likely
3 it is that a valve will fail to open, because you
4 can't understand all of those causes, and even if
5 you could, you don't have any data for any of them.

6 So it's impossible. You can't do that.
7 Miraculously now, however, we understand four
8 failure modes. We understand that it's impossible to
9 identify explicitly all of the possible causes.

10 However because we understand these
11 failure modes and we understand what is a valve, we
12 can actually use operating experience to give us
13 evidence of the frequency at which these failure
14 modes occur, with some uncertainty.

15 And we don't care necessarily, at some
16 level, about the root causes, for many purposes. And
17 what I hear an awful lot, and what I read is that
18 there is not that distinct concept of failure modes
19 versus failure causes.

20 And I will admit that if you try to
21 enumerate, and develop any type of systematic
22 analysis that tries to identify every possible cause
23 of some unidentified failure mode in software, it
24 can't be done.

25 Or maybe you don't have to do that, if

NEAL R. GROSS

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

1 you are sort of creative and stand back from the
2 thing.

3 The other thing is that it's impossible
4 for people who are very, very familiar with very
5 detailed systems to step back and do that. People
6 who originally started to model reactor protection
7 systems for PRAs knew that they were so complicated
8 that you couldn't model them.

9 And they tried to model all of that
10 complexity and determined they couldn't model them,
11 but that's because they knew too much about the
12 system. They were detail-oriented engineers.

13 So as part of your research work and
14 part of your conclusions, what I'm looking for is
15 that concept of someone standing back from the
16 detail of the system, learning what we have learned
17 from you know, the hardware analogies, if there are
18 hardware analogies, about not focusing on the
19 specific little fine-structure causes, but thinking
20 about how they are manifested within a context of
21 what in the hardware side of things, we have learned
22 to call failure modes, and what the effects of those
23 failure modes are, which is, I think, closing the
24 loop back to where Dennis is coming is, what are
25 these things called FMEAs really doing in that

NEAL R. GROSS

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

1 context?

2 MR. BIRLA: They are not doing anything
3 on the software. So the system level high level that
4 he talked about turns out to be, even though the
5 papers were published as software FMEAs, they turn
6 out to be system FMEAs.

7 So what they are doing is looking at
8 system functions.

9 MEMBER STETKAR: And just black-boxing
10 the software --

11 MR. BIRLA: Yes.

12 MEMBER STETKAR: as something that --

13 MR. BIRLA: Yes. Yes.

14 MEMBER STETKAR: could fail in an
15 indeterminate way.

16 MEMBER SIEBER: I don't desire to
17 prolong this unnecessarily but your example of the
18 feedwater control system is an interesting one
19 because you can write all the equations that will
20 control a feedwater valve, you know, you are looking
21 at the difference between steam out and flow in, and
22 you are looking at level as a bias signal, but the
23 main control comes from the difference.

24 And so you can write software for that,
25 but it's the scaling factors that have to do with

NEAL R. GROSS

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

1 proportional band, rate, reset action that comes
2 first of all from somebody's analysis of the size of
3 the various vessels, the performance of the valves.

4 They come up with initial figures which
5 in 50 percent of the cases aren't exactly right.
6 That's what makes the valve hunt. That's what makes
7 the level always incorrect, you know, and so forth.

8 And in about an hour's time you could
9 work your way through the software, the scaling
10 manual and whether it's scaled right, do some tests
11 and you've got it.

12 Now, if you take that system and combine
13 it with 100 other systems and the cool design
14 engineer says boy, if you can control this vessel
15 that well, and they will set some high standard for
16 that, I can reduce the size of the vessel, okay, and
17 once he does that, that makes it very difficult for
18 the instrument guy to be able to keep the plant from
19 tripping, and I think the solution to the problem is
20 to have all your control systems that vary valves
21 and pumps and drives and things like that separate
22 from the ones that trip the plant.

23 And that I think is where the industry
24 has gone. That's where your regulatory impact has
25 gone, so that when you reach some dangerous

NEAL R. GROSS

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

1 condition, independent of the control system. The
2 plant will independently trip.

3 And so I think you can work your way
4 through that. You can either do a detailed analysis
5 or you can do a test program that basically tests
6 all these different circuits to make sure that they
7 function.

8 But you know, the instrument engineer's
9 job is not over the day the day the plant starts up.
10 I mean you are currently doing -- making adjustments
11 to all these factors as valves wear and therefore
12 the flow doesn't match the original curve, and so
13 forth, and so to me, I tend to fox all these things
14 off and then look for logical separations in the
15 design of it so that I can assure myself I am
16 protected and on the other hand, I can assure myself
17 to a high degree that everything will work in
18 harmony with one another and I think that that is
19 basically the structure of what it is you are doing
20 here. Is that correct or not correct?

21 MR. BIRLA: Okay, so there are some
22 interesting principles you mentioned about being
23 able to assure the separation --

24 MEMBER SIEBER: Right.

25 MR. BIRLA: -- and we will come to that

NEAL R. GROSS

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

1 later in my presentation.

2 MEMBER SIEBER: Yes, right. You could go
3 and examine software and find out that there's no
4 fault but the plant still tripped as far as your
5 scaling factors.

6 MR. BIRLA: So, I'd suggest we at least
7 let him have a few slides so that we can get what he
8 is already prepared to answer and then come back to
9 the discussion.

10 MEMBER STETKAR: One last question on
11 this one. The last bullet, the -- if we have
12 concluded that the system level software FMEA really
13 isn't a software FMEA, is that also true --

14 MR. BIRLA: No. No.

15 MEMBER STETKAR: for the detail level,
16 or that is a --

17 MR. BIRLA: That is.

18 MEMBER STETKAR: Are you going to talk
19 more about what that might be or not, how they do
20 it?

21 MR. BIRLA: How they attempted to do it
22 and what has happened.

23 MEMBER STETKAR: Okay.

24 MR. BIRLA: But we were not going to
25 talk about that, just report the conclusions of

NEAL R. GROSS

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

1 that. The conclusion basically was that when you try
2 to do that at a -- the elemental component, which is
3 the bottom-up, there are so many of them, and it
4 takes so much effort, that that's really not the
5 right way to approach the issue.

6 So the same gentleman who published that
7 paper 15 years ago, has backed off from that
8 position, and that sort of goes along with what Dr.
9 Stetkar said earlier about not looking at the faults
10 because when you get down to the elemental software
11 and the component, it is really the inherent fault
12 and that's -- this kind of analysis is just not a
13 productive path due to -- look for those, and the
14 expression that we coined looking for a needle in
15 the haystack

16 10:11:51 AM J Yes, you could apply all these things
17 and not find the failure.

18 MR. BIRLA: Right, right. So that turns
19 out to be a needle in a haystack type thing, and
20 that's not --

21 MEMBER STETKAR: Remember my story.
22 Thirty years ago, people concluded that there was no
23 way that you could enumerate all of the causes for a
24 valve failing to open. That was an impossible
25 project. You couldn't do it. You couldn't do it

NEAL R. GROSS

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

1 because everybody could hypothesize another cause
2 for which there was no evidence, for which the
3 amount of effort to analyze that cause was so
4 labor-intensive that it wasn't possible. You just
5 couldn't do that.

6 MR. BIRLA: Yes, so let's pick up the
7 discussion --

8 MEMBER STETKAR: And people knew that.

9 CHAIR BROWN: Just a quick summary
10 before we leave this, and I liked John's comment
11 about the system level effectively black-boxes the
12 software and says we are going to treat it as a
13 black box. Whatever is in there is going to happen.
14 You are really looking at this as -- it's become
15 component. Effectively it has become a software in a
16 hardware package and then everything else --

17 MEMBER STETKAR: It's an ill-defined or
18 undefined component because -- and undefined --
19 because all you say is it fails, and --

20 CHAIR BROWN: Right.

21 MEMBER STETKAR: without --

22 CHAIR BROWN: With the wrong output or
23 the wrong whatever.

24 MEMBER STETKAR: No, it fails.

25 MR. BIRLA: Yes, so to add to the

NEAL R. GROSS

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

1 summarization, Chairman Brown, I'd say that the
2 system level software FMEA is not a software FMEA.
3 It's a system FMEA.

4 MR. BETANCOURT: So now we are going to
5 be talking about some of the purpose of the report.
6 Basically we are trying to examine the role of FMEA
7 in regulatory assurance in complex-logic intensive
8 systems.

9 As part of this limited role we are not
10 looking at the FMEA combined with other reliability
11 or software methods and also we are excluding the
12 role of FMEA during the development process. That's
13 not what we envision for. We are only looking at the
14 regulatory assurance or the software evaluation, and
15 the safety assurance.

16 Now going back to your question about
17 why did we change the terminology of failure modes
18 and effects analysis to fault modes and effects
19 analysis, when we used the term failure modes and
20 effects analysis, we used that in the context of the
21 overall DI&C system but the corresponding concept
22 for software and other implementations of complex
23 logic is actually fault modes and effects analysis.

24 Logic does not fail in the traditional
25 sense of the realization of the hardware component,

NEAL R. GROSS

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

1 but the system actually could fail due to a latent
2 or a pre-existing logic fault which could actually
3 be triggered by some other combination of inputs and
4 some system-internal conditions.

5 In addition if you look at the
6 definition for failure that we actually cited in the
7 glossary, basically it's just that if you apply if
8 to an item that is able to perform its required
9 function to start with, so you have an item of
10 software that is able to perform its function
11 correctly from the start, it will continue to do so.
12 It will not break.

13 However if you have a software item that
14 was actually broken from the start --

15 CHAIR BROWN: What?

16 MR. BETANCOURT: An item on the
17 software, like a system --

18 CHAIR BROWN: You mean a line?

19 MR. BETANCOURT: Huh?

20 CHAIR BROWN: When you say an item of
21 the software?

22 MR. BIRLA: Item is the term in the
23 definition. IEC defines the term item as a generic
24 term. Think of it as a component. It could be
25 hardware component --

NEAL R. GROSS

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

1 CHAIR BROWN: Item, I-T-E-M?

2 MR. BIRLA: Item, I-T-E-M? They avoid to
3 use the word component because component has
4 undesirable side-connotations, so they use the term
5 item. It can be a software component. It can be a
6 hardware component. It could be a sub-system, part
7 of another system. It could be the whole system.

8 So, but when it comes to software,
9 that's what you were saying, that if it is broken to
10 start with, it was defective to start with, then it
11 had a fault to start with. It doesn't break, that
12 break event, its hardware does.

13 CHAIR BROWN: It was designed in. So
14 it's not really a failure.

15 MR. BETANCOURT: Exactly. That's why we
16 changed the the terminology of failure to fault.

17 CHAIR BROWN: I would have said it the
18 other way around because if it's designed in, it's
19 there all the time, therefore it's a failure,
20 whereas faults are typically momentary I mean at
21 least in my view.

22 MR. BIRLA: Faults need not be
23 momentary. They can be on-off type things. But
24 typically fault is a state, is an event.

25 MEMBER BLEY: It's interesting, you have

NEAL R. GROSS

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

1 defined them the way you intend to use them in your
2 -- in that report and I can understand that. I could
3 see we could bicker about that, but that's not --

4 CHAIR BROWN: All right, well, you can
5 go on. I just wanted to make sure I understood what
6 you were talking about, not to say that -- I'm not
7 sure I understand it, but go ahead. Still, I still
8 like the old terminology however.

9 MEMBER BLEY: That's a decent point,
10 since I was driven to the glossary, you have a
11 mistake in here as well, and the way you use it,
12 it's clear that it's not consistent with what most
13 people in human sciences are using now.

14 Usually now a mistake refers to
15 something you did that's not correct, but you did it
16 on purpose. It's what you wanted to do, and there
17 are other names for other errors that weren't
18 intentional and yours is a little more general, but
19 it's still --

20 CHAIR BROWN: It's whether something's
21 not consistent with the technical community at large
22 and your definitions but that's not to argue about
23 here.

24 MR. BIRLA: So we have studied this a
25 lot, about different uses of these terms in

NEAL R. GROSS

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

1 different places and resorted to the clarifications
2 provided by the fault-tolerance engineering
3 community.

4 MEMBER BLEY: Okay.

5 MR. BIRLA: This is just to avoid
6 ambiguity, confusion.

7 MEMBER BLEY: Well, you have defined
8 them the way you are using them.

9 MR. BETANCOURT: Okay, to continue, the
10 scope of the study was actually going from software
11 to complex logic, and the reason is that we wanted
12 to enclose other implementations of logic such as
13 FPGAs, PLDs and ASCIs.

14 And as I talked before, we narrowed the
15 role to regulatory assurance because we didn't want
16 to include the role of FMEA in the development
17 process. We just wanted to investigate what was the
18 role of software evaluation and safety assurance.

19 CHAIR BROWN: This is your basis for
20 going from software to complex logic?

21 MR. BETANCOURT: Yes.

22 CHAIR BROWN: And you say it's so you
23 can cover other logic devices other than necessarily
24 what I would call microprocessors or software
25 control devices.

NEAL R. GROSS

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

1 MR. BETANCOURT: When we use the
2 terminology complex logic in this document, we are
3 talking about a product of a development process
4 that is either in the form of software in a
5 microprocessors-based system, or of implementation
6 of programmable logic so such FPGAs and CPLDs.
7 That's what we have referred to as complex logic
8 over here.

9 CHAIR BROWN: Yes, but FPGAs are
10 fundamentally not software-type devices, I mean they
11 are -- yes, you program them with software, but they
12 are fundamentally hardware systems -- they are
13 combinational logic systems once you program them
14 with your software tool.

15 MR. BIRLA: So once you have programmed
16 them --

17 CHAIR BROWN: With your software tool.
18 In operation they are not software-driven devices.
19 They are effectively an analog, a combinational
20 logic system that has been designed and hard-wired
21 via software to perform a certain logic or
22 algorithm-type function.

23 I hate lumping -- I just -- I got a
24 little problem with lumping those all in under the
25 same --

NEAL R. GROSS

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

1 MR. BIRLA: The intent is not to lump.
2 The intent is to say that a lot of these findings
3 are applicable to implementations of logic other
4 than software.

5 In other words, these findings are not
6 limited to just software. So in programming that
7 FPGA, if you have the same issues in the programs,
8 complexity, non-separation of the design functions,
9 you are going to run into the same issues.

10 So the applicability of these findings
11 extends beyond software. That's the message we are
12 trying to convey, not lumping the case where the
13 real-time system and execution is executing software
14 versus not, because I do agree with your implication
15 there that there is a difference and there is an
16 advantage in the --

17 CHAIR BROWN: Well, once programmed, the
18 FPGA is fundamentally a deterministic system for the
19 most part. It's not similar to the software-driven,
20 clot-driven systems. That's all. Unless you have a -
21 - in the microprocess, if you have got a fixed time
22 frame where everything gets done and there are no
23 interferences, then you can get there. But I got the
24 picture. You don't have to --

25 MR. BIRLA: Let me just make one slight

NEAL R. GROSS

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

1 remark on what you said. It depends on how you are
2 using that FPGA. People are implementing
3 microprocessors on FPGAs now. So you can create the
4 same kinds of issues, almost the same kinds of
5 issues, even with FPGAs. I don't think you intended
6 to exclude that. What you were trying to point out
7 was that there are some advantages in the technology
8 that we should maintain a distinct awareness of.

9 CHAIR BROWN: I don't like -- yes, I
10 just -- I don't want people to understand the -- the
11 two technologies are distinctly different and they
12 are executed distinctly differently. Doesn't mean
13 you can't perform a more complex function than they
14 typically are with FPGAs or those types of
15 programmable devices, software-controlled devices,
16 not meant to say that.

17 But they -- it's just more difficult.
18 You have got more stuff that you have got to stick
19 in there in order to execute though the equivalent
20 type -- that's why the microprocesses are attractive
21 in many circumstances. Software allows you to do a
22 lot of stuff in a more complex manner than you can
23 by just stacking up more logic gates.

24 Anyway, I got your point.

25 MR. BIRLA: Thank you.

1 MR. BETANCOURT: Anything else before I
2 move along?

3 (No response)

4 So I just want to tell a little bit
5 about the progress of the development process about
6 this NUREG-International Agreement Report. Basically
7 when you have a NUREG-International Agreement Report
8 it serves like a repository of unclassified
9 information received by another foreign government
10 and the NRC actually reports that.

11 We actually -- the foreign government or
12 the organization submits unclassified safety
13 information to the NRC for publication and it's only
14 on the technical basis.

15 As part of this international agreement,
16 we actually did not develop any regulatory guidance
17 criteria. It was only on the technical content.

18 We actually started just doing in March,
19 2010 as part of the bilateral agreement. Milton is
20 going to be talking more about that in his
21 presentation. However there was some interest that
22 it dates back to 2008.

23 Under this bilateral agreement we
24 actually started in March 2010 and we extrapolated
25 first with some teleconferences between the IRSN

NEAL R. GROSS

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

1 researchers which you can see over here is Pascal
2 Regnier and Jean Gassino.

3 So I wanted to talk a little bit about
4 the real-time I&C group on IRSN. Basically they
5 perform both safety assessment reviews and also they
6 perform research at the same time.

7 And the effort is actually trying to
8 allocate the engineer to do 40 percent of research
9 and 60 percent on safety assessment reviews, where
10 actually that depends on the allocation of the
11 review at the time.

12 They actually perform one review at a
13 time so they can actually have call the resources
14 applied to that. Pascal Regnier is actually the
15 deputy team lead for this group and he actually as a
16 foreign assignee to the NRC back in 2000.

17 He was over here for six months. He
18 worked at the office of NRR and also worked at the
19 Office of Research.

20 Jean Gassino is actually a senior
21 engineer working under Pascal, and he actually has
22 been involved in the EPR safety assessment reviews
23 and he is also the lead engineer for the IEC
24 standard of FPGAs.

25 We also perform, as part of the

NEAL R. GROSS

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

1 agreement report, a literature review that we talked
2 about earlier. We wanted to go a little bit more
3 outside the scope to include what others have been
4 doing on software FMEA.

5 The research method, basically this is
6 an analytical method that we actually employed over
7 here. The first thing that we did that I am going to
8 be talking about on the next slide is basically we
9 characterized the differences between the
10 traditional hardwired systems and the complex logic-
11 intensive systems and we actually identified some of
12 the technological trends that drive these
13 differences.

14 Then given those fundamental
15 differences, we actually discuss some of the issues
16 and limitations of applying this then linked to
17 complex logic.

18 Then we also took some examples from
19 experience in order to identify some real-life cases
20 of analytical conclusions when we draw the
21 conclusions and we actually have some open questions
22 that went outside the scope of what we identify in
23 this project.

24 Now I would like to talk briefly about
25 how we characterized the differences between these

NEAL R. GROSS

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

1 two systems. When you have hardwired systems that
2 were compromised -- where this I&C system were only
3 compromised by hardware devices, most of the faults
4 actually resulted from physical deterioration, by
5 wear and tear over the period of time, which means
6 that they have to necessarily occur during operation
7 unless the component or the system actually is being
8 replaced from service.

9 At the time, since the systems were so
10 simple, latent logic faults and systemic causes such
11 as engineering mistakes were not the significant
12 issue of the day.

13 However, but the focus was actually on
14 the hardware components compromising the system and
15 that was the focus of the analysis at that time.

16 In contrast when you look at these
17 complex logic-intensive systems, these faults can
18 actually be originated by -- in any part of the
19 development cycle and this actually may cause binary
20 mistakes.

21 Some of these faults may actually occur
22 during the design phase such as like a missing
23 statement. Others may -- can actually occur during
24 the requirements phase when the requirements are
25 missing or ambiguous. We have found that most of

NEAL R. GROSS

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

1 these problems are actually found over here.

2 On the traditional hardwired system you
3 have a limited number of fault modes as Member
4 Stetkar was talking about earlier, and this actually
5 was very well understood. Manufacturers often give
6 the failure modes and also you can actually -- it
7 was easy to understand these systems.

8 When you have these complex logic
9 systems, as you recall on the report, the potential
10 fault space is very, very high. It's not very well
11 understood and even in the high quality process that
12 we identify in the definition of complex logic in
13 the glossary, this actual number of faults is
14 actually quite small.

15 If you look on the traditional hardwired
16 devices, these propagation paths unfortunately to
17 physical and they were basically derived on the
18 printed circuits.

19 In compare, on the complex logic, there
20 is an unlimited number of propagation paths that are
21 not well understood and we can actually have this
22 dependent on dependent paths.

23 Finally, on the hardwired systems, these
24 faults can occur randomly although the causes are
25 not random. These propagation paths actually are

NEAL R. GROSS

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

1 basically known -- oh sorry, wrong talking point
2 over here -- good design and maintenance practices
3 may actually extend the interval between random
4 occurrences. In general, it was accepted that the
5 likelihood it cannot be reduced to zero.

6 If you look on the complex logic design
7 practices for safety systems, they can actually
8 follow principles that are intended to prevent these
9 faults from occurring.

10 A combination of verification techniques
11 that we identify in the glossary also are used to
12 discover and remove faults or conditions that could
13 actually lead to the failure of the safety function.

14 And only a limited number of faults is
15 actually present in the complex logic otherwise it
16 will be corrected.

17 MR. BIRLA: I want to elaborate on one
18 point. The propagation path, particularly in
19 software and that's an important distinction between
20 the implementation on something like an FPGA and in
21 software; propagation paths do not follow the
22 traditional pre-design propagation paths as in
23 hardware. In traditional hardware, they will follow
24 the path of the wire.

25 Where as in software, the design says

NEAL R. GROSS

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

1 that until you have separation, in actuality you may
2 not. This is an issue and that design separation
3 cannot be assured because of that issue. We will
4 come back to that in my presentation a little later.

5 MEMBER SIEBER: Before you switch that,
6 I see your finger on the button there. The very last
7 statement, engineering process can eliminate all
8 known faults, otherwise they would be corrected.

9 I contend that all the faults that you
10 would get out of an analog or hardwired system, will
11 still be there, you know, for example dirt in a
12 valve operator and things wearing out and
13 transmitters that don't transmit exactly the right
14 signal for their entire lifetime.

15 All those go from the old hardwired,
16 analog-type system to the new systems and what you
17 do is you add on another layer of failure modes
18 which comes from the software itself.

19 So, and perhaps the PRA specialist can
20 tell me whether the failure of a comparable system,
21 not one with a lot of built-in protections, but a
22 comparable software-driven system, has a higher
23 failure rate than a hardwired, analog system. Do we
24 have -- is there any such data or do we know that?

25 MEMBER BLEY: Not yet.

NEAL R. GROSS

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

1 MEMBER STETKAR: We don't know that.

2 MEMBER BLEY: But you know, the stuff
3 John talked about earlier really applies to some of
4 the things you are saying here. Just a couple of
5 examples.

6 Most faults are caused by physical
7 degradation. Well yes, but they are also, you know,
8 the mechanism for physical degradation is set up
9 often by the design and errors and it's in column
10 errors in the design; stress risers put in places
11 you didn't expect they were being put; a whole bunch
12 of things.

13 Limited number of fault modes -- that's
14 the thing John was talking about -- well there
15 really aren't. If you go into hardware systems, the
16 causes, they go on forever.

17 But there, we have managed to group the
18 things into functional fault modes, of which there
19 is a limited number. Sometimes you get surprised and
20 you learn a new one.

21 We haven't quite done that yet, over in
22 these systems that include the software, although
23 there are some folks around the world who are making
24 a start at that.

25 So I think you over-generalized or over-

NEAL R. GROSS

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

1 emphasized some things that don't quite work, but I
2 feel somebody behind me.

3 (Laughter)

4 MR. KURITZKY: This is Alan Kuritzky at
5 the Office of Research. Just to get to Mr. Sieber's
6 question, there was, as you mentioned, a couple of
7 weeks ago there was a study done by the Koreans
8 where they compared an analog protection system,
9 reactor protection system, with a digital.

10 And as I think Louis Chu mentioned the
11 last time, they showed that the analog system had a
12 lower failure probability than the digital. I took a
13 look at their results. I think before that report
14 and you may have seen it already, but the number --
15 they are looking in decimal places that made no
16 sense for a study of that type.

17 But they seem to be comparable. I think
18 the important thing is, just like you mentioned
19 before, when you go to a digital system, you are
20 carrying over those failure modes that you have in
21 the analog system for the hardware part of the
22 digital system, and now you are also adding in the
23 software part.

24 Now whether the failure probabilities of
25 all the hardware pieces of a digital system, how

NEAL R. GROSS

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

1 they compare to the failure probabilities of a
2 hardware analog system I don't know.

3 One thing you do have in a digital
4 system, is you have the software enabling you to
5 identify and correct for some hardware failures that
6 you don't have necessarily with the analog system,
7 but then you have other potential failures from the
8 software itself.

9 So there's no real evidence to say one
10 is necessarily better than the other.

11 MEMBER SIEBER: Well, the saving grace
12 is the software is so versatile that you can detect
13 otherwise available failure modes and prevent them.

14 MR. KURITZKY: Right.

15 MEMBER SIEBER: And that's something you
16 don't have hardwired analog systems and in -- so I
17 was curious as to whether the overall failures were
18 higher or lower --

19 MR. BIRLA: Let me address that. You
20 mentioned that everything that happened in the old
21 hardware world carries over, if those components
22 carry over.

23 MEMBER SIEBER: Right.

24 MR. BIRLA: But sometimes, that same
25 function that was implemented in an older technology

NEAL R. GROSS

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

1 component that had moving parts, can now be
2 implemented without those moving parts.

3 When that happens, you have reduced a
4 source of failures. So a lot of the transition has
5 happened that -- we'll take the example of
6 electromagnetic fillings. They used to have moving
7 parts. It was inevitable that eventually the contact
8 is going to wear or even fall apart.

9 And when you replace that with
10 electronic technology and logic with software, you
11 remove those moving parts and therefore those causes
12 of failure of those modes of failure also.

13 MEMBER SIEBER: Well, I was comparing
14 hardwired versus solid-state control, assuming that
15 the actual sensing and motive elements would remain
16 essentially similar.

17 But you are right, the old technology
18 did have a fairly high failure rate.

19 MR. BIRLA: So I'll give you another
20 example, on the sensing side.

21 MEMBER SIEBER: Right.

22 MR. BIRLA: The sensing of a neutron
23 flux, neutron flux detectors. So the old technology
24 had analog electronics.

25 MEMBER SIEBER: Right.

NEAL R. GROSS

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

1 MR. BIRLA: And the filtering was also
2 behind the analog, so the result was more analog
3 components than in the FPGA implementation of today.

4 MEMBER SIEBER: Right.

5 MR. BIRLA: And the claim is that with
6 the newer technology, which is using logic, and an
7 electronic base, the expectation of failures is
8 less.

9 MEMBER SIEBER: Okay.

10 MR. BIRLA: The expected value is less.

11 MEMBER SIEBER: And the response time is
12 better?

13 MR. BIRLA: Well, again now, you touch
14 upon a touchy issue here. Response time -- the
15 failures that have occurred have really occurred
16 because the response time is faster, unexpectedly
17 faster.

18 So yes, new issues did arise, but
19 industry is on the learning curve and --

20 MEMBER SIEBER: In retrospect, they
21 aren't comparable, the old systems to the new. It's
22 just a different way of doing things, and you know,
23 if you work hard enough at anything you will get the
24 error rate down to some minimum.

25 MR. BIRLA: Right, and the reason for

NEAL R. GROSS

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

1 using the word complex there was that you can make
2 even a totally hardware-based system have the same
3 kinds of issues if you start going up the complexity
4 curve.

5 And the point he was trying to make in
6 that --

7 CHAIR BROWN: But typically that
8 occurred when you tried to increase the
9 functionality. When you increased the range and the
10 broadness of the functionality in the hardware-based
11 systems they are much more difficult to implement
12 because they are more step-type corrective actions
13 that you can take.

14 Whereas with the software-based systems
15 you can expand the functionality without affecting
16 your response time as significantly -- that's based
17 on very personal experience-- and you can do a lot
18 of things with the system that you cannot do just
19 because you may have 22 setpoints or breakpoints
20 that you need to go through and if you accomplish
21 that with the analog systems, you are dying trying
22 to keep them straight, whereas with the software you
23 can.

24 I'd like to -- some of us get much older
25 than we should be at this stage and while we are not

NEAL R. GROSS

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

1 through with this I'd like to go ahead and take our
2 break now and come back before we go into the
3 extension of the FMEAs and the complex logic, if
4 that's a reasonable breakpoint.

5 I was going to take a 15-minute --

6 MEMBER BLEY: Even if it's not I think -
7 -

8 CHAIR BROWN: Even if it's not we are
9 going to take it. Put it that way, all right? Too
10 much information here. So we'll adjourn here for a
11 few minutes, or pause, whatever the appropriate term
12 is and we will reconvene -- recess -- thank you --
13 until 10:55.

14 (Whereupon the above-entitled
15 matter went off the record at
16 10:38 a.m. and back on the
17 record at 10:57 a.m.)

18 CHAIR BROWN: We are un-recessed. Got to
19 have a little humor in this somewhere. We also, in
20 order to try to get to Sushil's, we need to try to
21 exercise a little bit of discipline. I am not asking
22 for any relevant questions to be sidelined, but we
23 do need to keep things moving a little bit and I
24 admit I am as much at fault as anybody and I will
25 try.

1 So you can proceed on.

2 MR. BIRLA: At least you haven't failed.
3 You only faulted.

4 CHAIR BROWN: Yes. And I am probably a
5 continuous.

6 (Laughter)

7 MR. BIRLA: It's a state of mind.

8 CHAIR BROWN: Yes.

9 MR. BIRLA: Okay.

10 MR. BETANCOURT: I would like to go as
11 quick as possible on this slide so we can actually
12 catch some time for his presentation.

13 CHAIR BROWN: Okay.

14 MR. BETANCOURT: So now we are going to
15 be talking about some of the issues and limitations
16 as to the standard FMEA to complex logic, and in
17 order to evaluate the applicability of FMEA to
18 complex logic, you have -- you remember -- you
19 recall the example that we gave of Section 2.24
20 about the illustration about the -- on the enormity
21 of the potential fault space, what we are trying to
22 show over here that FMEA is not feasible, actually
23 finding the actual fault space, the faults in this
24 enormous space over here, this actually number of
25 potential faults cannot be bounded in general.

NEAL R. GROSS

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

1 Finding this fault through FMEA is
2 basically finding -- akin to searching for a needle
3 in a haystack, basically the required effort and the
4 duration for doing so we will be too large in order
5 to be feasible.

6 I think the system fail basically for
7 the largest because it has some fault from the time
8 of introduction and it remained latent until some
9 triggering condition some other combination of the
10 inputs, the state of the environment, the state of
11 the DI&C and the state of the faulty logic.

12 Also when we talk about the propagation
13 of the faults across the units, the NUREG argues
14 that basically since this potential fault space is
15 so huge, the set of fault mods cannot actually be
16 enumerated, the FMEA effort and duration will be so
17 large that it's not feasible.

18 FMEA actually doesn't look at the
19 semantic of the software and the computing
20 architecture, and these dependencies may not be easy
21 to find. That's why we are saying that these
22 propagation of the faults are very large and not
23 very well understood.

24 On the Appendix B that we have actually
25 in the report that is basically we are trying to

NEAL R. GROSS

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

1 identify some of the sources of uncertainty. When
2 this complex logic is implemented in software, it
3 actually increases this potential fault space, in
4 other words it basically say decrease in the value
5 of FMEA applied over here and Sushil will be talking
6 more about that in his presentation more on the
7 sources of these uncertainties.

8 And these propagation forces are
9 actually even unpredictable in software even in
10 known, hidden dependencies, where you have the known
11 dependency software can actually propagate
12 unpredictably, on functionally dependent paths, and
13 that depends on the behavior of the units and the
14 entire state history.

15 When we are talking about hidden
16 dependencies, these are functionally chain that
17 doesn't reveal the propagation paths through the
18 software and the system basically is not visible for
19 the functional requirements.

20 Any questions on that before I move
21 along?

22 (No response.)

23 In order for the technique to be
24 workable, it should be able to identify a small,
25 feasible -- a small number of fault modes like

NEAL R. GROSS

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

1 Member Stetkar was saying.

2 What we are going to discuss over here
3 is basically a compact set of fault modes that are
4 from the effect perspective at the system function
5 level in which it is even difficult to identify the
6 effects leading to a conservative evaluation.

7 The manner in which any module in the
8 functional path could malfunction basically its
9 fault modes is basically an interest understanding
10 the effect of that fault mode to the safety
11 function.

12 The first three bullets ready to perform
13 the module in time that will be in the --

14 CHAIR BROWN: These are software modules
15 you are talking about in this case, is that correct?

16 MR. BETANCOURT: Yes.

17 CHAIR BROWN: Okay. We are setting aside
18 the hardware parts of that.

19 MR. BETANCOURT: That's correct. We have
20 -- for the first three ones, basically the time
21 domain, the value domain and the performance of an
22 unwanted function by the module is difficult to
23 analyze because we have to take into consideration
24 the semantic of the software and the computing
25 architecture in order to predict the impact of each

NEAL R. GROSS

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

1 possible time and value error of the module.

2 We have shown over here two examples
3 that we actually found from real life, the AT&T 4ESS
4 toll switching system, basically that it was a
5 software fault that escaped from detection from the
6 AT&T tests, and it was actually because of a
7 misplaced break that is the FMEA actually --

8 CHAIR BROWN: A misplaced --

9 MR. BETANCOURT: Break. A statement
10 break.

1 CHAIR BROWN: A software break?

2 MR. BETANCOURT: Yes.

3 CHAIR BROWN: Oh okay, all right. I got
4 it.

5 MR. BETANCOURT: Exactly. Sorry about
6 that. And the second is basically Ariane 5 launcher,
7 I think most of you members are familiar with this
8 event that is actually there was a software
9 specification design defect on the system.

10 The last one then the interference and
11 unexpected coupling with another module is even --
12 is very common in software, a fault within a given
13 module may actually aggressively impact on another
14 module.

15 Even those modules that do not interact

NEAL R. GROSS

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

1 from the functional point of view as you recall in
2 my previous slide that is not visible in the
3 functional requirements.

4 MR. BIRLA: So I would like to connect
5 that with what Dr. Stetkar was asking for earlier.
6 How come, in the software world we haven't thought
7 in terms of a compact set at the function level, so
8 this is that complex set.

9 If you recall, in 2009, May was it -- is
10 Alan still here -- BNL held a workshop on this
11 subject and the experts that they collected
12 basically came up with this set of failure modes due
13 to software.

14 And at the system level you can it's the
15 same thing. So you have a set of failure modes. What
16 do you do with that? How do you risk-inform a
17 regulatory review process with this?

18 Dr. Stetkar mentioned that in the case
19 of hardware components to operating experience, we
20 could track and over time determine for each failure
21 mode what was the likelihood. There's no such thing
22 on the software side.

23 So the utility of this for this
24 conforming is not there.

25 MEMBER BLEY: And why is there no such

NEAL R. GROSS

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

1 think on the software side?

2 MR. BIRLA: Well first of all, here is a
3 set of failure modes. Now, your question is why is
4 there no such thing, meaning operating experience --

5 MEMBER BLEY: Yes.

6 MR. BIRLA: that you can use to estimate
7 likelihood of occurrence?

8 MEMBER BLEY: Yes.

9 MR. BIRLA: Okay. Because each one of
10 these can --

11 CHAIR BROWN: You are talking about the
12 AT&T and the Ariane 5 failures? Are you talking
13 about those specific failures?

14 MR. BIRLA: In general.

15 CHAIR BROWN: Okay.

16 MR. BETANCOURT: All of them.

17 CHAIR BROWN: Okay.

18 MR. BIRLA: Yes, the whole set. There
19 isn't enough operating experience and there is no
20 reasonable expectation that we will ever accumulate
21 that kind of operating experience.

22 If you had the same software component
23 working in a million vehicles, perhaps you could.
24 Even there it's questionable because the inputs, as
25 you mentioned earlier, the inputs base is so large

NEAL R. GROSS

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

1 that unless the same condition repeats enough times
2 to give you statistically significant values, you
3 can't come up with a credible likelihood number with
4 any kind of confidence.

5 MEMBER BLEY: But the point John was
6 trying to make earlier was once we identified
7 functional failure modes for hardware at a higher
8 level, not down at this little level where there's
9 no tracking it, and agreed that that's what we were
10 looking for, people began to collect that data from
11 many different systems, some of which have different
12 things in their design, but still, these manage to
13 be fairly consistent.

14 Unless you have found classes of
15 failures modes that are general and applicable you
16 will never collect the data, but if you've done that
17 then you can begin to collect the data.

18 Now you won't have it for several years
19 but you will begin to gather it. I think our
20 complaint has been that nobody has systematically
21 looked for it and your two papers essentially say
22 there is no hope of ever doing that.

23 And from some work I see elsewhere I'm
24 not sure I agree with you.

25 MR. BIRLA: Well, if you have a

NEAL R. GROSS

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

1 reference, I would like to have that reference. We
2 will review it, analyze it and report to you the
3 next time.

4 MEMBER BLEY: Sure, I will and I'll get
5 some more but I have one with me.

6 MEMBER STETKAR: Let me go back to my
7 valve failure mode. This is -- sorry -- no, but
8 there's a lot of analogy because 30 years ago people
9 were developing extremely complex concepts of data
10 systems, for example about, while it's important, we
11 might need data on a half-inch, motor-operated globe
12 valve. We might need data on a one-inch motor-
13 operated globe or we are up to a 12-inch motor-
14 operated globe valve, and then well, it might be a
15 double-disc gate valve, or a single-disc gate valve
16 and what about the difference in designs in the
17 motor?

18 So people were saying well, obviously we
19 need to collect data and my God there's no data
20 available in this so there's no way that we can
21 develop this data.

22 When people started to look at failure
23 modes and say, well, maybe it doesn't make too much
24 difference, the size of the valve or whether it's a
25 globe valve or a gate valve, because the things

NEAL R. GROSS

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

1 driving what makes a valve fail to open really don't
2 depend on all of that fine structure detail, people
3 suddenly started to realize well, my God we do have
4 relevant operating experience -- some less, you
5 know, you look at a valve spuriously opening, maybe
6 that doesn't happen very frequently, but it does
7 happen, and you have uncertainty and you can look at
8 operating experience and use that experience to
9 inform it, but until you've defined, as Dennis said,
10 that context, you're right, you just throw your
11 hands up on the air and say well, there's so many
12 things that I need to collect data for that it's
13 impossible that I'll ever have enough statistically
14 relevant data for each one of those things, so I
15 can't do any of it.

16 MR. BIRLA: Okay so here's that compact
17 set --

18 MEMBER STETKAR: A set.

19 MR. BIRLA: and let us pick up this
20 discussion in the operating experience research
21 segment.

22 MR. BETANCOURT: So we already talked
23 about this before on the literature review of
24 software FMEA --

25 CHAIR BROWN: Go back. I want to make

NEAL R. GROSS

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

1 one observation on the -- this is another experience
2 one -- but in terms of how you'll -- the software
3 issue and John just reminded me of that when he was
4 talking.

5 If you go back, one of the early
6 uneasiness with the use of microprocessor systems,
7 and this is 30 years plus, I guess, is the old
8 Therac irradiation medical device machine, where
9 people died because they thought they had keystroked
10 in the proper time for which they were supposed to
11 be irradiated and it turns out instead of three
12 microseconds, they irradiated them for 10 minutes
13 and then they had some unused.

1 Turned out it was -- and you couldn't --
2 they had a terrible time finding out what the cause
3 was, but it was effectively keystroke inputs by the
4 operators, and a fast operator would put in all this
5 information by keystroke and all of a sudden the
6 machine got confused, didn't know the proper -- in
7 other words it performed an unwanted function -- the
8 module, and so you actually had to slow it down.

9 So you know, you key it in, no matter
10 how fast they got put in, you couldn't put it in any
11 faster than would allow the machine to operate
12 properly.

1 That -- now we've got touchscreens. When
2 I was first designing ours, we had switches.
3 Everything you did, you know, pushbutton switches,
4 turn the switches, you couldn't have done those too
5 fast if you wanted to.

6 But now we have touchscreens which
7 people can go input and move and select what they
8 want to be done. That information has to go in. If
9 you do it too fast, could that cause a problem? I
10 don't know but it gets back to the point of a cause
11 that -- John's point again -- is do we really care,
12 how should we do it on the system level basis so
13 those things don't affect the overall performance of
14 a combination of channels or whatever it is.

15 It's just -- these particular examples
16 are valid examples of modes that you have to deal
17 with, but they can manifest themselves in a lot of
18 different ways, which we probably haven't
19 anticipated.

20 So that is just a five-minute lecture --
21 no, a two and a half minute lecture on -- or
22 discussion. But I just wanted to point that as just
23 a simple thing of how you manipulate and how we use
24 the new technology in terms of touch -- can those
25 affect what we are getting out of this stuff? Don't

NEAL R. GROSS

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

1 know. Anyway, that was it. Proceed. Thank you for
2 letting me blather on here.

3 MR. BETANCOURT: Okay, we already talked
4 about this before in the literature review of
5 software FMEA, that we actually look on 28
6 publications the literature review and analyze.

7 But we also did some interviews via
8 teleconferences and these are some of the people
9 that we actually interviewed via email or by
10 teleconferences.

11 The first one is Herbert Hecht. Now he's
12 working on SoHaR, software hardware reliability.
13 Basically they are implementing a software FMEA that
14 is built on a UML model and is basically -- it's
15 derived from the design, and requirements
16 documentation, and they are actually applying that
17 at the object level, which is at the component
18 level.

19 The other person that we have actually
20 interviewed, but this is via email exchange, it's
21 Robyn Lutz. She's actually a professor of computer
22 science at Iowa State University and she is also a
23 senior engineer at JPL.

24 But she has actually been doing -- she
25 has been using software FMEA coupled with software

NEAL R. GROSS

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

1 FTA for requirement analysis. She is doing first a
2 forward then a backward of the requirements.

3 She also has said that you can use the
4 other way around the FTA first and then an FMEA
5 later, but it has to be done on the design phase.
6 However there hasn't been any conclusion which one
7 is better at each phase.

8 The last one if you recall my previous
9 slides that I talked about two types of software
10 FMEA, it's because of Pete Goddard over here. Pete
11 Goddard actually works at Hughes Aircraft. He was
12 actually one of the ones who actually first
13 implemented software FMEA.

14 What we learned over there is basically
15 that there are two types of software FMEA, at the
16 system level and the detail level.

17 Some of the preliminary results, the
18 contribution of FMEA to develop the assurance is
19 basically marginal. Basically the required effort it
20 would be too much and the duration would be too
21 large to be feasible.

22 We need to look at other improvements in
23 order to ensure techniques that will be under
24 development assurance that we actually identify in
25 the glossary, and that will be also looking at the

NEAL R. GROSS

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

1 system internal hazard analysis including
2 instruments, sensors and actuators.

3 We need to clarify the appropriate role
4 of FMEA in the safety analysis of complex logic and
5 we are going to be actually discussing that on the
6 second RIL, which we are going to be publishing
7 around six months from now.

8 And finally, we don't see any related
9 changes to the digital I&C-ISG-06. This actually
10 does not propose the use of FMEA to be applied to
11 software.

12 CHAIR BROWN: Say that again. ISG-06 is
13 the licensing?

14 MR. BETANCOURT: That is correct, the
15 licensing process.

16 MR. BIRLA: So if you recall, the ACRS
17 wrote a letter --

18 CHAIR BROWN: I wrote it.

19 MR. BIRLA: With four recommendations,
20 recommendation number four is what he is referring
21 to, that our findings to date do not warrant any
22 change to ISG-06.

23 MR. BETANCOURT: Finally, on the path
24 forward we are planning to continue learning from
25 the other contrarian viewpoints. We are continually

NEAL R. GROSS

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

1 sending teleconferences with some of the experts
2 that we identify in the report just like Pete
3 Goddard, Herbert Hecht and Robyn Lutz.

4 The other path forward that we are
5 trying to do is also the second Research Information
6 Letter that is going to be built on the findings of
7 RIL-1001 in this NUREG.

8 Basically what we are trying to do is to
9 actually close the SRM and also close the
10 recommendation for all the ACRS. We are going to be
11 discussing some discussion related to the role of
12 FMEA in safety analysis.

13 We are going to be also discuss some of
14 the software defect classification that we have
15 actually identified in the NRC expert clinic and
16 also talking to these experts.

17 Finally, some open questions that I
18 should relate to this study but we couldn't answer
19 in this study because they were outside of the
20 scope.

21 System and software design as described
22 in the architecture, they don't convey all the fault
23 propagation paths. That's basically the discussion
24 over here, under what comparable conditions can
25 design documentation be deemed dependable for use in

NEAL R. GROSS

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

1 safety assurance.

2 Many other faults and propagation paths
3 cannot even be identified through an examination of
4 the design documentation because of these two well-
5 known causes -- incomplete, inconsistent, ambiguous
6 requirements, and inadequate, unverifiable
7 architectural constraints.

8 Therefore performing, analyzing that
9 information for system failure modes, or software
10 failure modes, is -- it can be misleading. So
11 further investigations are -- we are going to be
12 addressing that as part of the second RIL -- is
13 going to be addressing some of these questions and
14 we also -- we are going to be talking to some of the
15 experts on the issues.

16 MR. BIRLA: So, I would like to add to
17 this, in addition to addressing the SRM from three
18 years ago and the fourth recommendation from you in
19 the ACRS letter, we are also trying to derive some
20 benefit to the licensing offices from this work.

21 So keep that in mind in why we are
22 getting into a little bit more detail that we
23 believe would be useful in the licensing review than
24 what was necessary to address the SRM or your
25 recommendation.

NEAL R. GROSS

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

1 CHAIR BROWN: Did you explicitly write -
2 - you have said there were no related changes to the
3 ISG-06 based on our -- we made a recommendation or a
4 comment and you all evaluated that.

5 Was there ever a formal write-back on
6 that in terms of the response? My mind is drawing a
7 blank, that's all.

8 MEMBER BLEY: Well, we must have had a
9 response from the --

10 CHAIR BROWN: I'm sure we had a response
11 but --

12 MR. BIRLA: The response letter from --

13 CHAIR BROWN: You are going to use this
14 as saying we don't need to do anything, right? This
15 meeting.

16 MR. BIRLA: No no. The response letter
17 to the ACRS letter was that Research will
18 investigate this and there we said we are going to
19 investigate the fault modes.

20 CHAIR BROWN: Okay.

21 MR. BIRLA: And this is an interim
22 status report on where we are.

23 CHAIR BROWN: Okay, thank you.

24 MR. BIRLA: The second RIL will be the
25 closure.

NEAL R. GROSS

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

1 MEMBER STETKAR: But -- if, without
2 seeing the second, what's the schedule on the second
3 RIL?

4 MR. BIRLA: Six months.

5 MEMBER STETKAR: Okay. If that follows
6 what we are hearing today though, it sounds as if
7 the conclusion is that it's intractable to try to
8 identify failure modes and therefore the conclusion
9 to the ACRS recommendation and to the SRM is that we
10 can't do it. Is that fair?

11 MR. BIRLA: Well, we will report
12 whatever we find and there are many perspectives, as
13 you mentioned, on this complex set of failure modes.
14 We showed one, we are still looking. If somebody's
15 got another we will report that.

16 Many people say well, because one
17 concept is false and a different classification, we
18 will report that too.

19 But we are going to organize that
20 information in a way that has some value for the
21 licensing offices. If you have any specific
22 references that you want us to review, or specific
23 cases where people have applied it, that we can
24 learn from, please let us know and we will interview
25 those parties and review those papers, and we will

NEAL R. GROSS

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

1 make those a part of the second RIL.

2 MEMBER BLEY: I am trying to remember, I
3 am a little vague on this, but long ago there was a
4 Brookhaven report that had pulled out an appendix
5 that began -- they began looking at failure modes --

6 There. Is that included -- I didn't see
7 it referenced here in any way.

8 MR. BETANCOURT: There is no reference
9 over here but we are going to be talking about that
10 in the second RIL.

11 MR. BIRLA: Yes, so, mind you, this is
12 the work with IRSN, with a little bit of literature
13 review added by Luis. The second RIL is the more
14 comprehensive, so we will catch that Brookhaven
15 Appendix C, and later work from Brookhaven.

16 MEMBER BLEY: Okay, good.

17 CHAIR BROWN: Frankly I'm -- if you
18 happen to have it, I'm somewhat of a skeptic of how
19 to apply these and make them useful but yet we need
20 to really have it thoroughly looked at. We don't
21 want to throw any tool away that would help us with
22 this stuff so --

23 MR. BIRLA: That's right, so that's why
24 in one of his slides he mentioned we are looking for
25 contrarian viewpoints. If you know of any, that is

NEAL R. GROSS

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

1 published, that has --

2 MEMBER STETKAR: I was going to say, or
3 perhaps mainstream viewpoints, having heard the
4 contrarian viewpoints.

5 (Laughter)

6 MR. BIRLA: Contrarian to the findings
7 here, and the findings pretty much are based on IRSN
8 experience in this report.

9 MR. BETANCOURT: We are not saying that
10 this RIL is actually is not useful. We are just
11 saying that we are so far for our purposes, it's not
12 useful.

13 It can be used as another part of the
14 development process and that's the thing that we are
15 going to be discussing in the second RIL.

16 MR. BIRLA: So that is an important
17 distinction.

18 CHAIR BROWN: And that point -- you'll
19 make that point in the second RIL?

20 MR. BIRLA: Yes, yes.

21 CHAIR BROWN: With all the associated
22 stuff that' supposed to go with it?

23 MR. BIRLA: Yes.

24 CHAIR BROWN: Why.

25 MR. BIRLA: So, in the second RIL we

NEAL R. GROSS

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

1 have a little bit more freedom because we are not
2 constrained with the IRSN collaboration. With the
3 IRSN we have to limit ourselves to basically what
4 are we learning from them, with the appendix and the
5 foreword, convey some information to the licensing
6 offices, how it's relevant to them.

7 We did go one step further than we go
8 with traditional international agreement NUREGs, and
9 that was Luis added a literature review, which we
10 presented to IRSN, and we labeled as a -- we are
11 going to look for contrarian viewpoints and we are
12 going to give those to you so that we get your
13 evaluation response for that purpose.

14 So that was the deviation from the
15 traditional NUREG. But in the second RIL we have
16 more flexibility and this is the time to let us know
17 if you have any specific instances that you want us
18 to follow up on.

19 CHAIR BROWN: Yes, but your fundamental
20 conclusion is that the software FMEA -- correct me
21 if I'm wrong -- is the -- people can use it as a
22 design tool, an evaluation tool, but from a safety
23 assurance standpoint you are not comfortable with
24 saying that we can obtain adequate safety assurance
25 for a system per se, based on the FMEA approach

NEAL R. GROSS

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

1 alone.

2 MR. BIRLA: We are making a statement
3 stronger than not convertible. We are saying that
4 too many pitfalls.

5 CHAIR BROWN: That's fine. I just -- I
6 gave you a kind of a -- I was just trying to
7 summarize it just crisply in my own mind.

8 MR. BIRLA: Yes.

9 MEMBER STETKAR: Let's get to the real
10 presentation while Dennis is here.

11 CHAIR BROWN: Yes, that's what I want to
12 do. Are we done with this?

13 MR. BETANCOURT: Yes.

14 CHAIR BROWN: Okay, then we will go on
15 to the -- thank you very much -- to the discussion
16 and we'll move on to Sushil's presentation.

17 MR. BIRLA: Thank you, Luis. So the
18 presentation I am about to make is of the findings
19 from what we at that time called an expert clinic,
20 but later on we learned that there was an SRM that
21 came out about six months ago that had a
22 standardized term called the expert judgment process
23 or the expert judgement approach, so that's the term
24 we are going to try and use in describing our
25 activity here.

NEAL R. GROSS

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

1 MEMBER STETKAR: Sushil, is this really
2 expert judgement or expert elicitation in the
3 context of that SRM, or is this simply asking
4 experts for their opinions on particular topics?

5 MR. BIRLA: We have a set of slides to
6 describe the process. We believe it is a significant
7 contribution to what that SRM is looking for. It is
8 more than collecting opinions.

9 What products are in the form of
10 research information letters, the first result,
11 software-related uncertainties in assurance of
12 digital safety systems, is what I am presenting
13 today.

14 Basically, the material is in three
15 segments. The first is the background. I am going to
16 go over some of the same material that Luis went
17 over, emphasizing the purpose here, the scope.

18 The second segment is a description of
19 this expert judgement process and the third segment
20 is the findings resulting from that process being
21 reported in RIL-1001.

22 The authorization for this work stems
23 from this 2008 SRM, number M080605B. We subdivided
24 the digital I&C-related relevant portion into two
25 parts, the left and the right that you see here, and

NEAL R. GROSS

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

1 incorporated corresponding research activities into
2 the NRC's Digital Research Plan, into three parts of
3 that research plan, Section 3.1.5, analytical system
4 of traditional systems, and that's where we used the
5 expert judgement process, and second part is
6 knowledge management and a specific element of that
7 is what we can learn from operating experience.

8 You will see throughout the day that in
9 this knowledge management category, we are taking
10 different approaches to acquire knowledge from the
11 outside.

12 You saw the IRSN collaboration in the
13 previous presentation. You saw a more thorough --
14 you are going to see a more thorough expert
15 elicitation process applied here, and in later
16 presentations you will also see how we are trying to
17 get information from outside the NRC and outside the
18 nuclear industry by the way.

19 And the third segment is the PRA-related
20 project, 3.1.6, which you heard of reported on the
21 seventh of June.

22 Some of the results of our analytical
23 assessment will serve the digital system PRA project
24 as additional knowledge for them to use.

25 The second part of this SRM, the

NEAL R. GROSS

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

1 feasibility of applying failure mode analysis to
2 quantification risk associated with digital systems,
3 that part of the SRM will be answered -- is being
4 addressed through two different activities.

5 The PRA research is more focused on the
6 methods, assuming that the data will confirm
7 somewhere else. But those methods are also dependent
8 on knowledge: if you apply expert judgement, the
9 knowledge available at the time, the expert is asked
10 to exercise that judgement, the different that they
11 are going to make is change the statement of
12 knowledge, to provide additional knowledge. That's
13 the connection to the other project.

14 Again, let me refresh everyone's memory
15 about the concerns that led to that SRM. As Luis
16 mentioned, ISG-3 and the Brookhaven report that the
17 ACRS reviewed, and the concern was in the context of
18 risk-informing licensing reviews.

19 So our scope is limited to risk-
20 informing licensing reviews, not the development
21 process, not PRAs, but risk-informing licensing
22 reviews.

23 So you have seen this before. I am going
24 to skip over the rest of it. One reason of why this
25 is such a difficult matter in the process of

NEAL R. GROSS

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

1 assurance is that our regulation is pretty complex.

2 There are 70 sections in the regulations
3 that one has to refer to and they are connected with
4 200 or so relationships just at the section level
5 with approximately 10 different regulatory guides
6 that have references to 10 or so voluntary consensus
7 standards that further reference other references.

8 Through all this, one has to go through
9 a review process and come up with a safety
10 determination and we are trying to risk-inform this
11 complex process -- not only the process, the
12 regulatory review process, but the systems, the
13 complexity in the systems.

14 You see in the recent applications
15 interconnections and interactions across redundant
16 divisions, across safety and non-safety systems,
17 across lines of defense, across monitored and
18 monitoring elements of the overall system. You are
19 trying to risk-inform this kind of a system.

20 So now I'm going to part 2 of the
21 presentation, which is the research approach,
22 acquisition --

23 MEMBER BLEY: By the way. Two slides
24 ago, did you put together a catalogue of
25 specifically -- and could you share it with us some

NEAL R. GROSS

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

1 time, not now -- the 70 sections in the NRC
2 regulations, and exactly which are the 10 guides? I
3 am not sure I would know all 10 of them.

4 MR. BIRLA: Yes, this is work in
5 process. Later in the afternoon you will hear a
6 presentation on the state of this activity. Milton
7 are you here? So it will be part of that
8 presentation, and NRR, Norbert, started compiling
9 this information.

10 Our objective was to discover where are
11 the overlaps, where are the gaps -

12 MEMBER BLEY: But when you gave all of
13 this I'm thinking, I wonder if you have really been
14 able to -- actually have been tracking all of this.
15 There must be some gaps in --

16 MR. BIRLA: Yes, gaps and overlaps.

17 MEMBER BLEY: I hope he'll talk about
18 that.

19 MR. BIRLA: And inconsistencies. So we
20 are prepared to talk about what the gaps are, what
21 the inconsistencies are, but we will give you --
22 Milton will present a roadmap on where we are
23 headed.

24 MEMBER BLEY: If nothing else, that
25 should be a useful catalogue to have in hand.

NEAL R. GROSS

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

1 MR. BIRLA: Well we hope it's more than
2 a useful catalogue. We hope that it starts to drive
3 change.

4 MEMBER REMPE: Isn't it part of your
5 knowledge management effort, to simplify some of it
6 too. That's what I remember reading.

7 MR. BIRLA: Yes. Utilization of expert
8 judgment approach. Let me take to the SRM. It
9 defines it as the process used to elicit information
10 from experts, analyze the information and develop
11 results, and determine the implications of the
12 results to support regulatory decision-making.

13 Our customization is that last phrase
14 results to support regulatory decision-making. We
15 are applying that to decisions about research paths,
16 in other words reshaping our research plan to
17 develop the technical basis for regulatory guidance.

18 CHAIR BROWN: Can you help me and tell
19 me where this is in the --

20 MEMBER REMPE: Yes, it's not in the
21 package.

22 CHAIR BROWN: in the package. We stop at
23 43 or 46, with acronyms.

24 MR. BIRLA: This is slide 53.

25 CHAIR BROWN: But there is no slide --

NEAL R. GROSS

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

1 do you all have the slide 53?

2 PARTICIPANTS: No.

3 MEMBER BLEY: I don't think I got this
4 one electronically, did I?

5 MR. BIRLA: The electronic version has
6 it. Okay, I guess --

7 MS. ANTONESCU: We didn't get that.

8 CHAIR BROWN: We got a printed one,
9 didn't we?

10 MR. BIRLA: Okay, so if you don't have
11 this in the printed version I apologize. This was
12 part of the backup material.

13 CHAIR BROWN: Okay.

14 MR. BIRLA: And I organized my material
15 int his way depending on your time situation,
16 whether you wanted me to go to this extra detail or
17 not. Since you asked me the question, I did want to
18 go to this.

19 MEMBER BLEY: Well, we'll get it from
20 the electronic one after this.

21 MR. BIRLA: I am going to give you an
22 overview of 13 growth or course steps that we
23 extracted to describe our process, the process we
24 used. I am going to omit the steps to actually
25 design this process.

NEAL R. GROSS

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

1 So in step 1, I won't read everything
2 word by word, but on step 1, there is a slide coming
3 up next, building the candidate pool. We went
4 through referrals, three levels of referral, got to
5 a number of 75, and the number continues to grow.

6 In other words, the process hasn't
7 stopped, so this pool will be a resource for the
8 future. Screening criteria slide will be coming up
9 later on that.

10 This pre-briefing included information
11 about the project purpose: the nuclear application
12 domain and the NRC's regulatory guidance framework.

13 MEMBER BLEY: Were you able to put all
14 the questions on the table for them before they
15 came, before you got them together?

16 MR. BIRLA: They were -- I'll come to
17 the questions -- but this was just even before,
18 before we started into the questions, just to give
19 them the context.

20 So the purpose didn't have the detailed
21 questions, but the SRM was there, and obviously the
22 regulatory guidance framework is such a complex
23 thing we couldn't do justice to that. The
24 application domain is also complex but we focus on
25 the safety systems, RPS, SFAS.

NEAL R. GROSS

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

1 We believe they got enough context not
2 to go astray. That was the purpose, that we didn't
3 want experts from outside the nuclear industry to
4 bring this experience that we would consider not
5 relevant.

6 Step number 5, interviewing experts for
7 individual elicitation, yes we did have an inventory
8 of questions that they received before the
9 individual elicitation interview.

10 Typically, it was a one- to two-hour
11 duration, sometimes it spread over two sessions or
12 three sessions, sometimes followed up by email to
13 provide remaining answers, references.

14 The interview was customized to each
15 expert's strength and comfort zone so not all
16 questions were covered evenly in each individual
17 elicitation, so this was not like your typical
18 Delphi survey.

19 MEMBER BLEY: Did you do these one on
20 one or did you pull some numbers together?

21 MR. BIRLA: Both, multi-stage. So, that
22 step number 5 was individual elicitation, then once
23 we had the 30 or so individual elicitations we did
24 an analysis and integration of the information,
25 developed a consensus position document, and then

NEAL R. GROSS

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

1 iterated through the 30 or so individuals, went
2 through many cycles of review and revision, and then
3 after finding what the broad consensus areas were
4 and what areas needed for the discussion, we created
5 a set of focus topics for the face-to-face focus
6 group to work on, and selected the focus group
7 members to match that set of topics.

8 MEMBER BLEY: That was a subset of the
9 people that had participated in the solicitation.

10 MR. BIRLA: That's right. And then we
11 brought them together for two days and developed the
12 first RIL after going through several iterations of
13 review and changes, released that to the licensing
14 offices.

15 We are in the middle of organizing the
16 remaining information for the second and third RIL.
17 In the second RIL, and I'll bring that up later too,
18 we will add more information if we get more
19 awareness in the meantime.

20 MEMBER BLEY: So this first one, the one
21 we got, all the members at least of your focus group
22 would consider it a consensus document?

23 MR. BIRLA: Yes. So this basically shows
24 going from the 75-plus down to the 10 finally that
25 were part of the focus group.

NEAL R. GROSS

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

1 The initial scope boundaries means the
2 scope boundaries that were given to the -- for
3 individual elicitations. Digital systems for nuclear
4 power plant safety functions, contribution to
5 failure for causes such as software -- attributable
6 to software -- and some initial questions: what is
7 meant by failure modes in this context; how to
8 identify and analyze failure modes attributable to
9 software, attributable to - to quantify like these
10 other two SRM questions.

11 But we added one. Using risk insights,
12 how do you reduce variation in safety assessment,
13 variation meaning reviewer to reviewer
14 inconsistency, rooted in uncertainties from
15 software.

16 This is where we are trying to derive
17 some value for the licensing offices, while we have
18 got the experts on tap.

19 To screen the experts first some general
20 criteria, and then some match of interest, the
21 experts have their own ideas on what was matching
22 but our ideas are that they should have significant
23 knowledge and experience contributing to project
24 activities, objectives, safety mission critical
25 digital systems, some element of the nuclear

NEAL R. GROSS

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

1 application domain, broad and integrative rather
2 than narrowly specialized, ability to identify
3 influencing factors and their inter-relationships,
4 ability to identify failure modes that fall in the
5 inter-relationships.

6 So during the pre-screening interviews
7 or conversations, some of the experts disqualified
8 themselves. The match of interest versus crunch of
9 time they really didn't feel that they could
10 contribute or get that much out of it or contribute
11 much to us.

12 CHAIR BROWN: How many -- I'm sorry, go
13 ahead.

14 MEMBER BLEY: Is there a reason why you
15 didn't identify who your experts and your focus
16 group were in the report itself, that's a consensus
17 document?

18 MR. BIRLA: It should be --

19 MEMBER BLEY: I didn't see it. I saw the
20 process.

21 MEMBER STETKAR: Their initials are in
22 there --

23 MR. BIRLA: Their initials are explained
24 in a table. So in the report, we referenced with
25 their initials, as you mentioned, and then we have a

NEAL R. GROSS

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

1 table giving the names of --

2 MEMBER BLEY: In the report?

3 MEMBER STETKAR: I think it fell out. I
4 looked for said table and I guess I missed it so I'm
5 curious where it is.

6 MR. BIRLA: Also, remember that, in
7 Appendix B there are tables with references
8 hyperlinked, so all the information from the project
9 is accessible there.

10 MEMBER BLEY: So if I were looking on
11 the computer I could hyperlink some of that?

12 MR. BIRLA: Yes, so Table 7 gives you
13 the names. So these are the names of the individuals
14 referenced specifically within the RIL. But they are
15 not all the people that we have got here, but all
16 the people who were in the focus group happen to be
17 in there.

18 MEMBER BLEY: Let's not dwell on this
19 but somehow I think --

20 MEMBER STETKAR: Oh, there's Table 7.
21 There it is.

22 MEMBER BLEY: Oh, there it is.

23 MEMBER STETKAR: Sorry. I looked but I
24 didn't see it.

25 MEMBER BLEY: That's the focus group

NEAL R. GROSS

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

1 anyway.

2 MR. BIRLA: Well, that's more than the
3 focus group.

4 MEMBER BLEY: Okay.

5 MR. BIRLA: Because it's composed of
6 information that was condensed even before we got
7 the group together.

8 MEMBER BLEY: Is that everybody who
9 actually participated?

10 MR. BIRLA: No.

11 MEMBER BLEY: So even more than that
12 participated?

13 MR. BIRLA: Right, right. So then you go
14 to the links even in the Appendix B and you have
15 access to all the information.

16 MEMBER BLEY: Okay, okay. I have read it
17 in hard copy so --

18 MR. BIRLA: Okay, so what did we do with
19 the individual elicitations and we had more than 30
20 of them? Obviously in a one- to two-hour interview
21 you can't get everything explicitly stated. They
22 talk in terms of implicit contexts so we got
23 references from them.

24 To organize the information, we used two
25 previous studies from the Academies. The '97 study

NEAL R. GROSS

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

1 was sponsored by the NRC and the 2000 software
2 dependability study has --

3 MEMBER BLEY: That's Daniel Jackson's
4 one.

5 MR. BIRLA: Yes. Daniel Jackson headed
6 that, so you and I have discussed that. So that gave
7 a backdrop framework to organize this information
8 in, and then there were some other references that
9 were useful.

10 So the integrated information was
11 documented in terms of a consensus position. We
12 called it a reference position paper at that time,
13 and sent that back to all 30-plus individuals and
14 went through several rounds of review, changes --
15 gee, when I talked I was nuancing this and you
16 removed my nuance. So I want it back, or I can live
17 with it, or -- and so on.

18 So there was no major conflict.

19 MEMBER BLEY: Okay. And they got a look
20 at the final report, well, of this --

21 MR. BIRLA: Yes, yes.

22 MEMBER BLEY: of this report.

23 MR. BIRLA: There was one individual,
24 one expert who said that your document and your
25 approach seems to be slanted to using reliability-

NEAL R. GROSS

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

1 type quantification methods and you are just looking
2 for support for that, and you aren't listening to me
3 and I am saying to you that that's the wrong way to
4 go, you should do a development process assessment,
5 and I want to make sure my name doesn't get
6 associated with this report. So that was the only
7 conflict we got.

8 MEMBER BLEY: And that person is gone?

9 MR. BIRLA: Not gone, he is a very
10 respectable individual in European safety, in the
11 European safety community. He works for a supplier
12 organization in their research organization.

13 He has contributed significantly --

14 MEMBER BLEY: By "gone," I meant you no
15 longer reference him in the report, is that right?

16 MR. BIRLA: We do not reference him in
17 the RIL but if you go into the hyperlinked
18 documents, you can find the name.

19 MEMBER BLEY: History is history, yes.

20 (Laughter)

21 CHAIR BROWN: So the contrarian position
22 is not expressed in the -- other than through the
23 links? Is his -- I would view his as a contrarian
24 position to what you all were trying to do.

25 MR. BIRLA: His position was a

NEAL R. GROSS

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

1 misunderstanding. He misunderstood us.

2 CHAIR BROWN: Okay.

3 MR. BIRLA: He thought that we were
4 proponents of quantification as a technique to do
5 assurance.

6 CHAIR BROWN: Okay, all right.

7 MR. BIRLA: And he didn't want his name
8 associated because we weren't conveying that flavor.
9 So we really didn't have a conflict with him or his
10 ideas. We just had a misunderstanding and he is
11 still a valuable resource, he's part of that
12 75-candidate pool, and I'm sure that when we start
13 working with the international community European
14 research organization safety research we are going
15 to come across the individual again.

16 So it's not that the relationship is
17 broken. It's just that he perceived this work to be
18 quantification-oriented and therefore didn't want to
19 be associated -- in other words he is so much
20 strongly against that.

21 So from this analysis, and seeing what
22 happened in the consensus position, we selected
23 certain topics of the focus group, first to get some
24 value out for the licensing offices, which was, we
25 thought, going to be useful in their so-called

NEAL R. GROSS

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

1 determinate screening process and in resolving some
2 conflicts they were experiencing; and secondly, to
3 increase our level of confidence in the information
4 we were gathering.

5 In other words, certain questions we did
6 want them to discuss and other questions, we were
7 already in such a strong consensus we didn't want to
8 rehash that in the face-to-face.

9 From the clinic we have everything that
10 happened: oral records; written transcripts of the
11 oral records for the full two days; the expert
12 summaries -- their own summaries I mean; their
13 presentations; all that boiled down into the RIL.

14 So the RIL is not the only thing. This
15 is the published thing. There is more information
16 back there.

17 And on the left side of the diagram you
18 see that in the second and third RIL, particularly
19 for the second RIL, we intend to get other experts'
20 inputs because we have such a strong consensus, we
21 feel we still need to get some contrarian opinions
22 there, or contrarian positions I should say.

23 So what were those broad consensus
24 positions, even before meeting face to face?
25 Basically negative to both parts of the SRM.

1 So that's not what we wanted to spend
2 more time on so we shifted the discussion from
3 basically a difficulty in characterizing failure
4 modes or fault modes, to understanding why those
5 difficulties arose; what were the unknowns and
6 uncertainties leading to the large potential fault
7 space.

8 So, --

9 CHAIR BROWN: Going back to 15, make
10 sure I understand the whole -- as you stated
11 earlier, the contrast was as you just noted right in
12 the top, the ability to risk-inform the software
13 assurance issues.

14 So those are your conclusions from the
15 elicitation -- that's what I get out of these two
16 statements, that they couldn't -- there was no
17 consensus on a, or what you said, no compact set of
18 failure modes etcetera, and the feasibility was no.

19 MR. BIRLA: Right.

20 CHAIR BROWN: Okay, so fair and crisp,
21 plainly stated --

22 MR. BIRLA: Plainly stated.

23 CHAIR BROWN: I just want to make sure I
24 understood.

25 MR. BIRLA: I had those set of experts.

NEAL R. GROSS

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

1 CHAIR BROWN: Yes, that's fine.

2 MEMBER BLEY: I have a question because
3 I am -- experts are experts, but Brookhaven did an
4 expert group a year or two ago, and my reminder of
5 their report was that they were bursting with
6 optimism about how well you could, you know, model
7 this problem, much more than I personally am.

8 And maybe they are none of the same
9 experts across the two groups, or did you look at
10 their report or am I mis-remembering?

11 MR. BIRLA: Yes, I was there, mine was
12 there.

13 MEMBER BLEY: Oh you were actually at
14 the --

15 MR. BIRLA: Oh yes, yes, I was there.

16 MEMBER BLEY: Am I mis-remembering or --
17 ?

18 MR. BIRLA: First, let's refresh your
19 memory on what happened there. They came up with a
20 compact set of failure modes at the function level
21 but those were system functions.

22 And what you saw earlier in Luis's
23 presentation encompasses that set.

24 MEMBER BLEY: Okay, I didn't even
25 remember they came up with a set.

NEAL R. GROSS

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

1 MR. BIRLA: Yes.

2 MEMBER BLEY: Okay.

3 MR. BIRLA: On -- they didn't have the
4 last one, one clobbering another, but I prompted
5 Alan to get that added.

6 MEMBER BLEY: Okay.

7 MR. BIRLA: So the report documents
8 that, and they felt quite strongly, as Dr Stetkar
9 does, that there is no value in digging any deeper
10 or any finer. This is the level at which it is
11 appropriate to extract these failure modes.

12 Then, the question to them was is there
13 a philosophical basis for using failure mode
14 analysis to quantification, and their answer was
15 philosophical: yes, there is a philosophical basis.

16 One of the key premises was that for a
17 PRA expert or a group of PRA experts, it is quite
18 appropriate to give an estimation of their failure
19 likelihood based on the knowledge and information
20 available at the time the individual group is asked
21 to make that estimation.

22 So that's the context. And in that
23 context, yes, in their religion, their methodology,
24 that is the right thing to do.

25 Our contribution is based on the

NEAL R. GROSS

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

1 knowledge you had, if you had inadequate knowledge,
2 how can we change the state of that knowledge?

3 They also didn't take a position on the
4 degree of confidence in that estimate. What do you
5 use that estimate for? For PRA purposes, maybe it is
6 appropriate. Maybe it's good enough.

7 Steve Arndt was there. One suggestion he
8 made was well, can we not increase the degree of
9 knowledge by using the knowledge or information we
10 are gathering from the licensing-review process.

11 So we have a lot of artifacts that the
12 applicant is bringing in, in reviewing those, can't
13 we get some additional insights. That was recorded
14 as part of the Brookhaven report, and that's the
15 part we are addressing here.

16 MEMBER BLEY: Okay. Thank you. That
17 helps.

18 MR. BIRLA: So we shifted the focus
19 group to address these themes: what are the sources
20 of uncertainties; and what's the evidence needed to
21 reduce these uncertainties; and if you can't come up
22 with an answer to these questions, what are the
23 knowledge gaps.

24 In this picture, what I am going to show
25 is that this potential fault space is large if you

NEAL R. GROSS

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

1 have poor design practice. Now Dr. Stetkar, at the
2 seventh of June meeting, you had asked that
3 question, is there any relationship⁰ between meeting
4 certain standards and the likelihood of failure.

5 It is generally believed in the industry
6 that if you don't use good design practice, you are
7 going to have more defects in your product. So there
8 is a premise that you have to make before you can
9 talk about well, what are the additional
10 uncertainties.

11 The NRC's regulatory guidance framework
12 takes us a level above the commercial industry's
13 good design practice, and the Appendix A in this
14 RIL, which is a collection of all the -- some people
15 call them good practices, additional good practices,
16 well-known principles and criteria and conditions.

17 If you put that all together the level
18 goes up even higher. So we said look, if you do all
19 this correctly, if the applicant does all this
20 correctly in creating a system, what are the
21 residual uncertainties?

22 In other words, don't spend your two
23 days in telling us what we already know, what you
24 have already agreed upon. But given that as the
25 platform or the level, what are the remaining

NEAL R. GROSS

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

1 uncertainties, so focus the group on that, assuming
2 conformity to everything else that you see.

3 So in forming the group, we wanted to
4 limit the number to 10, 12 or so. We wanted to have
5 a minimum of six, in this size range. We still
6 wanted to get a full complement of expertise -- not
7 everyone knows everything -- and we wanted to
8 maximize the objectivity through the independence
9 and diversity in different dimensions.

10 So if you have strength in theory, then
11 at least you should be able to relate that theory to
12 something practical; and if you have strength in
13 practice, then you should be able to frame that in
14 the context of a theoretical model, analytical
15 model.

16 Diversity in application domains,
17 medical stays, and so on, and the types of
18 platforms, whether it's a platform level expertise
19 or application-level -- integrated-system level
20 expertise, or whether it's process expertise and
21 safety engineering processes or software engineering
22 process, or system engineering processes, and above
23 all, their problem-solving paradigm, wanted some
24 diversity in the schools of thought.

25 So these were the criteria we laid out.

NEAL R. GROSS

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

1 That is what we realized. So there were people with
2 expertise either in requirements, in architecture,
3 methods and tools, assurance, different application
4 modes, defense, space, aviation, auto, rail,
5 telecom, medical, and there was one nuclear,
6 although we were trying to really get information
7 from outside the nuclear industry.

8 And in schools of thoughts there were
9 some that were in the formal methods end of the
10 spectrum and some who had expertise in using expert
11 judgement.

12 MEMBER BLEY: Let me ask one last
13 question before I have to depart. Are the
14 differences we see in the results and the story
15 obtained from your clinic and from the previous
16 Brookhaven one, the product of the particular
17 experts we had, or the product of, as you talked
18 before , the charge to that group -- what's the
19 exact question they are trying to answer? Do you
20 have a good feeling about that?

21 MR. BIRLA: Well, the charge was
22 different. They were asked a question, is there a
23 philosophical basis, very limited scope.

24 MEMBER BLEY: Okay. Okay. Because my
25 concern was, gee, if -- if we are all picking the

NEAL R. GROSS

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

1 experts we like best for the cause we are after, we
2 are not getting that broad range of experts we want
3 to address this issue.

4 MR. BIRLA: But they weren't all --
5 look, if your like was dependent on the system
6 working, would you trust your number? They weren't
7 asked that question.

8 MEMBER BLEY: Okay.

9 MEMBER STETKAR: Well, but did you ask
10 your experts, if your life depended on defining a
11 half a dozen failure modes, could you please do
12 that? Did you ask your experts to do that?

13 MR. BIRLA: We didn't even get that far.

14 MEMBER STETKAR: But you didn't ask them
15 try? You didn't say your life depends on this?

16 MR. BIRLA: What they mean by failure
17 modes, it's hard to even get agreement on that, that
18 there is a --

19 MEMBER STETKAR: It might have been
20 useful to see what they thought were failure modes.
21 You might have seen that there was agreement or 60
22 percent agreement.

23 MR. BIRLA: There was quite a large
24 diversity, in the definition, in --

25 MEMBER STETKAR: Not in a theoretical

NEAL R. GROSS

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

1 definition. Did you ask them to please give me your
2 concept of six failure modes?

3 MR. BIRLA: Examples yes, we got
4 examples and yes -- and there was one end of the
5 spectrum that maps into -- for software --

6 MEMBER STETKAR: There wasn't too much
7 correlation at all?

8 MR. BIRLA: No, no.

9 MEMBER STETKAR: Okay.

10 MR. BIRLA: That is why the second RIL
11 is going to cover a wide waterfront.

12 MEMBER STETKAR: Okay.

13 MR. BIRLA: but there was -- if there
14 was some correlation, there was on this theme that
15 Luis mentioned earlier. Well, with software, if it's
16 properly done, if the system failed because of a
17 software issue, that was broken to start with.

18 So technically, the way we define
19 failure, it didn't fail, it was failed to start
20 with. So we shouldn't be talking in terms of
21 failures, we should be talking of fault, defect
22 classification systems and so on.

23 So this is the list of the actual
24 participants. These --

25 MEMBER STETKAR: Out of curiosity I

NEAL R. GROSS

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

1 don't see anybody there from -- and I know you tried
2 to avoid nuclear, but I don't see anyone there from
3 Korea. I see one UK, two Uks, Finland. Were people
4 in those countries contacted? The Koreans have done,
5 at least in the nuclear business, a lot of so-called
6 software. I don't know what they have done I haven't
7 seen it.

8 MR. BIRLA: Yes, so, through this
9 process, these were the 75 we were able to reach,
10 the 30 that we elicited individually, the 10 that we
11 brought together.

12 That doesn't mean that this is the whole
13 spectrum. In Luis's report, in the NUREG, you will
14 see a reference to a KAERI paper.

15 MEMBER STETKAR: Yes.

16 MR. BIRLA: And we do want to talk to
17 them. We have tried to establish teleconferences,
18 but there's a 12-hour difference and a language
19 difference, and we were not successful.

20 We are trying to find some time when
21 their experts, meaning not the bosses, but the
22 engineers, and our engineers can talk to each other
23 with a translator, and we have not been successful
24 at that.

25 So we know there is something to learn

NEAL R. GROSS

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

1 from KAERI's work. The Finland expertise is also
2 being accessed through other channels --

3 MEMBER STETKAR: Okay.

4 MR. BIRLA: connections in STUK and then
5 their technical support organization, and yes, you
6 don't see Norway here either, but we have other
7 channels. You don't see France here but you already
8 heard the IRSN connection.

9 MEMBER STETKAR: Through the IRSN.

10 MR. BIRLA: So this was one mechanism of
11 tapping knowledge outside our industry or our
12 environment, but this is not the only thing.
13 Throughout the day you are going to see different
14 approaches.

15 Now, when we brought them together, we
16 showed them this as the vetting model, that if you
17 look at the central horizontal bar, you see the
18 traditional evidence argument claim connections, and
19 if you look at it from top-down you see the basis
20 for the argument.

21 And if you see bottom-up, you see the
22 vetting process. What's the weakness in the
23 argument? What are the factors influencing the
24 validity of the argument?

25 And this is what we asked them to focus

1 on. And we asked them to give us their own
2 assessment of the strength they believed of their
3 conclusion, so the qualifiers could be either
4 reducing the scope, or some degree of strength.

5 Incidentally it's the same model that we
6 used in other parts of the process and I'll bring
7 that up again later.

8 CHAIR BROWN: Okay, you are fine right
9 where you are. In the interests of trying to
10 maintain some relative schedule, is this a
11 reasonable break point, right here?

12 MR. BIRLA: Yes. Yes.

13 CHAIR BROWN: Okay. We will go ahead and
14 if I can get this correct, we will recess for lunch
15 and we will un-recess at 10 minutes after one. You
16 have one hour and four minutes to execute thta. Is
17 that precise enough?

18 (Whereupon the above-entitled
19 matter broke for lunch at 12:05 p.m.)

1 A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

2 1:14 p.m.

3 CHAIR BROWN: We are un-recessed and we
4 will continue the dialogue on -- starting with the
5 software-related uncertainties. Okay Sushil, so you
6 are back on the floor.

7 MR. BIRLA: Okay, so just to reconnect
8 with where we were before lunch, before the break, I
9 was going over the expert judgement process we
10 utilized in this project, and I am at the tail end
11 of the description of that process, ready to
12 transition into what came out of the process.

13 So, as I said before lunch, we selected
14 topics based on what increase invalidation we were
15 seeking, and value to our licensing offices. So
16 these were the five topics. I am still going to do a
17 little bit of process description here, and I will
18 come back to the topics as we go into -- transition
19 into the outcome session part -- segment, part of
20 it.

21 So the group met for two days and they
22 used the first one and a half days as their own work
23 time, divided into five segments, one for each one
24 of these topics.

25 So typically, let's say two hours or so

1 on each topic, and they were asked to write down
2 their consensus conclusions at the end of each
3 section, so wrap up the topic right there.

4 Then the sixth segment was used to do a
5 second review of all the five section outcomes and
6 integrate -- with an integrated perspective, and
7 refine their conclusions.

8 So the write-up at the end of each
9 segment was sort of a textual narrative and in the
10 sixth segment, that means just before lunch the
11 second day, they created PowerPoint slides.

12 And then on the second half of the
13 second day, we had representatives of the licensing
14 offices in the room to listen to the outcome and ask
15 them questions, and the experts valued that
16 interchange, that interaction very well -- very much
17 too.

18 The 13th course steps here is feedback-
19 related so we did though a process of seeking
20 written feedback, oral closure, we have processed
21 the ideas, factored them into what we were going to
22 do with them.

23 I have got about seven or eight slides
24 that I can go through if you have an interest, if
25 you want through them later on, after I've finished

NEAL R. GROSS

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

1 the third segment, we can to that too. Your pleasure

2 CHAIR BROWN: Let's go ahead and get
3 through what we do here and then we will -- is that
4 satisfactory with you all? Okay.

5 MR. BIRLA: So, continue the feedback
6 process?

7 CHAIR BROWN: No, go ahead and go on.

8 MR. BIRLA: Okay.

9 CHAIR BROWN: And we will come back. Why
10 is there an echo?

11 MR. BIRLA: Again, you will have some
12 discretionary opportunity and you may say I don't
13 want to go back to that anymore, or you may say I'll
14 come back, so I'll follow your cue on it.

15 I summarized the impact of the clinic on
16 this slide. First, influence on the licensing
17 reviews. Immediately the licensing office
18 representatives saw that some of the positions were
19 reinforcing what they had already been believing but
20 were being challenged against, so it boosted their
21 confidence.

22 And then secondly it increased awareness
23 of issues and this awareness will help them through
24 exercising their judgement in future licensing
25 reviews.

NEAL R. GROSS

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

1 The second part of the influence was on
2 the research activities themselves. Three research
3 activities have been identified as being impacted,
4 influenced by this clinic.

5 One, the two automated processes, we
6 already had it explicitly in our research plan; the
7 other two we did not but they fall under one of the
8 umbrella project descriptions.

9 And work is under way right now in
10 defining the project for the framework for safety
11 demonstration and later on for change impact
12 analysis.

13 CHAIR BROWN: Now, so -- go back. The
14 post -- this was the second half of the second day,
15 you went through it with staff and whatever
16 management and then -- and this -- so you are saying
17 this was the impact of those discussions with the
18 staff after the first day and a half of reviews by
19 the --

20 MR. BIRLA: Right.

21 CHAIR BROWN: experts right? And their
22 conclusion's in their little presentation, I mean
23 they made a presentation from which this --
24 conclusions were drawn?

25 MR. BIRLA: Yes.

1 CHAIR BROWN: Okay.

2 MR. BIRLA: Hust to give you an example,
3 when the presenter for change impact analysis, and
4 that happened to be John Knight, made the
5 presentation, Rich Tattle, representing the NRR, one
6 of the people from NRR, made an observation, gee, in
7 my work in the plants, I had these issues and it was
8 very difficult to analyze the effect of a change.

9 So, sort of resonating, and on the two
10 automated processes, they already have a topical
11 report that they are working with, and a couple of
12 years ago we had a controversy on NRR's position,
13 NRO's position, and the vendor's aspirations on this
14 subject.

15 And you yourselves have challenged us
16 when we were reviewing this first plan with you, of
17 why in the heck we are even working on it.

18 So we have enough controversy in there
19 to put the topic to the focus group and got some
20 value out of it.

21 MEMBER STETKAR: Sushil, in the RIL, in
22 section 8.2, there -- and I don't know whether you
23 will cover this later or not, so if you will, then
24 I'll wait, but there was follow-on involvement of
25 expert focus groups, and one of the statements in

NEAL R. GROSS

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

1 there, it says these activities will also support
2 the creation of a challenge problem model, another
3 suggestion emergent from the expert clinic.

4 This model will be representative of the
5 system configurations, platforms and applications
6 seen or expected in the nuclear power plant domain.
7 In order to focus the experts' knowledge on problems
8 being experienced or foreseen in the NRC, these
9 activities will require the participation of
10 experienced NRC licensing reviewers.

11 I interpreted that as kind of a case
12 study problem. Did I misinterpret that? And if I
13 did, which of --

14 MR. BIRLA: Yes, so let's first just
15 take the term case study. What the experts are
16 asking for is look, we as researchers in academia
17 would like to work on a real-life problem.

18 MEMBER STETKAR: Right.

19 MR. BIRLA: Now, I call it -- use the
20 DARPA term challenge problem model --

21 MEMBER STETKAR: Okay.

22 MR. BIRLA: because we can't really give
23 to them something from a real case, an application,
24 a licensing application. So we have to sanitize
25 that. So not the case study in terms of take a real

NEAL R. GROSS

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

1 application or a safety analysis report and safety
2 evaluation report, and give it to the researchers

3 It's a little too sensitive. So genericize
4 that. So an example would be they take the Oconee
5 configuration and I showed you a picture, the BPR
6 configuration, there's Mitsubishi's very similar.

7 CHAIR BROWN: But publicly available
8 information. now, my question is, you, under the
9 influence on fiscal year 2010-14 research plan, you
10 have highlighted three bullets here.

11 I don't see this activity in those three
12 bullets, or I might be misinterpreting what those
13 three bullets mean. Is this what I am calling a --
14 I'll use your term -- challenge problem?

15 MR. BIRLA: So what you see in the RIL, in
16 section 8.2, is the general statement and the
17 challenge problem model was one specific thing, I
18 agree, but concentrate more on the general statement,
19 and then these three examples of three specific cases
20 of engaging them in follow-on research activities.

21 Now, the problem model --

22 MEMBER STETKAR: Yes, but as you
23 mentioned, these are three very general, in my
24 interpretation, conceptual, how you might deal with
25 things, issues. My interpretation of that item in the

NEAL R. GROSS

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

1 RIL was that it seemed to be an opportunity to focus,
2 as you put it, the academic experts' expertise on a
3 real-world real problem.

4 MR. BIRLA: A class of real problems. We
5 can't really focus them on a single case study, but
6 genericize to the domain. Future applications are in
7 this trend line. These are the characteristics -- so
8 that's the characterization part of it, the first
9 sentence, and the second bullet in the section 8.2

10 CHAIR BROWN: Where you say characterize
11 different kinds of DI&C and their relationships to
12 their environments?

13 MR. BIRLA: Yes. So, is Tom Burton's part
14 going to be presented later?

15 MR. SYDNOR: It is talked about in the
16 operational experience.

17 MR. BIRLA: The inventory classification,
18 and so on? Okay, so there's an activity already going
19 on and one of the uses of the results of that activity
20 is this characterization.

21 MEMBER STETKAR: Okay, thanks. I'll have
22 to think about that a little bit more, because --

23 MR. BIRLA: So yes, conceptually each one
24 of these project activities that you see on the slide,
25 we don't want to solve the world hunger problem in

NEAL R. GROSS

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

1 each case, but we want to focus the activity on our
2 domain.

3 What does that mean, and that itself is
4 going to take some effort. You can't just say look,
5 here's what the EPR application is, or here's the
6 topical report on tools, or here's the topical report
7 on change process.

8 So those are the real cases we have in
9 licensing offices, but we have to generalize in a
10 manner that the research is applicable for at least
11 that trend line.

12 They valued that. That's the important
13 thing. There were a number of academics in the group
14 and they valued that. Generally academics want
15 theoretical, publishable stuff.

16 MEMBER STETKAR: I understand that. On the
17 other hand in the real world, it's nice to see how
18 some of the theory might be applied to something
19 that's somewhat real, which generally requires that
20 you need not theoretical, simplified things of
21 somebody's concept of what some software might be, but
22 an actual integrated system.

23 MR. BIRLA: Right.

24 MEMBER STETKAR: So -- okay.

25 MR. BIRLA: So when you say the word

NEAL R. GROSS

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

1 actual, now that's where we have to step back a little
2 bit. We can't really give them actual data from an
3 application.

4 CHAIR BROWN: Well but your real --

5 MEMBER STETKAR: Wait a minute -- are not
6 the Design Certification information public knowledge?

7 CHAIR BROWN: Yes.

8 MEMBER STETKAR: Is not the Design
9 Certification information the information that NRC
10 licensing reviewers have available to them?

11 MR. BIRLA: It is. They have it, but it's
12 not enough.

13 MEMBER STETKAR: They have to ask more
14 questions certainly to perform their reviews. The
15 question is, are you asking -- are reviewers asking
16 the right questions and are those questions informed
17 by domain experts within the software community?

18 MR. BIRLA: That's where we want to go.

19 MEMBER STETKAR: Well fine, why don't you
20 give them a real system with publicly-available
21 information and say go apply what you have learned
22 here?

23 MR. BIRLA: What I am saying is they will
24 have all that but that information is not enough for
25 them, because take the design certification documents,

NEAL R. GROSS

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

1 they are basically process-description documents.
2 There isn't any design description there.

3 CHAIR BROWN: You are sounding like me
4 Sushil.

5 (Laughter).

6 CHAIR BROWN: Excuse me, I couldn't
7 resist.

8 MEMBER STETKAR: Well, but I mean if the
9 whole purpose of this is to make the licensing
10 reviewers' jobs more focused and more efficient, which
11 is what I hear you saying, then perhaps the questions
12 that the software experts would ask would be a useful
13 product.

14 MR. BIRLA: Yes. Yes.

15 MEMBER STETKAR: They might ask different
16 questions for example.

17 MR. BIRLA: Yes, that's right.

18 CHAIR BROWN: Let me -- can I amplify a
19 bit?

20 MEMBER STETKAR: Yes I am done.

21 CHAIR BROWN: When I look -- I have looked
22 at three point -- 1.5 out of the plan and I have
23 looked at your comment here, and you are effectively
24 talking about platforms themselves, which are -- they
25 have their own software and operating system, which

NEAL R. GROSS

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

1 has its own vulnerabilities and/or strengths and
2 weaknesses, whatever you want to call it, and that's
3 what you refer to in both the deliverable and -- and
4 then restated in the first bullet, in 8.2.

5 MR. BIRLA: The platforms are one part of
6 it.

7 CHAIR BROWN: Yes, no I understand that.
8 But platform to platform, the DCD shows you a platform
9 to platform whether they have a processing platform
10 then they have a voting-level platform.

11 The software in hose is -- you know, the
12 operating systems and how they operate. I tend to
13 agree with John, if you genericize them too much then
14 you lose the thrust of the pluses or minuses or
15 whatever this tool-automated and tool-assisted process
16 is supposed to deliver.

17 MR. BIRLA: And if you become too specific
18 then the result doesn't have much longevity.

19 CHAIR BROWN: Well, but it allows you to
20 assess whether the tools gave you a valid or a
21 reasonable assessment -- I'm not saying safety
22 assurance, but at least a reasonable assurance.

23 MR. BIRLA: So now we are talking of two
24 different things: one is to shape any such project;
25 and the other is to validate the results. So to shape

NEAL R. GROSS

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

1 the research project, I want them to use awareness of
2 this application domain and confine the research
3 project's code to address the class of domains rather
4 than address a much wider class.

5 But you are correct. When they have
6 research results, we need to have a test case for
7 testing, evaluating the results, and that's where the
8 specifics come in.

9 MEMBER STETKAR: So you are saying it's we
10 are too premature in the 2010-2014 time frame to do
11 that second step?

12 MR. BIRLA: I wouldn't say that. I was
13 just clarifying that as part of a research plan, if
14 you said now, here's your theoretical output of your
15 research, you need to validate, you need to test it,
16 you need to evaluate it, and we want you to evaluate
17 it against a real example, a real SER. Yes that would
18 be appropriate.

19 And then certainly, what you said Dr.
20 Stetkar would happen, they would say look, these were
21 the questions that should be asked. There isn't enough
22 information here.

23 And then we can take that list of
24 questions and see, well what are our RAIs asking? You
25 cannot make a safety determination unless you answer

NEAL R. GROSS

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

1 these questions. That's the kind of research result we
2 want from them.

3 CHAIR BROWN: Okay, let me apply a
4 slightly different questions, well, it's similar, but
5 -- in your earlier presentation on the research
6 program you talked about projects under way and fault
7 injection test methodology development that you had
8 done at UVA, and you talked about platform testing, if
9 I understand what you told me before and what you're
10 talking now, this was simply platform testing of its
11 operating system, but it had no application code,
12 which -- one of the major problems you have in any of
13 these software-based systems is not just the operating
14 system with which it's operating, but as well as the
15 programming of the application code in along -- you
16 know, so you utilize -- under that operating system.

17 So you didn't -- so this didn't even have
18 that type of stuff being done. This was strictly, from
19 what I gather, just operating system only testing.

20 MR. BIRLA: Now, let me clarify what that
21 was. That was testing, evaluating a method. It's
22 objective was not to evaluate the platform. A very
23 small configuration of the platform was used.

24 CHAIR BROWN: Okay, I've got that, but you
25 are only testing a subset of what that platform has to

NEAL R. GROSS

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

1 do.

2 MR. BIRLA: Right.

3 CCC ,I mean you've got all the stuff -- I
4 mean it's working with its own memory, it's working
5 with its own, built-in stuff that has already been
6 tested by a vendor, and doesn't include say, when you
7 have downloaded all the application code that is
8 necessary to process a plant, plant information,
9 that's not there, and its integration, or how it
10 coordinates with the operating system.

11 MR. BIRLA: That's not there and all the
12 inter-connections that you see with non-safety
13 systems, across redundant trains, across lines of
14 defense and between --

15 CHAIR BROWN: My point being is, that
16 those interfaces are part of the things you need to
17 test --

18 MR. BIRLA: Yes.

19 CHAIR BROWN: with the fault-injection
20 methodology, so concluding that the methodology is
21 good, bad or indifferent is really hampered by not
22 having a more system-level aspect. At least that's the
23 way I would -- I --

24 MR. BIRLA: Well, or conversely you can
25 say that the scope of what's being evaluated, the

NEAL R. GROSS

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

1 scope of the method, the scope of its applicability,
2 is not as wide as the real world needs, but still it
3 has some value, and with limited resources, you derive
4 the value you can.

5 CHAIR BROWN: Yes. Do you want to go on?
6 You're happy? Unhappy? We'll go on? Don't answer that
7 question.

8 (Laughter)

9 CHAIR BROWN: Go ahead.

10 MR. BIRLA: So this is the last slide on
11 the process itself, the expert judgement process. So
12 SRM on the expert-driven process says that as the
13 agency exercises this process, it will like to see
14 that documented what are we learning from each
15 exercise or each application of the process, so we are
16 going to document that.

17 So even though our work started before
18 this SRM came out, we believe it is exercising that
19 process for a regime that might not have been
20 contemplated at the time the SRM was written up, but
21 still we think it's valuable.

22 And you have seen the list of the three
23 projects on which -- which we have already identified
24 for application of such a process, customized to each
25 of those projects.

NEAL R. GROSS

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

1 So part of our theme here is -- part of
2 the process is you cannot just take a cookbook and run
3 through it. This has to be customized to the
4 situation. We did that for the purpose we had, but for
5 each one of these projects the purpose is going to
6 change and so the process has to be customized
7 accordingly.

8 CHAIR BROWN: Well, you just raised one of
9 the concerns we have with any type of automated
10 process, is they can become cookbook, in other words
11 people see the way it is, and they just apply it and
12 you reduce some of the --

13 MR. BIRLA: You are absolutely right. The
14 SRM says that within six months, the agency should
15 have a process that can be consistently applied. Now
16 the consistently applied could be interpreted as a
17 cookbook, and expert judgement by very nature is not
18 something you want a cookbook into.

19 CHAIR BROWN: Right.

20 MR. BIRLA: So part of the learning we are
21 going to report is that sort of stuff.

22 CHAIR BROWN: Okay.

23 MR. BIRLA: So, that was the value of
24 trying -- of taking up the time to reporting on the
25 process.

NEAL R. GROSS

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

1 Now, the main part.

2 (Laughter.)

3 CHAIR BROWN: I notice there's only two
4 slides on -- no, I'm just kidding. Oh, there is only
5 two slides.

6 MR. BIRLA: Well you have them in front of
7 you. They are very dense tables in there. I tried to
8 copy them in the PowerPoint slides, and it's not very
9 helpful to copy those tables in here.

10 CHAIR BROWN: What you're telling me is I
11 have got to have the electronic version open to click
12 on links. Is that what you are saying?

13 MR. BIRLA: Well, I see that Dr. Stetkar
14 has a copy. I think you have a copy of the RIL in
15 front of you.

16 CHAIR BROWN: Of the RIL --

17 MR. BIRLA: In fact you quoted from that.

18 CHAIR BROWN: Oh, I opened it up yes.

19 MR. BIRLA: Okay you have got the
20 electronic version.

21 CHAIR BROWN: Yes, I've got the electronic
22 version.

23 MR. BIRLA: I don't have that luxury, but
24 I do have a hard copy with me. So --

25 MEMBER SIEBER: That's the luxury.

NEAL R. GROSS

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

1 (Laughs)

2 MR. BIRLA: Okay, so you saw this list
3 earlier and let me just give you a little bit of the
4 background on the selection of these topics.
5 Verification is at the heart of what generates
6 evidence, based on which you evaluate a system, what
7 we call the product.

8 And so that was the first session or
9 segment in the clinic so that we could focus on what
10 is the state of the art today and what do you do when
11 there are uncertainties left in the verification
12 process, and how do you -- if you have different kinds
13 of verification activities, how do you put all the
14 evidence together in a meaningful manner. That leads
15 into the second topic.

16 And if you are using tool-automated
17 processes that will add additional issues or
18 uncertainties or unknowns, how do you integrate their
19 evaluation into the safety demonstration, and then
20 later on if there's a change, its effect.

21 So this is sort of the sequence in which
22 we laid it out. The fifth one, combined effect of
23 seemingly small defects, was a segment we put on the
24 table for the group because that idea, or that
25 observation, came from one expert and we needed to

NEAL R. GROSS

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

1 validate this through the group.

2 But it is germane to even the second topic
3 that you see there. So I am going to present it out of
4 sequence. I am going to present it before I go to the
5 safety demonstration framework

6 so a standardized template was laid out
7 for each of the five segments. The segment would be
8 kicked with a discussion-trigger, a question on
9 topic-specific uncertainty.

10 And then the second question would be
11 well, what is the evidence you need to reduce the
12 uncertainties you just identified? And if you can't
13 answer the question, why not. What are the knowledge
14 gaps? So that feeds into our research activities.

15 And lastly, the conclusions that you come
16 up with, how strongly do you believe in these
17 conclusions, the degree of validity. You assess that
18 and get back to us so that we don't have to.

19 So this was the template and the main
20 customization was the first question, the discussion-
21 trigger for each of the five segments. So let's see
22 how we exercised it on the V&V segment.

23 So the question we laid out was is the
24 complete V&V claimed credible in the context of the
25 kinds of systems we see in the nuclear domain. And the

NEAL R. GROSS

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

1 group right in the beginning said well, what does this
2 mean, there's a little ambiguity, but they eventually
3 rationalized that it is relevant to -- relative to
4 safety assurance, and if it is not, then what is the
5 additional evidence you need to reduce these
6 uncertainties, and if you can't answer that, then what
7 are the knowledge gaps. So this is the template we
8 followed.

9 So I'm going to show you a graphic version
10 of the outcome. So what you see in the red, which
11 looks pinkish here, or the major sources of
12 uncertainties are identified in the discussion.

13 So Luis in his presentation mentioned a
14 couple of them: assumptions about the environment;
15 correctness in terms of the requirements; incomplete
16 coverage; interference of one with another.

17 Just take one, what do you do to reduce
18 that source of uncertainties -- in this case it was
19 incomplete coverage -- so there are different
20 verification techniques, testing is only one, model
21 checking, analysis at different stages in the process.

22 So you perform different kinds of
23 verification techniques so that, given that you cannot
24 exhaustively test the whole space, you reduce the
25 amount of testing you have to do based on evidence

NEAL R. GROSS

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

1 generated in the other activities analysis model
2 checking and so on.

3 And they you integrate all this evidence
4 somehow, and that somehow is another research
5 question. Another observation was that make sure that
6 the different kinds of evidence you are generating is
7 complementary and there's some diversity in it, so
8 that if there is some uncertainty in one, we can cover
9 that with some results from another.

10 MEMBER STETKAR: But what do you mean by
11 coverage? I guess I'm --

12 MR. BIRLA: Well, let's just take the
13 testing example. So all the possible inputs going
14 through all the possible paths and all the possible
15 states in the system, if you could do that, that's
16 total coverage, so nobody can then --

17 MEMBER STETKAR: Okay I understand what
18 you are -- I just needed to get a context of what you
19 were talking about. Thanks.

20 MR. BIRLA: Another source of uncertainty:
21 interference. What do you do? Okay so there are some
22 ideas on proof of non-interference and it will show up
23 in the architectural conditions and criteria.

24 Then the environment and the requirements.
25 Similarly, generate evidence about them and integrate

NEAL R. GROSS

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

1 all that to make your assurance case or Safety
2 Evaluation Report.

3 So there's a table on the major sources of
4 uncertainties and there's a table on how you reduce
5 them in the V&V section of the RIL.

6 MEMBER STETKAR: Before you leave that,
7 the final desire for this is for it to have achieved,
8 based on your earlier comments, some level of safety
9 assurance, if you could use that for that as opposed
10 -- which you have -- you are not there yet, but I
11 mean, can you do that? Has anybody made an attempt to
12 say okay what are my acceptance criteria, I mean, when
13 somebody says oh I am assured -- I have a reasonable
14 feel that it's -- for the safety assurance, or the
15 assurance of safety of this design, or of the
16 software.

17 What -- do you have a set of criteria that
18 you look for?

19 MR. BIRLA: Meaning?

20 MEMBER STETKAR: Acceptance criteria. I
21 mean any time somebody says I've got all these -- how
22 do I know -- what is the basis on which I make a
23 judgement that I have gone through all the testing and
24 everything else, is there some metrics that you've got
25 laid out or have you thought about them? I mean

NEAL R. GROSS

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

1 typically you have to have acceptance criteria for
2 something, if you're doing --

3 MR. BIRLA: You're meaning the agency?

4 MEMBER STETKAR: Yes, the agency in this
5 case.

6 MR. BIRLA: Okay, in our current practice?

7 MEMBER STETKAR: Yes.

8 MR. BIRLA: Okay. The SRP lays out a whole
9 bunch of criteria and references, IEEE 1012 for
10 verification and validation --

11 MEMBER STETKAR: If they run that process,
12 you're happy?

13 MR. BIRLA: Well, the agency does an
14 audit, which is a sampling, and that's the current
15 state. Now --

16 MEMBER STETKAR: I haven't read 12 -- you
17 said 1210?

18 MR. BIRLA: 1012.

19 MEMBER STETKAR: 1012, I'm sorry.

20 MR. BIRLA: That's process-oriented. It
21 doesn't lay out the --

22 MEMBER STETKAR: That's I what I thought.
23 Just about all that I've ever looked at are process-
24 oriented so --

25 MR. BIRLA: So your question is are you

NEAL R. GROSS

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

1 happy. Now remember, these things were laid out years
2 ago, and systems are getting more complex. Should we
3 take a look at whether they are adequate, and that's
4 part of our research.

5 MEMBER STETKAR: Well how about problems
6 found? I mean, you know, you are running your
7 automated tool and it identifies a problem, more and
8 more and more and more and more and more and you
9 correct and correct and correct and correct and
10 correct and you've got some time frame in which you
11 are doing it, and at least 20 years ago, when we asked
12 this question, or more, the idea was well, we'll show
13 you a curve nad we get lots of errors we find and we
14 get those corrected in the beginning, and then it kind
15 of asymptotically approaches a lower number but you
16 are always finding errors, and that was the answer
17 that was given to us 25 years ago.

18 So I mean, ask Bill Gates. Do they ever
19 have software that doesn't have errors on it, and the
20 answer to that is no. so

21 So I mean, I'm -- how long do you test
22 before you are comfortable that -- if say all of a
23 sudden you've now tested for a week and a half and
24 you've shown no errors have come up, in addition to
25 the 247,000 you have found before, that's -- it's a

NEAL R. GROSS

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

1 metric. Whether it's a good metric or a bad metric,
2 it's a metric.

3 So that's what I was looking -- that's the
4 kind of thought process, I was just relating back to
5 past experience of the answers we got and the answer
6 we got was well, you are never -- there's always other
7 errors, we just haven't tested long enough to find
8 them or had put in the conditions, coverage, to ensure
9 that they are all identified so that's --

10 MR. BIRLA: But the more important
11 question is, if you look at the pink blocks, there are
12 three of the blocks, so in your -- even if you were to
13 go for 100 percent coverage, your coverage would only
14 cover your test cases that you identified.

15 But if you didn't even identify the right
16 test cases, you missed the boat. So that's the bigger
17 part of the message here. So then what do you do? Go
18 in a real plant and under real-life conditions test
19 for 100 years? That's not realistic either.

20 MEMBER STETKAR: Absolutely not.

21 MR. BIRLA: So you had in Luis's and
22 Russ's presentation you had this idea you had some
23 discussion with him on the emulator, simulator and you
24 have to simulate the old plant, you had to have a
25 plant model, you had to discuss those kinds of ideas.

NEAL R. GROSS

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

1 Yes --

2 MEMBER STETKAR: That seems to be the
3 direction that the folks over in the PRA camp if I can
4 characterize them in that way, are headed.

5 MR. BIRLA: Yes, so when you see --

6 CHAIR BROWN: How did you phrase -- how
7 did you think of what he said in terms of the PRA --

8 MEMBER STETKAR: No, I said, you know,
9 what Sushil mentioned is that the presentations that
10 we have heard from the work that is going on in
11 Brookhaven seemed to be focusing on more extensive use
12 of -- simulation of the real, the use of the real
13 software and hardware integrated with plant-response
14 models like, you know, TRACE or something like that,
15 to generate input signals to look at -- look for
16 potential failures.

17 That seems to be the path that they are
18 headed on. This is a different approach.

19 MR. BIRLA: Yes, so for the purpose
20 assurance, the main message here is that besides this
21 coverage, they've got three other blocks, or sources
22 of issues, uncertainties, or unknowns, that are not
23 being adequately addressed in the experience of other
24 application domains.

25 And I am sure if you were to talk to

NEAL R. GROSS

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

1 people in the FAA world you would hear horror stories
2 of this sort, hear the same thing from JPL people, the
3 same thing from the medical devices people.

4 So you need to do something better than
5 testing or more than testing, and that's what this big
6 block of coverage evidence talks about, but it is not
7 enough.

8 Even in the modeled world, the simulation
9 world, there's one similarity with testing, and that
10 is you can only reveal defects. You cannot guarantee
11 the absence of defects.

12 So, simulation is just making that process
13 faster with the use of a computer. It doesn't really
14 answer everything. So there is a human, again,
15 quality, expert judgement process element of it that
16 comes into the picture in addressing some of the other
17 blocks, and it shows up in recommendations later on.

18 So coming back to your question, just to
19 sum up, if you just focused on the question how much
20 testing is enough, that's not addressing the bigger
21 source of worry.

22 We have one data point from the clinic
23 relative to your question. And that is the experience
24 of naval reactors. So I didn't mention this earlier,
25 but in the clinic, as active observers, we had two

NEAL R. GROSS

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

1 people from naval reactors and one from the FDA, and
2 both of them from the naval reactors said that the
3 amount of effort we spent in verification, which
4 includes testing, is nine times what we spent in the
5 rest of the development process.

6 And this is after everything they do in
7 standardization of platforms and in limiting
8 complexity and in not having all these inter-
9 connections, that's where they are.

10 CHAIR BROWN: Yes, good idea.

11 MR. BIRLA: Now, so that's a data point we
12 have to cause us to worry, cause us to think about
13 this adequacy question. Now the answer is not you go
14 do nine times, but we need to probe a little bit
15 deeper. Why is it taking this much and what can be
16 done to get the same level of assurance?

17 So, simplistically, my question is look,
18 they are part of America, their safety concerns are
19 like everybody else's. if they found it necessary we
20 should listen, we should understand why they found it
21 necessary. How can we get a comparable level of
22 assurance?

23 CHAIR BROWN: There's an additional piece
24 of that which you didn't mention, but yes, we did it
25 a long, long, long time, with very detailed,

NEAL R. GROSS

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

1 integrated, exact replicas of the plant in terms of
2 the modeling and the inputs, and the test setups,
3 mockups, full-scale, was that after all that, even all
4 the testing, we put in a backup system because we
5 didn't trust it, that we'd catch everything.

6 So we had a backup system that was analog
7 to catch certain -- you know just to shut the plant
8 down, stuff like that. So that's kind of a conclusion.

9 I am listening and unfortunately I draw
10 conclusions when I listen to these types things.

11 MR. BIRLA: Yes, so as part of our
12 knowledge team learning from other organizations, one
13 of the targeted organizations is naval reactors. Dan,
14 where are you? I think he left the room. But he's our
15 interface. He's the agency's interface to get some
16 more understanding of what is the level of assurance
17 they see why -- why did they have to apply this kind
18 of effort, how can we do better.

19 CHAIR BROWN: Okay, no, it's nice to hear
20 that you had them onboard at least as part of the --
21 provide their input.

22 MR. BIRLA: Yes, so this is about as much
23 as I want to say because I was asked that they not be
24 quoted.

25 CHAIR BROWN: Yes.

1 MR. BIRLA: So even if we learn later on
2 I will probably in the future not be in a position to
3 say as much as I said today. What I said today is on
4 the record because they spoke it in the group. It's
5 part of our transcripts, but they would rather not be
6 quoted.

7 So this topic is about the combined effect
8 of a lot of the seemingly small things that could
9 result in some real serious mishap. The proposition
10 came from -- the concern came from Dr. Gerard Holzmann
11 of JPL. He leads the lab for software reliability
12 there.

13 And he cites Perrow's work. This is a book
14 named Accidents, and Perrow cites many examples of how
15 a lot of seemingly small, insignificant deviations
16 came together to cause a serious accident, and Three
17 Mile Island is one example he discusses in the book.

18 MEMBER STETKAR: Three Mile Island by the
19 way is a classic example of a software system, when
20 you translated that into a human being processing
21 information in the way they were trained to process
22 the information, and reacting perfectly to the way
23 they were trained to process the information, in other
24 words shutting off injection because they knw the
25 pressurizer was going water-solid, the same was as a

NEAL R. GROSS

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

1 software system might respond, precisely, to that
2 condition because the software knew that they were not
3 supposed to drive the --

4 So it's, although you might say it's an
5 accumulation of a lot of very small, complex things,
6 there are analogies here.

7 MR. BIRLA: Exactly.

8 MEMBER STETKAR: And there are ways -- in
9 fact we have learned from looking at human responses,
10 there are ways to characterize those things if you
11 pull back from the detail. That's just another kind of
12 nudge in the direction of this pulling back from the
13 detail.

14 MR. BIRLA: So historically what we do in
15 our review process is that we -- whether you call them
16 criteria or clauses or requirements -- we take each
17 one, and see if the application is meeting this
18 requirement or condition by itself, and make an
19 evaluation, we see some very minor deviations, say
20 gee, this is insignificant and we let it go.

21 Now you have a whole bunch of these that
22 you let go as individually insignificant, but your
23 mental model was that they were independent.

24 MEMBER STETKAR: Right.

25 MR. BIRLA: So this was a wake-up call, we

NEAL R. GROSS

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

1 put it in the clinic for discussion, and the
2 triggering question was well, given that these things
3 have happened in real life, and caused real-life
4 accidents, is the likelihood more in software, and if
5 so, what can we do to reduce this likelihood, and if
6 we can't answer that question, what are the knowledge
7 gaps, and so on.

8 Well, Dr. Gerard Holzmann was the one who
9 made the proposition and immediately he challenged our
10 question. He says why are you asking that likelihood
11 is more in software? It's not a matter of software
12 versus hardware. It's a matter of complexity of the
13 system.

14 So he changed the word software to complex
15 systems and then they proceeded with their discussion.

16 Well it turns out that the discussion
17 didn't go very far because Dr. Holzmann asked the
18 other experts, well, have you -- any of you had any
19 similar experience in your life, in your career, in
20 your work?

21 Well, he obviously did in his work in the
22 software, in the lab for software reliability. But
23 none of the other experts had this kind of an
24 experience, so we rated the degree of strength of
25 validation of the original proposition as low.

NEAL R. GROSS

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

1 So then Dr. Holzmann wrote the conclusion
2 that well, the conclusion then is that we need more
3 research in this area and all of us and everybody said
4 yes.

5 So that conclusion got a high concurrence.
6 So this is an example of how the process got exercise.
7 We never really had polarization. They just changed
8 the scope to what they could agree upon.

9 MEMBER STETKAR: The researchers can
10 always agree that more research is needed.

11 (Laughter)

12 MEMBER STETKAR: It's pretty easy to get
13 consensus on that one.

14 MR. BIRLA: Well, there are opinionated
15 researchers who feel they have the answer and we were
16 fortunate that we didn't get one of those in the
17 clinic.

18 Dr. Holzmann still feels very strongly
19 that this is the case and this is something you need
20 to be concerned about, and until you can address this,
21 you need to have diverse, alternative backups or
22 whatever you want to call them.

23 CHAIR BROWN: Well, intuitively, the
24 thought process makes sense. The more complex your
25 software system, the more likely you are to have small

NEAL R. GROSS

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

1 defects that you don't necessarily find. I mean -- at
2 least in my limited intelligence, intuitive thought
3 processes, I would kind of conclude the same way he
4 did. The more lines -- if I have got a million lines
5 of code, I have got more likelihood of having small
6 defects than I have got 10,000.

7 MR. BIRLA: Burt when you run the
8 probabilistic method in a traditional, typical manner,
9 and you say each individually has close to zero
10 probability --

11 MEMBER STETKAR: You know, that's exactly
12 -- let me stop you right there. That's exactly the
13 problem. Running the, what you are calling the
14 traditional, probabilistic manner, in a -- there is no
15 applicable traditional, probabilistic manner. So any
16 reference to that is pretty much irrelevant. So we
17 will --

18 MR. BIRLA: But that's still what people
19 end up doing.

20 MEMBER STETKAR: I don't care what people
21 end up doing right now.

22 (Laughter)

23 MEMBER STETKAR: I would like to
24 understand -- you know I don't care how people did it
25 wrong in the past.

NEAL R. GROSS

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

1 (Laughter.)

2 MEMBER STETKAR: Thirty years ago I saw
3 people trying to evaluate electrical systems by doing
4 a piece-part count you know, which was also the wrong
5 way to evaluate electrical or control systems. That's
6 the way people did it.

7 We have learned that that was the wrong
8 way to do it. So I think what we are struggling with
9 here is recognizing that it's not been done very well
10 in the past, either from predicting likelihood of
11 occurrence, what are the key attributes of software
12 systems. Is it complexity? Is that a key attribute? We
13 honestly don't know. But simply because saying that
14 people have counted up, you know, large numbers of --
15 whether it's lines of code or whatever in the past and
16 said you know, we can assign a nominal probability
17 that there will be an error in each line of code and
18 a million of codes have a million more you know, a
19 million times higher likelihood of having an error in
20 it than one line of code, may not be the right
21 context.

22 So that's kind of the challenge of where
23 we are.

24 MR. BIRLA: Yes, so intuitively, I --

25 MEMBER STETKAR: I mean it sounds right,

NEAL R. GROSS

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

1 but indeed it might not be correct.

2 CHAIR BROWN: Well, instead of speaking
3 theoretically, we had a particular system that had x
4 number of channels and those two channels were
5 required for startups, and there was a trip function
6 associated with those channels, only needed one, and
7 every -- so that the most reliable place I wanted to
8 see our plants was operating. I hated to have them
9 shut down and trying to start up.

10 And I went to my first boss after I became
11 in charge of the group, because I got tired of
12 processing the reports that I had to deal with about
13 why the ships were having difficulties with the x
14 number of channels that we had.

15 And he threw me out of the office and said
16 we will never put any more of those, they are the --
17 the more stuff you put in, the worse you are. Well I
18 tried to explain to him that the new systems that we
19 were putting in were micro-electronics, you know,
20 chips, you know, solid-state stuff, not vacuum tubes
21 or just straight transistors, and he threw me out.

22
23 Well, when a new boss came in and I showed
24 him we went -- we doubled the amount of channels, in
25 other words, twice the amount of hardware well

NEAL R. GROSS

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

1 actually far more than twice the amount of hardware,
2 because of the number of chips we were using, and I
3 never had a plant that I couldn't start up.

4 MEMBER STETKAR: And if you did a two to
5 the n type of complexity, the number of possible
6 complications or failures --

7 CHAIR BROWN: Ultimately more complex.

8 MEMBER STETKAR: there were probably
9 billions and billions more complexity.

10 CHAIR BROWN: Yes, ways to fail, and it
11 did.

12 MEMBER STETKAR: But it worked a lot
13 better.

14 CHAIR BROWN: Not just a lot better, I
15 mean it just virtually eliminated all the time spent
16 and the plants were easily started up in some fairly
17 interesting situations where they needed to get back
18 online.

19 So I agree, just, on software, it's a
20 little bit different than that. It's not exactly the
21 same as hardware but you have got to be careful on the
22 generalizations.

23 MR. BIRLA: But people try to do similar
24 things. In hardware it was piece count and in software
25 they do lines of code, which is not right.

NEAL R. GROSS

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

1 MEMBER SIEBER: But there is a basic
2 fundamental difference you know. Hardware wears out
3 and when it does, it fails, so it's easy to assign a
4 probability.

5 But a software defect is a latent failure
6 ready to happen not based on things wearing out but
7 based on hitting the right circumstances, and so it's
8 much more difficult to assign a probability to that on
9 a rational basis.

10 CHAIR BROWN: here is, but there are
11 analogies in hardware failures. I know of a plant that
12 shall remain unnamed that had five valves fail to
13 open. They were tested regularly, monthly throughout
14 the plant's life, it was operating for quite a while.

15 They failed to open under an actual demand
16 because nobody had ever tested under the actual
17 differential pressures that they would see, and they
18 found out that the designers had designed the motors
19 too small.

20 Now that's a design problem that resulted
21 in a common cause failure of five valves that existed
22 for many years in a plant. So any of the analogies
23 that you draw between latent, undiscovered failures
24 that come in through the design process, I can give
25 you examples from hardware that are directly

NEAL R. GROSS

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

1 analogous. You can't thing of a problem that I haven't
2 seen in the hardware space.

3 MEMBER SIEBER: On the other hand it would
4 be difficult to look at that valve with a superficial
5 analysis --

6 MEMBER STETKAR: That's right.

7 MEMBER SIEBER: and determine a failure
8 possibility.

9 MEMBER STETKAR: On the other hand you
10 could actually question, has that valve ever been
11 tested under the actual operating conditions that you
12 would see during an accident and if the answer is no,
13 you might say might you do that.

14 MEMBER SIEBER: And the example you are
15 citing is not the only one I have heard.

16 MEMBER STETKAR: No, no, that's just one
17 that came to mind quickly. So --

18 MR. BIRLA: But you could take that
19 discussion further and say, well, were the operating
20 conditions properly understood and transformed into
21 the requirements specifications, why wait until
22 testing?

23 MEMBER STETKAR: The -- well, yes, the --
24 I don't know the root cause of the reason why the
25 motor was too small. I have no idea, you know, the

NEAL R. GROSS

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

1 records were lost, I don't know. The people who did
2 the accident analysis said it had to operate under a
3 certain -- the fundamental point is I don't
4 necessarily care about all of that fine structure
5 detail, about why we eventually got to the point where
6 the valves didn't open.

7 There Indeed was a design deficiency that
8 was manifested in the fact when the valves were
9 required to open, they didn't, and there might have
10 been a test protocol that would have discovered that
11 at some time or another, but nobody ever asked that
12 question, and that's part of kind of systematic
13 evaluation of the types of things that can occur and
14 how you might either check for them you know, if you
15 determine how important they are quantitatively, or
16 develop qualitative ways to ask the right questions of
17 -- whether it's the design process or a V&V process,
18 you know, would be the analogy here, in the software
19 life cycle.

20 MR. BIRLA: Yes, the analogy I was trying
21 to take from your example to the software side was
22 that if you just focus on test protocols missing, you
23 can't have enough of them.

24 So you really have to catch the problem at
25 the early stage in the life cycle. Operating

NEAL R. GROSS

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

1 conditions should be properly understood. Worst case,
2 or corresponding cases could have transformed into
3 requirement specifications, then you are sure you are
4 going to have a test case corresponding to that
5 specification.

6 And if you have designed to that
7 specification, you will need less testing anyway. So
8 --

9 MEMBER STETKAR: Anyway, we are going to
10 run short on time here.

11 MR. BIRLA: Yes, so that is a big issue on
12 the software side. Another way of addressing that
13 testing question you asked, how much is enough.

14 Well to start with we need to have
15 preventive approaches, what IRSN, Luis referred to as
16 development assurance, they used that term. In other
17 words, assurance development process itself.

18 Given that it is going to be a function of
19 some design defect, why even let the design defect go,
20 or worse yet, requirements missing.

21 CHAIR BROWN: Okay, you can turn the page
22 now.

23 MR. BIRLA: This is a pictorial
24 representation of the issue you are faced with trying
25 to integrate the effect of these uncertainties, given

NEAL R. GROSS

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

1 the discussion that individually, each one could be
2 dismissed as insignificant, but they all come together
3 in so many different ways.

4 But what are the major sources? At the
5 system level, again requirements in architecture, if
6 you miss something there, the only place you are going
7 to catch it is at the final acceptance test when the
8 system is integrated.

9 Then inbetween, on the software side, the
10 life cycle requirements architecture, default design,
11 unit testing, integrated testing.

12 The size of -- this question mark
13 represents the unknown, the degree of uncertainty.
14 Size represents a relative uncertainty. Again you can
15 see that the bigger contribution -- well let me
16 preface myself.

17 In the context of a high-quality process
18 executed by a high-performance organization,
19 conforming to the Appendix A and the NRC regulatory
20 guidance and good, decent practice, what you are going
21 to find is that very little contribution to this
22 uncertainty from unit test, unit test meaning unit
23 components and small components, but much bigger from
24 requirements and architectural issues, relative sizing
25 roughly speaking.

NEAL R. GROSS

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

1 But the point is there are so many sources
2 that have to be integrated, and if you are going to
3 start dismissing what seems to be an individual, in
4 each individual case, something insignificant, beware.
5 And then you add the effect of change that adds even
6 more uncertainties.

7 And so this leads us into needing a more
8 systematized way of integrating the effect of all
9 these uncertainties. We label this segment of the
10 clinic as a safety demonstration principle discussion,
11 generally it's been known as an assurance case or
12 safety case. Deliberately avoided the term safety case
13 because it carries some baggage.

14 So the triggering question was how to
15 evaluate, integrate the effect of all the
16 uncertainties. What's meant by the safety
17 demonstration bit of a definition of information here,
18 structured argument, integrating complementary
19 evidence items, it shows that the safety goals are met
20 and shows how the uncertainties have been dealt with.

21 In other words, an uncertainty from one
22 area has been compensated for, covered by some
23 evidence from some other area and so on.

24 But at least it makes all the known
25 uncertainties explicit in how you have provided for

NEAL R. GROSS

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

1 them.

2 So this is the same model that you saw
3 earlier, so I won't go over it again, but this is the
4 argument structure underlying a safety case or an
5 assurance case. Do you want to ask something?

6 MEMBER STETKAR: Did any of your experts
7 indicate that this sort of structured thought process,
8 or information processing methodology or however you
9 want to characterize it, is actually implemented in
10 any of their experience, or is this something that has
11 evolved out of this exercise that you are in -- you
12 have in progress?

13 MR. BIRLA: Four of the experts out of 10
14 have actually --

15 MEMBER STETKAR: Implemented this type of
16 -- okay.

17 MR. BIRLA: worked with projects where a
18 safety case was applied, but there was a fifth expert
19 who was not in the clinic who -- Chris Johnson from
20 the UK -- who pointed us to a downside in the Nimrod
21 report.

22 And the downside in the Nimrod report is
23 that if you do the goal-structured notation type
24 safety case or something as rigid as that, you end up
25 with thousands of pages of a safety case which is very

NEAL R. GROSS

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

1 difficult to follow, and people typically use it as a
2 boilerplate to meet the UK's legal requirements, but
3 nobody ever looks at it afterwards, so that's useless.

4 And then the Nimrod report makes the same
5 statement for FMEAs and for --

6 MEMBER STETKAR: And occasionally they
7 lose them too, but that's --

8 MR. BIRLA: So we --

9 MEMBER STETKAR: But I was thinking about
10 this thought process, I mean, this sort of organized
11 thought process, whether people have applied it with
12 some degree of rigor and documentation.

13 MR. BIRLA: That last part is the part
14 that's lacking.

15 MEMBER STETKAR: Okay. Thanks.

16 MR. BIRLA: So if you document this, this
17 becomes very rich and very useful.

18 MEMBER STETKAR: Exactly, yes.

19 MR. BIRLA: But that's the part that's
20 lacking. So the outcomes. So you need the argument
21 structure that you just saw, but you also need good
22 evidence and the evidence should be complementary,
23 diversely redundant. This is in the context of what do
24 you do about the uncertainties, so the redundant
25 evidence is one approach to it.

NEAL R. GROSS

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

1 Yes, there were gaps in knowledge,
2 mathematical, logic-based arguments not always
3 feasible so that's the weakness of the goal-structured
4 notation.

5 The recommendation was, besides the
6 mathematical ideas, you integrate techniques from
7 other disciplines -- philosophy, law, linguistics --
8 and the degree of agreement was high.

9 Now move to the topic on tool-automated,
10 tool-assisted processes. So, Chairman Brown mentioned
11 that this presentation on the RIL part is very thin,
12 so I said well, let me see how we can make it thick,
13 so I did try to copy the table, got all eight rows but
14 I had to edit the descriptions a little bit.

15 You are better off reading the RIL itself
16 but this gives you an idea of the limitations. If you
17 want to spend time on it, we can go through it, if you
18 don't, we can move on.

19 CHAIR BROWN: Yes, that is not in here.

20 MR. BIRLA: Okay.

21 CHAIR BROWN: That's in the --

22 MEMBER REMPE: The electronic version.

23 MS. ANTONESCU: The back-ups.

24 CHAIR BROWN: Oh, it's in the back-ups?

25 MR. BIRLA: That's slide number -- that

NEAL R. GROSS

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

1 was slide 64.

2 MEMBER REMPE: It is in the electronic
3 version.

4 CHAIR BROWN: I got it. Okay.

5 MR. BIRLA: Okay, so this was a project
6 already in the research plan, and the results of the
7 clinic feed into that research project. The last topic
8 here is change impact analysis. We do have a -- at
9 least on paper -- a slot for a research project, but
10 haven't really started activities on it.

11 Again, in terms of sources of uncertainty,
12 section 6 of the RIL, particularly Table 5, and what
13 do you do to reduce these sources of uncertainties,
14 Table 6 in the RIL.

15 To make this change impact analysis
16 feasible, you need a very good quality architecture.
17 You need to understand all the dependencies, and so
18 that aspect shows up in the architecture area.

19 So if you look at the architecture section
20 in the appendix you will see conditions there.

21 CHAIR BROWN: I'm not doubting that,
22 without even looking at it, that it's -- change impact
23 is almost impossible so unless you have the whole
24 thing, what you are looking at is the whole integrated
25 system, it's kind of hard to assess impact of

NEAL R. GROSS

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

1 anything.

2 That's fundamentally what you are saying.
3 You have to look at the architecture to see that.

4 MR. BIRLA: You need that and -- although
5 the experts didn't say that, I am also personally of
6 the belief that you also need to look at the process.
7 If anything had changed in the process -- I'm not
8 talking about development process of the system, but
9 process in the environment.

10 So it's a challenging area. The experts
11 recognize that, and in the NRC's case, we have a
12 topical report on change process but there's a lot of
13 depth you need before you can say that look, if this
14 piece has changed, then its impact -- it will have no
15 impact on everything else.

16 CHAIR BROWN: Well, another aspect of the
17 change impact is if you don't have a real good
18 configuration control process, so that you know what
19 you are changing, then you have more difficulty also.

20 MR. BIRLA: Right, right. So --

21 CHAIR BROWN: And I would have thrown that
22 in here in terms of -- well, architecture -- you have
23 got to maintain both the software and the hardware
24 architecture, good configuration control, otherwise
25 they determine your change impact is --

NEAL R. GROSS

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

1 MR. BIRLA: So that's baseline, so if you
2 look at the appendix you will see all those conditions
3 in there -- change control process, configuration
4 management process, and so on.

5 But even with all that, it's a challenge.
6 So those were the five topics that were structured
7 sections but there were certain threads running
8 through the individual elicitations as well as the
9 discussions on those five topics, in two broad areas
10 -- validated requirements, and the other is
11 architecture.

12 So the RIL has a couple of sections
13 devoted to that, and the topic of complexity and
14 freedom of interference and architecture show the
15 present area of concern.

16 So again, this is the second-to-last
17 wrap-up slide, two work products have been reviewed
18 today. The other two are in the works.

19 CHAIR BROWN: Two and three, RIL two and
20 three are the ones in the works, right?

21 MR. BIRLA: Yes, yes.

22 CHAIR BROWN: Okay.

23 MR. BIRLA: So at the time we held a
24 clinic, we had conceived of those three RILs being the
25 vehicles to capture the results of the clinic and

NEAL R. GROSS

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

1 transmitting those results to the licensing offices.

2 But since then, this opportunity for the
3 IRSN collaboration came in, so we interjected that as
4 part of the relevant information.

5 CHAIR BROWN: For the what -- my brain was
6 thinking something else as you were saying this.
7 Opportunity for the what, or this other --

8 MR. BIRLA: The collaborative activity
9 with IRSN from France, that was reported on earlier --

10 CHAIR BROWN: Oh, okay. All right. All
11 right.

12 MR. BIRLA: which is relevant to the same
13 topics. And we have also decided that in the second
14 RIL, we will add content beyond what we heard from the
15 experts in this clinic.

16 In other words, we are looking for what I
17 had termed earlier the contrarian viewpoints, or any
18 other pieces of information, if you have any
19 suggestions, we will work those suggestions, follow up
20 on the papers or on the people with the experience,
21 and interview them, particularly people with
22 industrial experience.

23 We have identified two. One's at the --
24 the individual is not available until later in the
25 year, and the other was moving from Indiana to

NEAL R. GROSS

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

1 California, not available for interviewing at that
2 time.

3 But two who have done work in industry
4 using FMEAs, FTAs, hazard analysis, that we would like
5 to interview and --

6 CHAIR BROWN: The FTA is a fault tree
7 analysis?

8 MR. BIRLA: Yes.

9 CHAIR BROWN: Okay. Make sure I got that
10 right.

11 MR. BIRLA: But if there are any others
12 that anyone can suggest, we would be very interested
13 in interviewing the people, exactly what did they do,
14 how did they apply, what utility they got out of it
15 and so on.

16 CHAIR BROWN: Did Dennis say -- he had
17 something, didn't he?

18 MR. BIRLA: He had one paper --

19 MEMBER STETKAR: We have some stuff.

20 CHAIR BROWN: Okay, yes, because I am not
21 in that loop, so --

22 MR. BIRLA: So to -- Luis gave you a
23 timing of about six months on the second RIL to be
24 able to include the new information in the second RIL,
25 when we need it pretty quickly.

NEAL R. GROSS

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

1 CHAIR BROWN: How far down the line is RIL
2 three?

3 MR. BIRLA: Another six months, Luis's
4 estimate there. That's at the level of the first RIL
5 that you see, now I'm hoping to find a way to get it
6 at least in a draft review mode to the licensing
7 offices sooner. ut I'd like to talk to Luis and our
8 other team members on that.

9 Okay, so that wraps up my part.

10 CHAIR BROWN: Okay, now these -- in both
11 of these I was -- I did a quick look through the
12 matrix, and I was trying to identify, there's a couple
13 of items in there that if you will correct me, I think
14 one of them was the software safety demonstration
15 somewhere, the V-06064 and I know there's V-06 -- V-
16 6025 I believe which was tool automation and
17 assessments etcetera.

18 So these fall under those categories I
19 guess in terms of projects or those were the projects
20 I guess, whatever.

21 MR. BIRLA: I think we have a V number JCN
22 too on there too -- on the change --

23 CHAIR BROWN: Change impact?

24 MR. SYDNOR: Yes, I think it's in the --
25 this is Russ Sydnor -- for budgeting purposes, I

NEAL R. GROSS

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

1 created some JCNs which are really a budgeting --

2 CHAIR BROWN: I just use those as the --
3 that's kind of the one, two, three, four --

4 MR. SYDNOR: I'll give you that
5 correlation.

6 CHAIR BROWN: on the left-hand side of the
7 page.

8 MR. SYDNOR: I'll be submitting that
9 correlation.

10 CHAIR BROWN: Okay, the stuff we talked
11 about and things like that --

12 MR. SYDNOR: Don't spend your valuable
13 time on trying to correlate budget numbers on this.

14 CHAIR BROWN: I was using words to do it.
15 I went to the next column. Okay any other questions on
16 this? Jack? John? Joy?

17 (No response)

18 CHAIR BROWN: Thank you very much.

19 MR. BIRLA: Thank you for the interaction.

20 CHAIR BROWN: Good discussion, good
21 presentation and I think a challenging interaction
22 here with the Q&A and the back and forth. It's very
23 good.

24 MR. BIRLA: I enjoyed it very much. Thank
25 you.

NEAL R. GROSS

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

1 CHAIR BROWN: I enjoyed it -- well done.

2 MR. BIRLA: Thank you very much.

3 CHAIR BROWN: Well we are right now at a
4 time for --

5 MEMBER STETKAR: Lunch.

6 (Laughter)

7 CHAIR BROWN: John, I can't work on that
8 for you, okay? We are now five minutes ahead of
9 schedule, which is absolutely amazing, thanks to
10 Sushil's crisp presentation.

11 And we will take a 10-, 15-minute break as
12 scheduled and we will resume --

13 MEMBER STETKAR: Just bang your gavel.

14 (Bangs gavel, laughter)

15 CHAIR BROWN: 2:45, no excuse me, 2:40. I
16 don't want to give you guys any more time than you
17 possibly are going to get.

18 (Whereupon the above-entitled
19 matter went off the record at
20 2:24 p.m. and back on the
21 record at 2:45 p.m.)

22 CHAIR BROWN: We are now un-recessed
23 again. We will proceed. And now we have got Karl for
24 the learning digital operating experience.

25 MR. STURZEBECKER: Yes.

NEAL R. GROSS

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

1 CHAIR BROWN: All right?

2 MR. STURZEBECKER: Yes.

3 CHAIR BROWN: And we are one minute behind
4 schedule again, thanks to Coke and Pepsi discussions.

5 MR. STURZEBECKER: Good afternoon. Nice to
6 see everyone. I am Karl Sturzebecher. I am the lead
7 for the OpE team, and I am going to be talking about
8 learning from digital operating experience.

9 And part of my team is here -- or all my
10 team members: Derek Halverson, Dr. Derek Halverson in
11 the back there; Tom Burton; and Luis Betancourt right
12 there.

13 So we work together on specific projects
14 and we come together once a week and go through
15 operating experience and I will continue from here.

16 This is my outline. I am going to start
17 off with a little background, what's the motivation
18 for the team, then go through a little bit of a mind
19 map to explain what we are doing with the different
20 areas we are looking into, and extend into the
21 collaborative efforts, international, domestic and
22 non-nuclear.

23 I am going to skip tools and methods
24 because I think we have talked about and discuss a
25 little bit about the framing process, where -- what we

NEAL R. GROSS

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

1 are trying to build from what we have learned at this
2 point, and then a path forward.

3 CHAIR BROWN: Is -- just to make sure --
4 it this on your all' research list, or is this a
5 related subject?

6 MR. SYDNOR: No, it is in the research
7 list.

8 CHAIR BROWN: Oh it is?

9 MR. SYDNOR: Yes, and we do have a project
10 to support it. Right now we are using mostly in-house
11 resources, but there is a project on the list --

12 CHAIR BROWN: Oh, I see it okay.

13 MR. SYDNOR: to support it should we need
14 some external help.

15 CHAIR BROWN: Okay thank you, I have found
16 it.

17 MR. STURZEBECKER: Background. There's an
18 SRM from 2007 that asks us to continue forward with
19 this idea of inventory and classification, and how it
20 relates to digital systems for nuclear power plants.

21 There's also a second part to that, which
22 is evaluate the OpE and how it relates to nuclear
23 power plants and other type of industries, and to
24 extend into looking for failure modes and mechanisms
25 that go with this operating experience.

NEAL R. GROSS

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

1 In 2009, if you recall, there was,
2 probably the last time, I think, from my knowledge,
3 that OpE was discussed with the ACRS Subcommittee and
4 that was over the EPRI report, operating experience,
5 insights on common cause failures and digital
6 instrumentation control systems.

7 And I would say the interim conclusion
8 from that was there wasn't enough events really to
9 substantiate yes or no about a common cause software
10 at the time.

11 The other thing that came out from that
12 meeting was the LERs. They are difficult to pull
13 information from, and we'll talk about that later. And
14 then third is the -- I like the quote there that we
15 picked up, that you know, the categories need to be
16 flushed out and you know, what's also associated with
17 the architecture. That was also -- came out of that
18 discussion.

19 So you sum all that up and we come to the
20 third bullet, which is our research plan and this is
21 3.4.5, operating experience analysis, and what we were
22 trying to produce for product would be in the realm of
23 can we provide a failure framework with the type of
24 events we are looking at , and how do we categorize
25 them, and just what can we learn from these these OpE,

NEAL R. GROSS

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

1 these OpE's experiences that we can improve in
2 guidance, and eventually -- that's part of the lessons
3 learned that we are trying to shoot for.

4 So the team got together and created this,
5 which we displayed at the RIC, this past March. This
6 is a mind map. It's a little bit in the reverse
7 because it's pointing back towards the center.

8 But it typically -- I'm not sure if you
9 are familiar with mind maps, what they do, it's a way
10 of putting the different areas we are looking into in
11 one big overview, and it's a great brainstorming tool,
12 a way that people can be creative and think of other
13 options that we are not looking at.

14 There's not really a process orientated
15 with this, and this tool here is something we will
16 always be continuously updating, or you just simply
17 orphan it at the end of the project.

18 So I am going to step through the
19 international efforts, the domestic leg, and the non-
20 nuclear leg. In the international efforts, we have
21 some conversations going on with the Canadians right
22 now. It's just started. We are hoping to get some
23 operational feedback, information from them. NRR is
24 taking the lead on this, the DI&C activities there,
25 INER, which is from the Republic of Taiwan, we have

NEAL R. GROSS

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

1 established an OpE research collaborative there, I
2 think we are going to get maybe eight events from
3 them.

4 Dr Huang is also one of the steering
5 committee members from COMPSIS. IRSN, which we have
6 heard earlier. We are hoping to get some EDF points or
7 events from them, through IRSN. And then lastly I have
8 here is the Halden research project which we talked to
9 the operating agent who is the one who maintains the
10 COMPSIS database, and this is a good segue to jump
11 into COMPSIS, computer-based systems important to
12 safety --

13 CHAIR BROWN: Can I ask one question?

14 MR. STURZEBECKER: Sure.

15 CHAIR BROWN: The comments in here are the
16 first times I have -- I know Canada has got reactor
17 plants. How many do they have?

18 MR. STURZEBECKER: I am not sure.

19 CHAIR BROWN: Anybody know? Two, three,
20 four -- on no, there's -- units? Is that the CANDU,
21 whatever it is?

22 MEMBER STETKAR: I don't know how many
23 have digital systems.

24 CHAIR BROWN: That was my next question,
25 was how many --

NEAL R. GROSS

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

1 MR. STURZEBECKER: Well, I think we --

2 CHAIR BROWN: This is the first mention
3 I've seen of --

4 (Simultaneous speaking.)

1 MEMBER STETKAR: They have a large number
2 of units. When I say large, probably 20 plus, I'm
3 guessing.

4 CHAIR BROWN: Reactor -- nuclear power
5 plants.

6 MEMBER STETKAR: But they are you know,
7 there's a wide range of --

8 MR. SYDNOR: This is Russ Sydnor. They
9 have actually done a lot of digital upgrades, and they
10 started some -- they started theirs back, I think in
11 the '90s. They have some --

12 MEMBER STETKAR: I mean a lot of their
13 refueling machines are probably digital.

14 MR. SYDNOR: One of the experts that we
15 are working with that Sushil was talking about, Dr.
16 Allen Nikora not only came to the RIC and supported
17 our presentations, but he was involved in some of the
18 reviews of those early digital systems and they are
19 actually looking at, you know, further updates now, a
20 second round of updates.

21 CHAIR BROWN: Are they on protection

NEAL R. GROSS

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

1 systems, or in control systems like feedwater control?

2 MR. SYDNOR: No, well they have those, but
3 they did protection system upgrades, they did -- and
4 those are the ones that he was involved with, where he
5 was hired as an outside consultant to do the
6 independent --

7 CHAIR BROWN: So they are ahead of us?

8 MR. SYDNOR: I can't speak to the detail.
9 We are trying to get the detail of their learning. We
10 are trying to tap into their learning. I'm not going
11 to claim one way or the other.

12 CHAIR BROWN: I mean they have got -- they
13 have put in production --

14 MR. SYDNOR: Have they done more --

15 CHAIR BROWN: Implementing reactor
16 protection systems.

17 MR. SYDNOR: Implementing protection
18 systems, I'd say yes --

19 CHAIR BROWN: Okay, that's all I meant.

20 MEMBER STETKAR: You can pretty much say
21 that of most every other country in the world.

22 MR. SYDNOR: I was trying to refrain from
23 making that --

24 MEMBER STETKAR: I will say that for the
25 record.

NEAL R. GROSS

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

1 MR. SYDNOR: Okay, thank you.

2 MR. STURZEBECKER: COMPSIS has eight
3 different countries in it right now -- Finland,
4 Sweden, Germany, Hungary, Switzerland, Korea, the
5 Republic of Taiwan and ourselves.

6 The idea is to pool all the events into
7 one database and do an analysis at every particular so
8 many years, that we have got the go-ahead for the
9 third phase of COMPSIS to continue, and that's a good
10 thing considering that we only had 27 events from 2005
11 to 2007.

12 The root causes from that particular
13 review of those events were about design defects,
14 configuration management issues, and hardware
15 failures. It's sort of minimum.

16 But at this point we have -- our group,
17 the team has put in about 58 of the 80 new events, and
18 they -- we just finished publishing them also.

19 When you put an event in COMPSIS it goes
20 through several phases of quality checks until the
21 end, when it's published. The other countries that
22 have participated are Germany, Hungary, Sweden has a
23 few points.

24 MEMBER STETKAR: Is COMPSIS a database?

25 MR. STURZEBECKER: It's a database.

NEAL R. GROSS

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

1 MEMBER STETKAR: Okay. So in addition to
2 having the acronym, it's a -- who's in it, it's a --
3 I better guess -- I wasn't sure, I didn't realize.

4 MR. STURZEBECKER: Halden owns it -- or
5 not really owns it -- but controls it and that's the
6 operating agent we talk to when we put an event in.

7 And it's quite hard to put a point in, I
8 mean it's a research grade level expectation of
9 events, so you can see here, we have got five required
10 fields.

11 Each of these fields breaks down from like
12 a grandfather father to daughter type, when you are
13 filling it in, because it's all web-based and you are
14 stepping through it.

15 The main info is just your basic plant
16 site, with the status it is and COMPSIS, high-level
17 deficiency characteristics is what, you know, the
18 actual or potential issue that could have happened, or
19 did happen, and there's like 21 different states that
20 you go through trying to pull for that particular
21 item.

22 For example, I could -- like a transient,
23 if you have a power supply failure and this is a
24 higher view of what's going on with that particular
25 event.

NEAL R. GROSS

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

1 Later on when you get down into the
2 details, there is a question that comes up for the
3 lower-level deficiency, which you might pull out
4 exactly why that power supply failed.

5 So they try to balance between one level
6 of looking at the event towards the lower level when
7 you actually pick out from the root cause what the
8 issue is.

9 We have detection, there's a behavior and
10 dependency series of questions, or parts you have to
11 fill in, plant information before or after, the
12 severity that happened, how it relates to what
13 regulation, and then system, the system that typically
14 is the way we work with most of the power plants, is
15 it's all system-based, which system it was, and you
16 get into the details like I said about the written
17 report in the lower deficiency.

18 So typically you fill in these five areas.
19 It can take, depending on who it is, it can take one
20 to five hours to put any of that in, and it also
21 depends upon the event that you are searching through,
22 you are reading through.

23 Typically what we have been finding I
24 think, Luis and I have been really concentrating on
25 this, is you have got to read through the entire LER

NEAL R. GROSS

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

1 and parse it out so sometimes we do come up with
2 consequence analysis or corrective actions, and never
3 really a lesson learned.

4 CHAIR BROWN: Cause analysis is not a
5 field?

6 MR. STURZEBECKER: It is a required field
7 that you have to fill in.

8 CHAIR BROWN: So there's really six fields
9 then?

10 MR. STURZEBECKER: Oh, I miscounted that.
11 I'm sorry.

12 MEMBER STETKAR: I've not seen this, but
13 thinking again back to the analogy of what people were
14 doing 30 years ago in going through LERs and creating
15 large tables with large numbers of Xs and numbers in
16 them, does the COMPSIS database include documentation
17 of the narrative of what occurred?

18 MR. STURZEBECKER: Yes.

19 CHAIR BROWN: It does. Good.

20 MR. STURZEBECKER: You cut and paste --

21 CHAIR BROWN: Good.

22 MR. STURZEBECKER: Those parts of the LER.

23 CHAIR BROWN: Because eventually, if we
24 ever do define failure modes, what we found were the
25 narratives were often much more useful than somebody's

NEAL R. GROSS

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

1 arbitrary notion of what they were trying to create
2 those data fields for, without any focus.

3 So I was -- I'm hoping -- I'm glad to hear
4 that indeed the narrative context is preserved.

5 MR. STURZEBECKER: And you will find some
6 very creative writers there too.

7 (Laughter.)

8 MEMBER STETKAR: As were LERs, you know,
9 is there any sense, speaking of that, and it's always
10 a problem because LERs, certainly 30 years ago, were
11 as much political documents as they were technical
12 documents, I used to be an operator, I wrote LERs, so
13 I understand this.

14 Given the fact that this is a shared
15 database among a variety of different countries, is
16 there any effort to go back and mine additional
17 information from the context, from the narrative, to
18 sort of you know, circumvent a little bit of that --

19 MR. STURZEBECKER: I think I know where
20 you are going with this.

21 MEMBER STETKAR: politicization or
22 whatever the term is.

23 MR. STURZEBECKER: Well, there's -- I have
24 some examples later at the end, which talk to that,
25 where you may have something said in one LER but if

NEAL R. GROSS

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

1 you find the sequence, there's always -- some of them
2 have sequences, some of them don't.

3 If you find the sequence, you can learn
4 more and pull out more and more information. If you
5 put the narratives together, you can literally paint
6 a picture of modernization going on at that site.

7 You follow what I'm saying?

8 MEMBER STETKAR: Not quite.

9 MR. STURZEBECKER: Okay. So if I have 125
10 systems in my power plant and I am the licensees and
11 I say okay, my best return on investment is to start
12 with the feedwater system because I get a two-year
13 return, turbine six-year return, money-wise, feedwater
14 level, they'll start digitizing these different
15 sectors or systems.

16 As they are going through it, they have
17 certain issues and you can see certain LERs -- I
18 haven't seen -- I mean I've got some examples but you
19 see a trend where they have a problem with the
20 turbine, the new turbine system they put in, and they
21 blame this particular oil switch, when it really --
22 you know, and then the next LER comes out, it trips
23 again. There's another problem.

24 They don't really find the true solution
25 until about four or five LERs down.

NEAL R. GROSS

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

1 MEMBER STETKAR: That's part of -- I guess
2 that's part of what I was asking you about, but the
3 other part is, even within the context of a specific
4 isolated event, if you want to call it that, the --
5 you are calling them LERs, whatever they are, the
6 summaries inside that are input to this database
7 contain abbreviated information. That's always the
8 case.

9 MR. STURZEBECKER: Yes.

10 MEMBER STETKAR: And the question is, is
11 there an effort to go back and obtain a bigger picture
12 of the entire context, or having not seen this, I
13 don't know what information is there.

14 The reason I bring it up is that you know,
15 back in the day again, this is old war stories,
16 reading LERs gave you a notion that something happened
17 but it was a particular spin on what happened.

18 There used to be a subscription service
19 that was called Nuclear Power Experience, one private
20 subscription service, they actually dogged all of
21 these things.

22 They went back and looked at LERs and went
23 back to the utilities and said can you please give us
24 more information about the context, and they kept
25 track of them, so that they for example, you could

NEAL R. GROSS

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

1 read the history of the fact that you know, the oil
2 switch was blamed 12 times but that wasn't the root
3 cause by five years down the road.

4 MR. STURZEBECKER: Right.

5 MEMBER STETKAR: And I was curious whether
6 that type of sort of investigative forensics was
7 folded into this.

8 MR. STURZEBECKER: That is in our mind
9 set.

10 MEMBER STETKAR: Okay. Because that
11 actually was almost more useful than the tabulation of
12 people checking off boxes.

13 MR. STURZEBECKER: Exactly. I'm right --
14 yes, agreed completely.

15 MEMBER STETKAR: Okay.

16 MR. STURZEBECKER: So let's go to our
17 friends in France. We had discussions with EDF through
18 the EPRI MOU specifically with Thuy Nguyen, and he is
19 part of the research side of EDF.

20 And they -- we are learning quite a lot
21 from them. They are right now endeavoring on redoing
22 all their 6800 microprocessors and Motorolas, 34
23 plants, the 900 megawatt series, and they are all
24 going to --

25 CHAIR BROWN: 6800?

NEAL R. GROSS

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

1 MR. STURZEBECKER: 6800, yes. Your classic
2 eight-bit registry, 16-bit address and 192 upcodes. I
3 love that one. That's the first one I started with.
4 These plants have been around for a long time --

5 CHAIR BROWN: No, I understand that -- I
6 took a Heathcliff continuing education --

7 (Laughter)

8 CHAIR BROWN: Okay, in 1983, and it used
9 a 6800 where I programmed in the 192 upcodes. I never
10 want to do that again.

11 (Laughter)

12 CHAIR BROWN: That's why I liked my
13 management job. I had other people work on that, but
14 I am just -- there's a point at which you say -- but
15 they are around and they work.

16 MEMBER STETKAR: We have plants that have
17 relays that go like this, okay?

18 (Laughter)

19 CHAIR BROWN: John, I took my last vacuum
20 tube source range instrumentation out in 1994.

21 MEMBER SIEBER: Do you still have it?

22 CHAIR BROWN: It's on a shelf.

23 MEMBER STETKAR: Oh you still have it? Oh
24 God.

25 MEMBER SIEBER: Just in case.

NEAL R. GROSS

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

1 CHAIR BROWN: I'm sorry, I couldn't pass
2 up the 6800 microprocessors.

3 MR. STURZEBECKER: So they are building an
4 FPGA platform and they are going to drop -- they are
5 building on that FPGA a 6800 series microprocessor.
6 They will keep their same program they have used for
7 the last 30 years and run it through the FPGA.

8 That's an easier upgrade, because they are
9 at a point where they are saying okay, I need to
10 upgrade the system, the brains, so they take out the
11 chip and they drop in an FPGA.

12 MEMBER STETKAR: But they are using the
13 same application code?

14 MR. STURZEBECKER: Same application.

15 MEMBER STETKAR: What's the point?

16 MR. STURZEBECKER: Because it works and
17 they have no problems with it, the software runs. They
18 have actually said, you know, that they have found
19 some issues in reviewing it that maybe some programmer
20 30 years ago just commented out or left it in there,
21 but it never really affected the program.

22 So it's interesting, the discussions with
23 them. I mean, the fossil side just completely replaces
24 the DPU, like in a Westinghouse, or an Emerson,
25 they'll pull the DPU out and they'll put an Ovation

NEAL R. GROSS

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

1 in.

2 MEMBER STETKAR: And I thought we were bad
3 and our program with 8086s and 8088s, so -- or how
4 about the Z80?

5 MR. STURZEBECKER: Z80.

6 MEMBER SIEBER: I had one of those.

7 MEMBER STETKAR: Well, that was the first
8 one I ever used, that was 1978 when we started that,
9 when it went into the Abraham Lincoln --

10 MEMBER SIEBER: Did it really?

11 MEMBER STETKAR: and the '72 and '73, and
12 it worked.

13 MEMBER SIEBER: Yes, '74 I had 2.3
14 megahertz or something like that processor, it was in
15 hertz.

16 MEMBER STETKAR: That's great. I'm sorry,
17 you are bringing back old memories with 6800
18 microprocessors, I didn't think anything was that old,
19 except for me. Okay, I'm sorry go ahead.

20 MR. STURZEBECKER: So, another particular
21 event mode 1 that we kind of latched onto was, Thuy
22 said you take a black bag and it's got marbles in it,
23 white, black and red, and he says every time you have
24 an event, a digital event, you reach in and you pull
25 it out.

NEAL R. GROSS

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

1 And you know, it could be a white marble
2 which equates to just a normal, everyday event, a
3 digital system that may have failed but didn't trip
4 you; a black marble would be a trip; and then a read
5 would be your classic TMI.

6 So we kind of latched onto this because it
7 was simple and for what we are doing --

8 CHAIR BROWN: Did you determine which they
9 were by which color marble you pulled out?

10 MR. STURZEBECKER: Yes, when you pull out
11 the --

12 CHAIR BROWN: So no matter what happened,
13 if you pull out a red marble, that meant you had a
14 TMI, regardless of whether it was just a switch
15 failure?

16 MR. STURZEBECKER: Right, because we were
17 saying that that could happen in that situation. So we
18 grabbed this model because it was easier to talk in
19 these terms because we were looking for resources now.

20 I mean, the idea is, in this mind map, is
21 to say okay, I have got my LERs that I need to track
22 down, they are typically black marbles or trips, most
23 of them.

24 But what about -- what other items do we
25 have that are out there and the ENs, the event

NEAL R. GROSS

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

1 notices, there's about 850 produced a year, so that's
2 another source of points or information to pull into
3 our database.

4 So that's kind of what we have picked up
5 from learning from the French.

6 MR. SYDNOR: Karl, this is Russ Sydnor, I
7 would like to just add to that, that Thuy -- EDF and
8 IRSN have access to thousands of events that they have
9 been tracking in their experience and they claim, in
10 digital systems that they have had lots of white
11 marbles and a few black marbles. They have never had
12 a red marble on a digital safety system thank God, and
13 we never want to see that one.

14 But they have learned a lot from the white
15 marbles and obviously you do learn a lot from the
16 black marbles, but the white marbles which are just --
17 can be just somebody finding a software glitch and
18 fixing it.

19 And so they have accumulated that amount
20 of operating experience and they are sharing that with
21 us. It's important because we haven't been able to
22 access that through any other more formal means, and
23 so we have been able to get some valuable learning
24 from this interaction with EDF.

25 MEMBER STETKAR: Russ, do they categorize

NEAL R. GROSS

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

1 the events any -- in any different detail than what is
2 shown here?

3 MR. SYDNOR: They do. They have a whole
4 event -- actually I was fairly impressed with their
5 even tracking, but then they are the utility and they
6 are also a designer so they have access, and they are
7 using them in the right way, as a learning tool for
8 that, not the same situation we have here, where you
9 have many different utility operators, many different
10 vendors, and an LER reporting system. So you have
11 different means of gathering the data and access to
12 it, but there's a lot we can learn from their
13 experience. It's just that they are quite often now
14 willing to share that openly.

15 MEMBER STETKAR: I was going to -- that
16 was -- the question is -- proprietary information.

17 MR. STURZEBECKER: And it is. And they
18 also say it's EDF French so it's another form of
19 understanding. We have conversations on the domestic
20 side with INPO. Obviously we have EPIX and we think we
21 are tying that also into for background information,
22 as we start tracking more of these LERs.

23 They are working on possibly updating
24 their -- the digital side of their EPIX database. I
25 think we have heard that from INPO.

NEAL R. GROSS

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

1 EPRI, we have an MOU with them. They do --
2 or they are working on a project right now where they
3 will take a deep dive in a particular event that
4 happened and talk to the utility, go through all the
5 different stages of what happened and create an
6 infomercial or a -- I forget exactly what -- was it a
7 PowerPoint or -- but they will show or give it to
8 their licensees to learn from.

9 Inventory and classification. That's Tom's
10 project right now. We have Oak Ridge working on this.
11 We have a draft report right now. In approximately
12 three -- another three months we will have a finalized
13 version for the classification structure and the
14 initial inventory.

15 The initial inventory was all volunteered
16 -- on a voluntary basis with plants and we plan on
17 bundling that in also to our database to help -- maybe
18 establish certain --

19 CHAIR BROWN: What is inventory in this
20 case, that you -- number of -- is that an event?

21 MR. STURZEBECKER: No, this is not an
22 event. This is actually -- okay, you go to, you ask
23 the plant to tell you how many systems you have
24 digital --

25 CHAIR BROWN: Oh, okay that type of thing.

NEAL R. GROSS

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

1 MR. STURZEBECKER: That's not inventory.

2 CHAIR BROWN: That's all I am -- okay fine
3 -- the conventional inventory thought process.

4 MR. STURZEBECKER: Yes, the conventional
5 inventory check.

6 CHAIR BROWN: okay.

7 MR. STURZEBECKER: And the first go-around
8 with this, the draft report on classification, there's
9 basically three attributes that Oak Ridge is saying to
10 look at is, again, systems, like we talked about,
11 function and then get into what kind of platform it
12 is, and there's more to come on that.

13 I mentioned the ENs earlier, operator or
14 OpE summaries that David Garmin from NRR is working
15 on, so we are keeping contact with him. Did I get to
16 the non-nuclear efforts?

17 We have an MOU with NASA/JPL and we are
18 very interested to find out how they are learning from
19 their processes and how -- what their lessons learned
20 influenced the way they have been moving through by
21 the applications of digital for their particular
22 unmanned flights.

23 There is a standard 7150 and it's in its
24 second rev. The first rev came out in 2002 and we have
25 had the opportunity to talk to Martha Wetherholt, and

NEAL R. GROSS

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

1 the idea here is to keep learning from what
2 experiences they are going through.

3 The next slide is a little bit more of a
4 deep dive into this particular standard. They came to
5 a point before 2002 where they said we need to step
6 back and reassemble everything and what you see on the
7 left is -- or my left -- in the pink, is the overview
8 of how those standards come together.

9 My arrow is right on top of -- there's
10 actually a standard for lessons learned, how they
11 accumulate lessons learned. This is the standard we
12 are looking at right now.

13 When you go into, you do a micro-look into
14 the standard, On page 14, they get into guidelines,
15 and this goes to the contractor. This is nine of 25
16 and this is well, I don't want to say rules, but more
17 like specifications or guidelines that they are asking
18 their programmers to follow.

19 If you step through -- what I found was
20 interesting, is as you step through each one of them,
21 you can pull out an attribute name, I mean the first
22 one is about flow control, the second one is flow
23 control of when you are coding, the third one, c, it's
24 predictability of logic.

25 These are terms that we have actually in

NEAL R. GROSS

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

1 our NUREG/CR-6463 that came out in 1997. So there's
2 connections here that we need to get -- we need to
3 look into further and try to draw from where they've
4 gone, where they have been going, and what we can
5 learn from these steps that they are going through.

6 I mean they are a mature industry compared
7 to where we are at.

8 CHAIR BROWN: Have you looked, and this
9 question may be -- I may be asking this wrong -- I
10 guess years and years ago we asked the question from
11 NASA also, but what they were doing 30 years ago and
12 we -- in the naval nuclear program when I was there,
13 and we found the difference between our systems
14 application-wise and theirs, since they were
15 fundamentally dealing with control systems, for flight
16 controls and bringing the shuttles back in and all the
17 other kind of stuff, and they were -- and I guess I am
18 going to ask you the question -- they had like five,
19 four or five systems that were all operating and doing
20 computations on information and they all had to agree
21 before they would control the surface, which is
22 totally different from what we did, which was, we had
23 four different systems operating on different
24 information, we didn't want them talking to each other
25 at all, and just wanted to shut down the plant.

NEAL R. GROSS

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

1 So it's the difference active control for
2 control purposes and single function reactor
3 protection or safeguard function, which in a way
4 dictates, not dictates, our conclusion was they used
5 a very extensive review, standards review that was
6 different, oriented different just because, in our
7 mind, different from the application process.

8 Have you all given any thought to -- I
9 mean I am not against using that when you are looking
10 at NASA's stuff, but you have got to look at it in the
11 context of how true, how they actually use their
12 control systems.

13 MR. STURZEBECKER: And I think that's
14 probably why we have moved a little bit closer towards
15 the unmanned flights because their flight control
16 system would be something similar to what we are doing
17 with the safety system at this point.

18 We have a few people we have some
19 communication with at the Johnson Space Center but we
20 haven't really made any further steps on that. David
21 Therrop is doing parsing of events for like the
22 different shuttle accidents, why through all these
23 different what they call incident surprise anomalies,
24 can they learn from those anomalies.

25 So there is effort that they are doing on

NEAL R. GROSS

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

1 that side and we haven't really been able to --

2 CHAIR BROWN: Okay, I was just -- that's
3 fine. I just want to -- it's just a thought process,
4 an application process, that their's was very, very
5 complex.

6 MR. STURZEBECKER: Right. Well, it is true
7 that I mean they have --

8 CHAIR BROWN: If you think we spend a lot
9 of money on it, they really do.

10 MR. STURZEBECKER: Yes, I think they have
11 like class A to class H, is that right Derek?

12 MRL HALVORSON: Derek Halverson. I don't
13 know what -- they -- after -- they have got A, B, C,
14 D, E, and then after that you kind of get into the
15 ground hardware and sometimes used for experimental or
16 not, something like that, H maybe is the lowest,
17 right, so that's your, you know, email at your desktop
18 or something, and it's not really mission-critical
19 there.

20 CHAIR BROWN: Okay, thank you.

21 MR. STURZEBECKER: And since I was on
22 rules, I'll go to the power of 10. Now, we had the
23 chance to sit down with Dr. Gerard Holzmann, and go
24 over some of the work he is doing and this whole idea
25 of power of 10.

NEAL R. GROSS

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

1 What he found was your programmers cannot
2 remember a large guideline book. It's just impossible.
3 So he simplified it to 10 basic rules and it's
4 useable, something understandable, and you can
5 remember when you are doing your programming.

6 The first two rules, actually the first
7 three, kind of set the flow and the transparency of
8 the program to keep it very simple and so it's easy to
9 test in the end and to troubleshoot.

10 The other four to seven, four to eight I
11 think it was, was the good, standard type of guideline
12 that you use whenever you are coding that he picked
13 out, and the last two, one was, nine was to use a
14 tool, always a static checker tool of some sort and 10
15 was every time these programmers are working, that
16 day, when they finish, they run their program through
17 his -- these 10 rules. It's kind of draconian but he
18 forces them to follow this every day.

19 So it was kind of interesting to hear how
20 he is enforcing this, because the NASA missions, the
21 JPL ones, every mission seems to have double the lines
22 of code, so they are trying to control this and at
23 least minimize the possibility of issues.

24 The second item there is JPL database, the
25 NASA JPL database. We have access to the 14,000

NEAL R. GROSS

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

1 mission events or actually they are incident surprise
2 anomalies.

3 And they have a varying degree of fidelity
4 levels and there are about seven different missions.
5 We haven't decided yet exactly how to thin-slice
6 through this, we may team it up with maybe some of the
7 lessons learned database, and pick one particular
8 lesson or flight and follow through and see what we
9 can find out.

10 The Mars Climate Orbiter there, I'm going
11 to talk a little bit more detail on this one.

12 MEMBER STETKAR: Karl, before you get into
13 the climate, it's going by itself, so I'll let it --

14 (Laughter)

15 MEMBER STETKAR: Before you touch that
16 button --

17 MR. STURZEBECKER: Okay.

18 MEMBER STETKAR: those 14,000 mission --

19 MR. STURZEBECKER: Events.

20 MEMBER STETKAR: as they are called, are
21 those equivalent conceptually to the information that
22 you are receiving let's say from EDF? I mean these are
23 the white balls if you will on your slide.

24 MR. STURZEBECKER: It could be white
25 balls. It could be --

NEAL R. GROSS

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

1 MEMBER STETKAR: Okay.

2 MR. STURZEBECHER: Yes.

3 MEMBER STETKAR: But they are actual
4 things that occurred?

5 MR. STURZEBECHER: Right.

6 MEMBER STETKAR: Do you know of any -- I
7 mean 14,000 events is daunting. Has JPL or have others
8 gone through those events and are there lessons
9 learned from them, or is there any compilation? You
10 mentioned EDF apparently has some sort of coherent --
11 some formulations of their events.

12 MR. STURZEBECHER: There's three or four
13 papers on the different -- on the 14,000.

14 MEMBER STETKAR: They are only papers,
15 they are not --

16 MR. STURZEBECHER: They are only papers,
17 they haven't really. See, that's what we are trying to
18 find out more and more, how does that tie back to like
19 the second rev of 7150, you know, what was fed back
20 into it so --

21 MEMBER STETKAR: I am only trying to get
22 an understanding of -- you know you are mentioning
23 several different sources out there. Is there any
24 sense of coherency in the way that people are
25 collecting all of this information for you know,

NEAL R. GROSS

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

1 various and sundry purposes, is there any sense of
2 coherency in terms of the types of information they
3 are collecting, how they are processing it, how they
4 are documenting it, how they are recording it so that
5 in case of -- as you are -- trying to share all of
6 these resources, there is some sense of consistency?

7 MR. STURZEBECKER: I think that's where
8 the quality level of these events varies, and
9 sometimes that happens and they don't even -- they
10 don't report it. It was just fixed on the fly.

11 MEMBER STETKAR: Okay. I was going to say,
12 that could be a problem and if you are trying to
13 estimate frequencies from the events, if you haven't
14 have an event recorded fine, you don't learn anything
15 from that event. But at least the ones that are
16 recorded, that are documented to some sense or
17 another, are they --

18 MR. STURZEBECKER: There was a -- there is
19 a correlation between the Mars Climate Orbiter. There
20 was only 45 of these ISAs compared to typically 200 on
21 another mission, and it failed.

22 So there is -- but you can't really say
23 there's a lesson learned other than, well, that was a
24 good reporting tool that says they were paying
25 attention and a lot of -- there's other issues I've

NEAL R. GROSS

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

1 got to -- I'm going to go into deeper --

2 MEMBER STETKAR: Okay.

3 MR. STURZEBECKER: on that one.

4 MR. BIRLA: Dr Stetkar, I think you asked
5 if JPL has done some analysis of this data. So I'm
6 addressing in that question now. We got connected with
7 this information, this source, through Dr Allen Nikora
8 at the Brookhaven work shop that you mentioned.

9 And his interest in analyzing the data was
10 the PRA perspective, can I get enough information to
11 do some quantification out of it.

12 So he worked with Dr. Robyn Lutz, who was
13 mentioned earlier in Luis's presentation, she has a
14 part-time appointment at JPL -- and together, they
15 processed a few hundred events.

16 They had to read the narratives. You
17 cannot extract easily from the database the tabulated
18 information, so you have to read the narratives.

19 That became very time-consuming so Dr.
20 Allen Nikora began writing a machine-learning program
21 so he is -- that's the direction he went into.

22 So we agreed that we will not want to take
23 that machine-learning approach. We want to learn from
24 it by direct reading. He gave us the database. We
25 consulted Dr. Holzmann as Karl had mentioned on how to

NEAL R. GROSS

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

1 go about getting value out of this database.

2 We are going to track what Dr. Allen
3 Nikora is going to do and see if it yields anything.
4 But he also connected us with a researcher at Johnson
5 Space Center who is also developing some kind of a
6 machine-learning approach to it.

7 So those are two things we know and Karl
8 has also made a connection at headquarters where
9 there's a lessons learning activity, how to extract
10 lessons from -- so he's got a lessons learned database
11 on the website.

12 So we are tracking that and trying to see
13 what approach they are using. I don't think anybody
14 has the answer, but we are trying to learn from what
15 they are doing and how we can work together.

16 MEMBER STETKAR: Okay, thanks. That helps,
17 but it also illustrates a bit of my concern regarding
18 the fact that I hear a lot of different people doing
19 a lot of different work without much focus.

20 In other words, how I process -- how I
21 spend my time, whether it's automated or paper cuts,
22 processing the information in 14,000 events, if my
23 world view is that the only usefulness is to try to
24 quantify some non-descript failure rate for something
25 that I don't understand, I might spend an awful lot of

NEAL R. GROSS

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

1 time doing that.

2 Someone else might have a different focus
3 and spend an equally large amount of time processing
4 those same 14,000 events for a different purpose, and
5 a third person might handle those 14,000 events
6 separately for a third purpose, and that's a bit --
7 it's an old story -- it's where we were in hardware
8 failure data 30 years ago, because we didn't have a
9 context that forced a focus in terms of thinking about
10 what you learn from those events.

11 That's why I asked the question about, you
12 know, how's EDF focusing their context from the events
13 that they have, and is there a focus for these 14,000,
14 you might call it lessons learned or you might -- you
15 know, it -- what type of information are you trying to
16 mine from this?

17 MR. STURZEBECKER: I agree with that, I
18 mean it's one thing handing it to the database and
19 saying okay, go look. In this case we are hoping to
20 keep -- we have -- every six months we have a meeting
21 with NASA to try to reverse-engineer backwards how
22 they came up with this standard, and what was the main
23 lessons learned that pushed them to that point?

24 And I think that's more value because
25 someone has already done the work necessarily than

NEAL R. GROSS

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

1 going through all 14,000. We may go through one
2 particular thin slice of that, on a particular issue
3 like you said, focus it, but for now, that's kind of
4 where we are sitting.

5 We still -- go ahead.

6 MR. BIRLA: Since you mention EDF, I don't
7 know if you want to get to that Karl, but we did
8 understand what they ran into. Essentially, when we
9 asked them if we could learn from their data, the
10 answer was that the way the information is written up,
11 it is EDF French, that means, even standard French
12 interpretation cannot get value out of that
13 information.

14 So they have got their own colloquial way
15 of writing and each plant is different.

16 MEMBER STETKAR: You are talking to a
17 person that at one time spent six weeks out of his
18 life sitting in the basement of a nuclear power plant
19 reading 60,000 Maintenance Reports on paper, written
20 in Swiss German. I understand the problem.

21 But still, when you have a way of -- that
22 still doesn't obviate the need to have some bins to
23 throw those events into.

24 MR. BIRLA: Right, so --

25 MEMBER STETKAR: It is a problem. I mean

NEAL R. GROSS

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

1 it's a -- I'm not trying to belittle this. It is a
2 real communications problem.

3 MR. BIRLA: Right. So let me get to the
4 next step in the discussion. So that originally
5 written manuscript had to be interpreted. After
6 interpretation, and there's some possibility that the
7 interpretation may not be right, they were trying to
8 bin it three ways: is it an issue with the system; is
9 it an issue with the procedures; or is it a mistake
10 the operator made, a human mistake?

11 And in the classification -- and again,
12 you can classify these things differently with
13 different mind sets. You can say something was a human
14 mistake or a procedural or you can also say it's a
15 system weakness that allowed such a thing to happen.

16 So the way they categorized it, most of
17 the things were not system issues.

18 MEMBER STETKAR: But I mean they were
19 categorized at that level is part of the message.

20 MR. BIRLA: Yes, yes.

21 MEMBER STETKAR: And that's why those
22 narratives are -- retaining the narratives, whether
23 they are translated interpretations or whatever is
24 really important, because that's where the real
25 information is.

NEAL R. GROSS

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

1 MR. STURZEBECKER: And from my experience,
2 when I was doing analog from good old pneumatics to
3 digital on fossil sites as a startup engineer, we
4 would keep a problem listing, and that narrative, that
5 whole idea of what was going on when you go from
6 analog to a digital, what was the interface issues
7 that this new, brand new item that no one has really
8 played with, I mean we went through the FAT test and
9 etcetera etcetera.

10 But there are certain parts, or certain
11 things that I see in some of these LERs that point out
12 right away they are running into the same problem we
13 had, you know, interfacing with a governor on a
14 turbine valve.

15 MEMBER STETKAR: And that is the type --
16 that could be very, very useful information, both in
17 terms of trying to quantify frequencies, if that's
18 your goal, or to understand the types of problems that
19 occur, which can help both in terms of licensing
20 reviews to make reviewers aware of these types of
21 issues, or modeling or whatever your preferences might
22 be.

23 So you are right Karl, that's important
24 information -- and regardless of whether it's you
25 know, a control system or even a protection system, if

NEAL R. GROSS

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

1 there are interface problems, there are interface
2 problems. Anyway go on, I'm sorry, I interrupted too
3 much.

4 MR. STURZEBECKER: So we are showcasing
5 this one that was heavily documented. 1996 there was
6 the paradigm at NASA/JPL where you were going to do it
7 faster, better, cheaper.

8 and this was the Mars Climate Orbiter that
9 was created during that time, launched in 1998. It was
10 going to be the first interplanetary weather
11 satellite, so you have a Martian weather satellite.

12 It had a Mars Polar Lander that was
13 following behind it and it was supposed to also
14 communicate to it. In this situation, it launched,
15 everything was fine, and the way the flight control
16 and this is the way it works, is it is going to swing,
17 after nine months, come up and swing behind Mars, and
18 then burn to slow down and get into an orbit.

19 There's a program on board, and this is an
20 IBM rev -- I forgot the series -- 6000. It only has
21 128 megabytes for memory, working memory. It has
22 another flash memory for actually doing, sending data
23 back and forth for pictures and so on.

24 But in this situation it's depending on
25 Ground Control to send up info and on -- for its

NEAL R. GROSS

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

1 flight path that it's going on, the trajectory. So
2 it's supposed to fire its jets to keep from going out
3 too far from Mars as it comes in because you have this
4 phenomenon from the solar winds and so on.

5 Well there was this problem with the
6 ground flight software called small forces. It wasn't
7 really small forces. It was coded in -- what was it,
8 foot-pounds per second versus newtons per second so
9 it's got the units issue, four and a half times more
10 powerful.

11 So this satellite is flying up and it
12 keeps pushing itself back in, back in, closer towards
13 the sun. They knew something was wrong in April. The
14 detection was there but they just didn't know where it
15 was coming from, and on the eleventh hour of course
16 it's too late. They still didn't discover it until
17 afterwards. It -- the Mars Orbiter was supposed to, I
18 mean it's supposed to come in at about 140 miles
19 outside orbit, the -- if it goes anything lower than
20 80, it's iffy whether it's going to survive.

21 Well, it came -- it was calculated it came
22 in at 57 miles. So it was too close of an orbit. They
23 don't know if it skipped out, or just burned up. It's
24 hard to say.

25 So, there is a simple I would say design

NEAL R. GROSS

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

1 issue with whoever put that software together, you
2 know, and even when they did have the -- and idea that
3 was something was wrong, they were using emails with
4 the contractor, so there was another issue going on
5 that they didn't elevate it to this ISA state to try
6 to get everybody involved, to talk about it.

7 So a little -- so that's why I put down
8 the series of white, small, little issues and then you
9 are gone, and that's still -- I was talking to Martha
10 yesterday --- it's still sort of one of their fears
11 because the systems are getting more and more complex
12 that they are working with, and it's going to be one
13 of these hidden things, where you are going to have a
14 series of things that happen and it's over. So it's a
15 concern. They still have this concern.

16 So, what are we doing with all this
17 information that we are trying to gather and the data?
18 We are trying to frame thus and synthesize a way of
19 pulling in this knowledge, and it's really based upon
20 starting with the LERs, because we are still feeding
21 into COMPSIS, and we have got the types of events, the
22 levels, classifications, their quality and we are
23 trying to look at what kind of failure types as we
24 start collecting these.

25 So this is a rough, what we're doing at

NEAL R. GROSS

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

1 this point, run-through starting with the left side.
2 I'm feeding into a database. We already had the
3 database established. It's in access right now.

4 There's 53,000 LERs dating back to 1980.
5 We've -- I think we have gone through one pass-through
6 one year, 2003, and we have done other hits all the
7 way through as far as '82 for a digital rod system
8 that failed.

9 The ENs, there's only 7,000 and that
10 starts at 2002 when they started recording them, EPIX
11 and then hopefully inventory studies.

12 So what we are going to try to do is
13 funnel this into the database, start creating what the
14 attributes we need to link them together, and in some
15 ways you have got to start reading through the main
16 LERs to pull out what comes up.

17 I mean I don't think there is a silver
18 bullet in this other than passing through more events
19 and learning as we go, which will create possibly more
20 attribute categories and then we have also used ADAMS
21 to validate like a power uprate on one particular set
22 of a series -- a sequence of LERs that had happened
23 that they did.

24 And that's how we are digging through the
25 information. We are trying to piece together what's

NEAL R. GROSS

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

1 going on. The parsing of the info -- if you get
2 something that's -- there are software packages now
3 that you could take the data and possibly create a
4 type of lessons learned that goes with things.

5 Human Factors came to us and asked us,
6 when we started going through these LERs, to mark them
7 if we see a human factors aspect. They want to know,
8 while we are doing this dirty grind work of going
9 through it.

10 And then there's the typical feed into
11 COMPSIS and the COMPSIS report. There's our lessons
12 learned and then what we are doing with NASA, the
13 whole idea of a database of what their lessons learned
14 are, maybe work through their engineering standards.

15 So this is a rough -- the format that the
16 team is working on to try to create a product, and
17 results, lessons learned.

18 MEMBER STETKAR: Karl, you say the team is
19 working on it. How -- where are you in terms of
20 developing this structure that you show here, or
21 framing process or however you characterize it?

22 MR. STURZEBECKER: It's -- right now the
23 database is about this thick when you print it out.
24 It's got all the white Mike Waterman items in it. It
25 has previous COMPSIS items.

NEAL R. GROSS

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

1 We haven't started feeding any other
2 inputs other than the last 80 we have done and we
3 haven't even started with the ENs or the EPIX, but the
4 idea is to start pulling in the main LERs and I am
5 more -- I mean I want to cover all the areas but there
6 are certain systems that we know that they are always
7 digitizing, so why not focus on them?

8 But we still have to keep a management
9 inventory of how we are looking through these events,
10 and it's going to take some time. It's not any
11 different than keeping a 3000 IO list for a digital
12 system. It's going to take some work.

13 So our path forward is to add more events,
14 find these sequences that can actually tell you more,
15 that could give you a lesson learned, or with a single
16 event, it can also just provide that lesson learned,
17 continue to expand on the mind map, there's other
18 areas, besides the aerospace that we can move into,
19 transfer techniques and each area of interest, and
20 build this flexible database.

21 It has to be flexible because we are still
22 kind of synthesizing these categories and develop the
23 OpE reports and lessons learned.

24 MEMBER STETKAR: The word -- the phrase
25 that you skipped over there pretty quickly that we are

NEAL R. GROSS

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

1 still categorizing these, I forgot the term you used
2 already, but the events?

3 MR. STURZEBECKER: Well -- Oak Ridge is --

4 MEMBER STETKAR: See, part of what I think
5 yo have heard from the ACRS for about three years now,
6 is that that thing you said well, we are still working
7 on this categorizing this structure, is what we have
8 been advocating that, that's sort of step one.

9 You need to identify the fact that you are
10 creating 37 square boxes and you understand what those
11 square boxes mean, as opposed to 900 spheres. And
12 either one might be fine but without that context and
13 structure, processing these thousands of events that
14 you have, now, recognizing that in today's information
15 processing technology it's a lot easier to handle that
16 amount of information than perhaps it was, certainly
17 than it was 30 years ago, but still without that
18 structure, you are not quite sure what you are going
19 to eventually do with it.

20 You know, the stuff on the right side of
21 your slide is -- there are things to be learned. But
22 it's not quite clear what you are going to do with all
23 of that information, and I don't hear a strong focus
24 from -- you know, you say you are working on it --

25 MR. STURZEBECKER: Well, I know Oak Ridge

NEAL R. GROSS

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

1 is --

2 MEMBER STETKAR: I don't hear a lot of
3 focus on it.

4 MR. STURZEBECKER: trying to focus on what
5 those particular categories are. And we already -- you
6 know, from experiences I know it's systems and that
7 it's function.

8 And you know as for platform, I kind of
9 question, but we have got to get into that further. I
10 mean, my experience has been more of I like what Susan
11 Slaughter wrote, it's called you build a building for
12 500 years, and you do this idea that you look at the
13 function, you know where the location is of the
14 instrument and how it ties in, and then in the
15 operating room you are going to have spatial
16 interaction kind of aspect, where you may have two
17 different systems and they are completely separate
18 from each other but they have the same look and feel
19 to the operator.

20 So that's the spatial interaction. So
21 there's the three basic rules there, and if you look
22 what Emerson is doing -- and this is like a few years
23 ago on their website, they can take your plant, this
24 is a fossil plant, because it's mostly my background,
25 and they can say okay, we'll come in and we can

NEAL R. GROSS

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

1 automatically figure out where your systems are laid
2 out and how we should position them as an architecture
3 in a digital control system and put 22 cabinets in and
4 bing, they are done, because they know -- they have
5 done it enough times, that's technology we -- I would
6 love to know how they do that.

7 So there's a lot of learning that we need
8 to go through, and I understand what you are saying,
9 at the same time we have got to refocus on what the
10 plant's here are doing. They are hybrids. They are not
11 going to go full digital.

12 A typical full digital will take a year to
13 do. That's what --

14 MEMBER STETKAR: They're not for the
15 operating reactors but all the new reactors are --

16 MR. STURZEBECKER: The new reactors yes.
17 So you know we have to keep that in mind.

18 MEMBER STETKAR: Right, that's true also.
19 That's true.

20 MR. STURZEBECKER: So, but that's why I am more
21 focused on the LERs at this point, from that standard.
22 But I know what you are saying, that we have got to be
23 careful on what we are looking for.

24 I think it is important to exhaust through
25 and find those digital events, because there might be

NEAL R. GROSS

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

1 53,000 but they are not all digital, and right now, I
2 tried using the word digital, and I came up with
3 50,000. There's no way. It's -- something's wrong with
4 the parsing in our program. So I understand what you
5 are saying.

6 MEMBER STETKAR: Okay thanks.

7 MEMBER STETKAR: So if I go back to slide
8 14.

9 MR. STURZEBECKER: Yes.

10 MEMBER STETKAR: And I'm trying to spring
11 from your all's interchange here, you are still
12 working on the first little circle and getting it
13 categorized to go into the database?

14 MR. STURZEBECKER: We have a basic
15 categorization in the database now. It's -- when it
16 happened, the plant, the system involved, and we
17 hadn't really broken down further from there. I have
18 some ideas of what we are going to do.

19 CHAIR BROWN: But you are working on the
20 one line effectively, in getting something categorized
21 into that database?

22 MR. STURZEBECKER: Right. And it's a
23 learning experience at the same time. I mean, we just
24 after doing the 58 for COMPSIS, we started seeing this
25 sequence idea that it's just not once that it happens.

NEAL R. GROSS

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

1 Sometimes they have two or three times with the same
2 system. They are still learning, and some of the
3 events you point out, really questionable engineering,
4 you know, the de-bouncing button on a step change from
5 an operator. There's no way, in 1996, that that -- I
6 think it was 1996 -- should be happening like that.

7 You know, the technology was far ahead
8 back in the '80s when I was at Kodak and we already
9 had that idea, or the idea that you were saying about
10 --

11 CHAIR BROWN: Contact de-bouncing.

12 MR. STURZEBECKER: A simple keyboard, yes,
13 that you should have the right step change, two-second
14 step change when you hit that, that it holds and it
15 doesn't -- and when it drops out it just holds until
16 it's supposed to.

17 So you know they would have trips like
18 this because of very simple design mistakes. So that's
19 what we are seeing. So in some ways we are already
20 coming across a lot of information just on what they
21 are doing wrong, or what they should be doing, and
22 hopefully they are learning from it.

23 But you know I have a ahrd time gauging,
24 because if you look in the '90s, did they really learn
25 it in the aught-ies (00s,) you know, you have got to

NEAL R. GROSS

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

1 move up, so it's -- you follow what I'm saying? The
2 same plant, did they get up further --

3 MEMBER STETKAR: Yes, I mean, certainly
4 the date is important because you can look at that,
5 but it's still -- it still comes down to how you
6 categorize and bin those events basically, because you
7 can't --
8 you can't look at 60,000 events or 80,000 or 100,000
9 events individually every time you get an idea about
10 well, gee, let's look at it this way.

11 CHAIR BROWN: Yes, but you can bin and
12 expand bins, I mean you have got a -- you can over-
13 think it also in terms of how in trying to ensure
14 before you ever get started that you have got every
15 possible thing that you could stick stuff into into
16 and therefore you never get around to sticking all the
17 marbles into any bin at all.

18 It's just a -- and I don't know when you
19 started this. I was just looking at part of your
20 report in here where this started --

21 MR. STURZEBECKER: Last August is really
22 when I think the team came together.

23 CHAIR BROWN: Well this one said for 60/30
24 it was 3/1/2011, and on the COMPSIS it was 2/28/2006,
25 so I'm -- I'm working somewhere inbetween those two

NEAL R. GROSS

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

1 dates.

2 MR. STURZEBECKER: Well that -- right, I
3 didn't start until 2008 so I am not really sure, so --
4 we come aboard and the team is trying to pull this
5 together and --

6 MEMBER STETKAR: So it sounds like there's
7 quite a bit of activity going on now at least trying
8 to identify you know, sources off to the left of your
9 diagram there, trying to figure out what to do with
10 the information you have while you find new
11 information.

12 MR. STURZEBECKER: And that's the next --
13 right.

14 MEMBER STETKAR: And if it's active that's
15 good, it's just a question of how will it be focused.

16 MR. STURZEBECKER: Because I can say
17 there's a difference between if you have a fully
18 automated plant like what I have come from, where the
19 highway that talks between each of the DPUs,
20 distributed processing units, when they talk, you try
21 to keep -- minimize the traffic on the highway. You
22 never, you keep centralized the control loops, your
23 simple control loops, and whatever you need to send on
24 the highway is minimized because if you have an alarm
25 burst you have got to be able to handle that.

NEAL R. GROSS

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

1 And yet, you see incidences where you have
2 a variable frequency drive that's on a plant data
3 network, and I see them saying okay we are going to
4 put a firewall to slow down this traffic because it's
5 overloaded the PLC, the PLC's fault.

6 This is poor design, very poor. That has
7 an IT flavor to it. It's not a control engineer. So --

8 CHAIR BROWN: All right. I've flipped your
9 back.

10 MR. STURZEBECKER: I am done.

11 CHAIR BROWN: Okay, acronyms, we won't go
12 through those.

13 MEMBER REMPE: And if you --- since you
14 are almost done, just a stupid question, the 14,
15 what's the color coding? What's the -- why are some of
16 the dots light blue on the far left, does that
17 indicate something like for --

18 MR. STURZEBECKER: You know, I made a
19 mistake.

20 MEMBER REMPE: Oh that's okay, I just was
21 curious and I was -- it was kind of --

22 MR. STURZEBECKER: I didn't even notice it
23 until now.

24 MEMBER REMPE: Okay, never mind.

25 CHAIR BROWN: They should be just open

NEAL R. GROSS

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

1 circles?

2 MR. STURZEBECKER: They all should be open
3 circles. The inventory study is just as important as
4 EPIX, you know, so that was a mistake there.

5 I mean the only other thing I had, I don't
6 know if you wanted to go through. These are a couple
7 of the events I put up that the LERs, single events.

8 The first one is a power-supply related
9 event, and that one, when you read through the LER,
10 they talk about how they should have put it -- they
11 were thinking about putting HVAC to protect the
12 digital feedwater system, but they didn't do it, and
13 then they did it later.

14 It's sort of -- you can't tell, it's sort
15 of wishy-washy in that sense, but you get the failure
16 that you know why the power supply failed because it
17 overheated.

18 The second one was interesting because now
19 the licensee is asking the contractor to build its
20 software design because it's got perturbations in the
21 power supply, to take for this condensate demin
22 system, to address what the valve positions are and
23 put it in memory, and hold it, because it keeps having
24 power supply problems.

25 Well when they go in to change the CPU it

NEAL R. GROSS

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

1 drops out, because CPU does not -- is not able to
2 handle -- it starts up with its own initiation phase.

3 And that's another thing, is you shouldn't
4 be changing the brains of the computer while the
5 plant's running. I mean, it just throws me. That's
6 2007.

7 The digital feedwater, that was the one I
8 already talked about, the de-bouncing, and the digital
9 feedwater, that was an interesting one. I'm sorry,
10 I've gone through so many of them, I have to look at
11 my notes. So they start looking the same.

12 That was interesting. I liked that one
13 because they had tuning problems with the digital
14 feedwater system they put in, the new turbine and then
15 they had a power supply later -- a power supply
16 failure within a year later, and very complicated
17 recovery because they had the RCIC did not work; it
18 tripped out.

19 And it's because this was an old Bailey --
20 I forget the series -- an electric controller that was
21 not tuned. They did not tune that controller and yet
22 there were tuning problems earlier with the other
23 system.

24 So, you know, it's this idea you are
25 mixing two things, who is getting the attention? So

NEAL R. GROSS

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

1 that's the kind of stories you start seeing when you
2 put these things together.

3 It gives you a better picture of the
4 modernization going on in the sites.

5 CHAIR BROWN: Yes, unintended
6 consequences.

7 MR. STURZEBECKER: Yes.

8 CHAIR BROWN: Okay is that it?

9 MR. STURZEBECKER: Yes.

10 CHAIR BROWN: All right. We are now eight
11 minutes behind. Next.

12 MR. SYDNOR: Paul Rebstock

13 CHAIR BROWN: Okay. I'm trying to figure
14 out which one is next on the schedule.

15 MS. ANTONESCU: The white paper.

16 CHAIR BROWN: Oh, the white paper. Okay.

17 CHAIR BROWN: Fire away.

18 MR. REBSTOCK: All right. I am Paul
19 Rebstock. I am with the Office of Research and Digital
20 I&C, and I want to present this paper on redundancy
21 and independence among safety channels.

22 Motivation for the work that we did, why
23 did we write the paper? We find that there are
24 proposed designs and licensing applications that
25 include features that have raised questions about

NEAL R. GROSS

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

1 independence among digital systems.

2 We have got industry claims that for
3 instance single-failure resistance without
4 independence is good enough. We have got claims from
5 industry that says that their design is so
6 comprehensive and so well-studied that they know it's
7 not going to fail so you don't have to worry about it.

8 We suspect that might be a questionable
9 claim. Discussions oftentimes involve different
10 aspects of independence. Sometimes people talk about
11 physical independence and you can talk about
12 electrical independence, communications independence.

13 The 2009 version of IEEE 603 talks about,
14 what do they call it, digital communication
15 independence, but they don't define what that means.
16 Again, there's another thought that says independence
17 means it ain't dependent.

18 NRR and NRO got together and issued a
19 joint request to the Office of Research to look into
20 all of this and give them an opinion as to what the
21 independence requirements are, and what the
22 implications of lack of independence are.

23 So that's what we did and that was the
24 source of this paper, and one caveat I would say is
25 that in this paper what we are talking about is from

NEAL R. GROSS

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

1 the point of view of digital I&C.

2 Somebody that reviewed the paper once came
3 back about something about station batteries and you
4 know and stuff, this is talking about digital I&C and
5 for the most part that's fairly -- hope fairly clear.

6 MEMBER STETKAR: But, Paul, in a licensing
7 perspective, when we think about consistency in terms
8 of deterministic licensing requirements, why is
9 digital I&C different from diesel generators or
10 batteries, in the sense of independence of redundancy.

11 MR. REBSTOCK: It's not.

12 MEMBER STETKAR: Okay.

13 MR. REBSTOCK: It's not fundamentally.
14 What I mean by that isn't that this stuff doesn't
15 apply there, it's that's the point of view I'm
16 looking. So if somebody looks at some of this work and
17 says well, I know of a case regarding station
18 batteries where it doesn't work that way, is that may
19 very well be the case, but that's not what we are
20 talking about here.

21 It's not that digital I&C is different, in
22 that sense.

23 MEMBER STETKAR: Thanks.

24 MR. REBSTOCK: So, we have got a set --
25 the requirements are set forth in the Code of Federal

NEAL R. GROSS

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

1 Regulations. The main issue is through IEEE 603-1991.
2 Then there are general design criteria.

3 And part 52 has a pointer in it that
4 points right back to Part 50 for issues that are
5 concerned with the topic of this paper. As far as the
6 IEEE standard is concerned, there's rulemaking in
7 progress right now to update to the 2009 version of
8 IEEE 603. That's ongoing work that is fairly early in
9 the efforts right now.

10 CHAIR BROWN: Which year, two thousand --

11 MR. REBSTOCK: 2009 is the latest version.

12 CHAIR BROWN: 2009, yes, and that's the
13 one you are actually looking at then?

14 MR. REBSTOCK: That's the one that there's
15 a rulemaking effort to incorporate that into the Code
16 of Federal Regulations. There was at least one version
17 inbetween '91 and 2009 --

18 CHAIR BROWN: 2003.

19 MR. REBSTOCK: and they are skipping over
20 that. Yes.

21 CHAIR BROWN: I thought it was a 2003.

22 MR. REBSTOCK: So those are the
23 requirements. In addition we have got guidance. One of
24 the elements of guidance is Interim Staff Guidance 4
25 which we have presented some time ago to this group.

NEAL R. GROSS

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

1 Basically, it talks about, among other
2 things, the subject is communications. It also
3 addresses independence among safety channels.

4 It points out that safety channels
5 shouldn't need one one another and it provides in it
6 an acceptable process for inter-divisional
7 communications.

8 It points out, though, that the safety
9 channel shouldn't need input from outside and it
10 shouldn't perform non-safety functions. So the need
11 for inter-divisional communications is questionable,
12 but if it is needed there's a way to do it that
13 doesn't compromise anything.

14 Standard Review Plans, chapter 7, section
15 7.9 clearly indicates that the redundant systems
16 should not influence one another.

17 There are several regulatory guides that
18 address the question of independence. They don't
19 really give strong guidance as to what independence
20 requirements are among channels as far as function is
21 concerned, but they don't contradict anything that we
22 are saying here, either.

23 Other sources of information. We have got
24 the -- from an international perspective we have got
25 the Multi-national Design Evaluation Program I think

NEAL R. GROSS

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

1 is what it's called.

2 Their common position, in EPR-01 on the
3 EPR reactor, and then there's also a joint regulatory
4 position statement by the United Kingdom, Finland and
5 France.

6 ACRS has issued a letter to the Commission
7 on design closure for -- on closure of DACs that
8 addresses as part of it the question -- the issue of
9 independence, and the National Research Council has
10 written a report, Software for Dependable Systems:
11 Sufficient Evidence?, which is a rather interesting
12 small book.

13 All of these are cited in the paper.
14 There's strict bibliographic references and there's a
15 little section that talks about what each one of these
16 has to say. All I want to say right now is this is all
17 consistent. It all falls into line with what we are
18 suggesting.

19 Practical reasoning. I don't want to just
20 say that it's the rule. I don't think it's good
21 enough. I don't think that's what we were called upon
22 to do.

23 I wanted to get into, when I wrote the
24 paper, I wanted to get into why is that the rule. Why
25 does that make sense?

NEAL R. GROSS

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

1 To be redundant, systems have to be
2 independent. If one systems needs another, then it
3 can't be redundant to the system that it needs.

4 So we talk about good design. We go --
5 nuclear requirements go beyond what the rest of the
6 world might consider to be sufficient. No matter how
7 good your V&V is, we can't be adequately confident
8 that you have considered every conceivable kind of
9 failure and covered every conceivable error.

10 No matter how good the analysis is, we are
11 skeptical that -- that you can obviate -- that you can
12 say everything that is going to happen. There will
13 always be unknown events.

14 So in the nuclear industry, we say do good
15 design, what the rest of the world thinks of as good
16 design, and then do some more.

17 Need for simplicity. This is a recurring
18 theme. There's been lots of reference to simplicity,
19 and the need for simplicity or the need for lack of
20 complexity.

21 Complex things are difficult to verify and
22 when you mix complexity with compromised independence
23 I think that's not a good direction to go.

24 Inter-divisional information sharing. The
25 most important issue is that if information is shared

NEAL R. GROSS

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

1 among divisions, it has to not compromise the safety
2 function, and the receiving system has to not need the
3 information in order to perform its safety function.

4 Now the immediate reaction whenever I say
5 this to somebody, somebody almost always comes up and
6 says what about voting. Well obviously voting is an
7 inter-divisional function. That's the whole point.
8 That's the reason you have multiple divisions, is so
9 you can vote.

10 So I'm not talking about voting here. I'm
11 talking about the channels that go up to making the
12 decision that goes into the voter.

13 MEMBER STETKAR: Paul, why don't you talk
14 about voting? Thank you. I'm sorry.

15 CHAIR BROWN: You beat me.

16 MEMBER STETKAR: You can get the shared
17 input transmitters.

18 CHAIR BROWN: Okay.

19 (Laughter)

20 MR. REBSTOCK: We'll get to that.

21 MEMBER STETKAR: Seriously, why just
22 because historically the agency has allowed certain
23 practices, you now define a very narrow focused view
24 of the term independence.

25 It must be this for this, but never mind

NEAL R. GROSS

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

1 this other stuff --

2 MR. REBSTOCK: Nonono, no.

3 MEMBER STETKAR: because we allow sharing
4 of information for voting. We allow single
5 transmitters to provide information to all four safety
6 divisions, but that's okay because we have allowed
7 that in the past.

8 MR. REBSTOCK: Well, I thought we don't,
9 but --

10 MEMBER STETKAR: We absolutely do.

11 MR. REBSTOCK: Okay.

12 MEMBER STETKAR: And we have licensed
13 plants that do that, exiting plants and new plants.

14 CHAIR BROWN: New plants, in particular,
15 yes.

16 MEMBER STETKAR: Why must these two things
17 be absolutely independent in terms of their ability to
18 write, but other things be allowed to share
19 information? I mean it doesn't sound like a consistent
20 view of independence.

21 MR. REBSTOCK: Right, there are multiple
22 questions there

23 MEMBER STETKAR: But if your view, if your
24 view is everything must be absolutely independent, as
25 this white paper seems to indicate, it says that we

NEAL R. GROSS

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

1 can't license the plants that we have licensed.

2 MR. REBSTOCK: Okay.

3 MEMBER STETKAR: So I am really torn with
4 that notion.

5 MR. REBSTOCK: I understand that. I
6 understand that.

7 CHAIR BROWN: But he is not the only one
8 that's torn with it, so as I've made the point several
9 times in some of the stuff we've been looking at,
10 about that inconsistency.

11 And you can have voting systems that are
12 not -- that are totally independent. But there are
13 voting systems that are independent. So I mean I am
14 not saying you want to use them, but I'm just saying
15 you can have a voting system that is totally -- in
16 fact it's the old voting systems, if you go back 40
17 years, were independent.

18 MR. REBSTOCK: Well, I think it depends on
19 how you are defining and where your scoping the
20 systems there. There's a whole bunch of different
21 issues here and I'd like to address them one at a
22 time.

23 MEMBER STETKAR: Okay, sure. Sure.

24 MR. REBSTOCK: Okay, as far as voting is
25 concerned, we have got typically four channels, four

NEAL R. GROSS

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

1 sensing channels in four different safety divisions.
2 The issue is, should we take the safety action or
3 shouldn't we, if two of the channels say do it, then
4 you do it. If only one of the channels says do it,
5 then you don't.

6 So in order to determine that all -- how
7 many channels are saying to do it, you have to compare
8 the channels. That's not an exception. That's a
9 logical thing. There has to be a way to combine that
10 information.

11 If you combine that in one voter that's in
12 one division, you combine it another voter that's in
13 another division as well, and those two voters are
14 independent of one another, although they are
15 receiving all the channels. If they didn't receive all
16 the channels, they are not voting.

17 MEMBER STETKAR: Okay, why are they
18 independent? They are receiving -- you just said they
19 are receive information from all of the other
20 channels.

21 MEMBER STETKAR: Yes, if I send four
22 signals -- the four signals to two different voting
23 channels, four divisions, they go to two different
24 voting channels, I've just sent four signals -- they
25 are not -- the four signals are all the same. They've

NEAL R. GROSS

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

1 gone --

2 MR. REBSTOCK: That's right. At the voting
3 level, at the voter they are independent.

4 CHAIR BROWN: No, at the trip they are
5 independent. But at the time they are all sent to the
6 voter, now each voter has exactly the same data coming
7 into it.

8 MR. REBSTOCK: That's right.

9 CHAIR BROWN: Channel 1 feeds both,
10 channel 2 feeds both, 3 feeds both and 4 feeds both.
11 So in a microprocessor-based system, once you have
12 done that, if you have got corrupt data, you can shut
13 both of the voters down.

14 MEMBER STETKAR: There is the point
15 Charlie, that we have to be careful with, if you've
16 got corrupt data, it's a two-out-of-four voter, if
17 you've got corrupt data from three separate inputs,
18 it's not going to work. If you've got corrupt data
19 from two, it will work. If you've got corrupt data
20 from one --

21 CHAIR BROWN: No. No.

22 MEMBER STETKAR: it will work.

23 CHAIR BROWN: Not true. If you lock up the
24 microprocessor --

25 MEMBER STETKAR: Okay, that's --

NEAL R. GROSS

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

1 CHAIR BROWN: based on one set of bad --
2 you will lock up both, if it will lock up one, it will
3 lock up the other.

4 MEMBER STETKAR: And if that failure -- if
5 that type of failure can occur you are absolutely
6 right, from a single corrupt signal.

7 CHAIR BROWN: You can't say it can't based
8 on the -- and by the way you say that in here.
9 Conceptually you make that point, on a generic, on a
10 general basis you make that point, but that's the
11 circumstance I mean, how do you deal with -- when you
12 use a microprocessor for a voting unit, that's
13 inherently taking data from all of them, and if the --
14 if you can get a data stream, whatever that data
15 stream looks like, if it's a serial data stream or
16 whatever, it has all the components with the ability
17 to potentially stop the voting unit from operating.

18 MR. REBSTOCK: If you are looking at the
19 A voter, and you are looking at the information from
20 the B system, that communication channel should be of
21 a nature that the B system is not able to interfere
22 with what the A channel does.

23 It simply says it votes to trip or to not
24 trip, but it can't alter the program in B. It can't
25 lock B up.

NEAL R. GROSS

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

1 CHAIR BROWN: Once you start sending a
2 serial data stream with a header data stream and a --

3 MR. REBSTOCK: You don't do that.

4 CHAIR BROWN: Well that's what they do.

5 MR. REBSTOCK: The ISG-4 communication
6 would not permit that.

7 CHAIR BROWN: One of the -- I hate to tell
8 you but that's what you have got.

9 MR. REBSTOCK: I -- okay. Personally I
10 don't think that's a very good idea.

11 MEMBER STETKAR: In the sense of single
12 failures versus things, I classify that as not
13 single-failure-proof because you can indeed have a
14 single corrupt data stream sent from that B processor,
15 if you will, to --

16 CHAIR BROWN: To all four.

17 MEMBER STETKAR: So that's not in the
18 traditional sense of being single-failure proof.

19 CHAIR BROWN: Exactly, but we were able to
20 look at that from the standpoint that there was a
21 watchdog function which stated if you lock up all four
22 of the voting units, it would end up tripping the
23 system.4

24 MR. REBSTOCK: That is layering on things
25 that -- CHAIR BROWN: Well, that is --

NEAL R. GROSS

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

1 MR. REBSTOCK: complicate a problem that
2 shouldn't exist.

3 CHAIR BROWN: Well that's a layer to --
4 because independence has been -- I don't want to say
5 completely compromised, but has been reduced.

6 MR. REBSTOCK: Okay, you are talking about
7 a system -- you have some specific system design in
8 mind and I'm not familiar with that so --

9 CHAIR BROWN: That is not a matter of
10 being in mind. We have already gone through two of
11 them.

12 MEMBER STETKAR: Well, the question is if
13 this white paper is -- I don't know how this white
14 paper will be used, but if this white paper is being
15 used to influence agency regulatory positions, going
16 forward, some of the implications of what is said in
17 words here, in terms of what is independent, what is
18 not independent, what is allowed, what is disallowed,
19 are quite significant, especially in light of past and
20 ongoing agency reviews and approvals of licensing
21 practices.

22 MR. REBSTOCK: Is your concern that this
23 would permit things that shouldn't be permitted, or
24 that it would forbid things have have already been --

25 MEMBER STETKAR: No, it would -- my

NEAL R. GROSS

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

1 concern is that it would permit some notion of things
2 that have been permitted in the sense of shared
3 information for voting is okay, and shared input from
4 common sensors would be okay, because we have
5 permitted that.

6 However, some of the things in here seem
7 to say that things that we have accepted will not be
8 permitted also.

9 CHAIR BROWN: That's correct.

10 MEMBER STETKAR: So that is why I am
11 having difficulty in terms of trying to understand
12 where you are, what this paper is trying to enforce in
13 the context of where we are now, versus where the
14 agency says we should be in terms of this notion of
15 independence going forward.

16 MR. REBSTOCK: The purpose of the paper is
17 to set forth the requirements and the -- to set forth
18 the requirements as we see it. The issue of voting, I
19 think, that you are talking about, where the voting
20 causes interference between channels --

21 CHAIR BROWN: No, the voting -- no.

22 MR. REBSTOCK: It's the communication.

23 CHAIR BROWN: The trip, the processing
24 unit that issues a trip, you have to send data to four
25 voting units.

NEAL R. GROSS

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

1 MR. REBSTOCK: Right.

2 CHAIR BROWN: Every -- there are four trip
3 processors.

4 MR. REBSTOCK: Right.

5 CHAIR BROWN: Each processors sends its
6 serial data to all four.

7 MR. REBSTOCK: But it's generally tow
8 voters but it sends it to --

9 CHAIR BROWN: No, well in this case
10 there's four.

11 MR. REBSTOCK: Okay, okay.

12 CHAIR BROWN: I'm trying to remember the
13 specific project, but it's -- whether it's two or four
14 is irrelevant. Okay? And so does processor two, so
15 does processor three, so does processor four, sends it
16 -- whether it's 2 or 3 or 4, each one sends it to all
17 one of them, so that any of the processors generating
18 a fatal data stream could lock up all four of the
19 voting units.

20 MR. REBSTOCK: Right, but that's where the
21 problem is. It's the concept of the fatal data stream.
22 If the data are exchanged properly, that can't happen.

23 CHAIR BROWN: That's -- I am glad you are
24 -- I'm --

25 MR. REBSTOCK: I mean if you are using --

NEAL R. GROSS

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

1 if you look in ISG-4, it describes --

2 CHAIR BROWN: I understand. I have read
3 ISG-4 and I agree with what's in ISG-4, except once I
4 read ISG-4 and started reviewing the projects, I found
5 that well gee, that's not what was going on. It was
6 because people were making the same statement, as we
7 can make sure that data stream is okay.

8 MR. REBSTOCK: Well, that's part of the
9 motivation for writing this paper. That gets into the
10 design is so good it won't fail.

11 CHAIR BROWN: I'm not disagreeing with the
12 writeup of the paper. It's a good -- put together a
13 lot of information, should be good food for thought to
14 coalesce and focus about what you really want to do.

15 MR. REBSTOCK: I can't comment on the
16 designs that you are talking about. I am not familiar
17 enough wiht them. I have an inkling of what you are
18 talking about and where you are going with it but I'm
19 not really in a position to be able to --

20 CHAIR BROWN: Well, there's serial data
21 communication going between the trip units and the
22 voting units. It's not -- if the voting units -- I let
23 me step back.

24 If the trip units converted that instead
25 of a serial data stream, generated a single on/off

NEAL R. GROSS

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

1 analog signal that was sent, that's all, like a relay
2 contact, you know, put it however you want to, it
3 trips something, that contact closes.

4 That's a different from in which it would
5 need to be dealt with in terms of how it is received.

6 MR. REBSTOCK: Right.

7 CHAIR BROWN: When you send information
8 into the processing stream, where it could possibly
9 get mixed up with general communication -- excuse me,
10 the general -- the way the system, operates, then you
11 have got a potential problem.

12 MR. REBSTOCK: You are asking for trouble.

13 CHAIR BROWN: You are at potential
14 problem. Does it say will happen? No. Does it say it
15 won't happen? No. And that's the problem. And that was
16 the issue with having a backup, some way to say are
17 these systems -- can you make them work and the
18 watchdog timer is kind of a clue at the end.

19 And Hi Dan.

20 MR. SANTOS: Hi. Dan Santos, NRO. A
21 question I have got to ask is how you plan to use this
22 in the regulatory context framework. Right now this is
23 an opinion from the Office of Research and it will
24 have to vet it formally and probably include OGC and
25 others.

NEAL R. GROSS

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

1 But what is happening is that with the
2 recent applications, the trend has been more and more
3 integration, and more interdependencies that were very
4 hard to assess only backed up claims similar to what
5 Paul referred to at the beginning, which were
6 problematic.

7 So they create a lot of confusion to the
8 staff of what independence meant, what our regulatory
9 stance was on this, as reviews were ongoing.

10 So we felt the need, we had to come up
11 with a more consistent way to provide guidance to our
12 staff, who are facing these reviews of what should be
13 the approach we ought to take when we are facing some
14 of these applications.

15 So that's what Research took us down on
16 this. So at a minimum this should give us pause as
17 reviewers and take into consideration some of the
18 things that are being highlighted before we decide to
19 accept some of the more complex integrated platforms.

20 CHAIR BROWN: And to your point, that you
21 made initially, it could be, depending on how somebody
22 read this, they could say well gee, it's allowed to do
23 this, relative to the voting level exception, and the
24 shared data exception, or it can be looked at the
25 other way, the Commission should be taking a harder

NEAL R. GROSS

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

1 line in terms of their review and saying oh no, that's
2 not what we meant and this is -- you have got to go
3 some other direction. So there's a dichotomy.

4 MEMBER STETKAR: My problem with the paper
5 quite honestly is that I don't understand what
6 independent means. There's some notion in this paper
7 underlying the paper of what independence means, but
8 I quite honestly don't understand what it means
9 because it seems to say that we must be absolutely
10 positively 100 percent independent except in these
11 other things where we don't need to be.

12 MR. REBSTOCK: Other than voting there
13 should be no influence from one channel to the other,
14 one --

15 MEMBER STETKAR: So can I have a single,
16 Train A pressurizer pressure sensor that sends
17 pressure signals to Trains A, B, C and D?

18 MR. REBSTOCK: No.

19 MEMBER STETKAR: Okay, we -- we license
20 plants to do that.

21 MR. REBSTOCK: There's a point in the
22 paper that talks about spatial distribution and there
23 is a problem with spatial distribution.

24 MR. RICHARDS: This is Stu Richards. Can
25 you give us an example? I'd like to track that down.

NEAL R. GROSS

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

1 MEMBER STETKAR: New plant designs do
2 that.

3 MR. RICHARDS: I'm sorry?

4 MEMBER STETKAR: New plant designs do
5 that. Dan?

6 MR. SANTOS: I am not familiar with the
7 specific example.

8 MR. RICHARDS: I need to go find out where
9 that plan is.

10 MR. SANTOS: If you are referring to the
11 -- the one I can think of is AREVA SP&D which has
12 spatial dependency that we can talk about, but not to
13 the one --

14 MR. REBSTOCK: Not to --

15 MR. SANTOS: It doesn't ring a bell, the
16 one on the pressurizer example of pressure that you
17 are --

18 MEMBER STETKAR: It is just a single --
19 they have four channels and each of the four channels,
20 the other channels.

21 MR. RICHARDS: Just to be clear, you are
22 saying that there's one pressure transmitter --

23 MR. REBSTOCK: It could be second worst
24 value type of -- it could be second worst value is
25 what you are referring to I think.

NEAL R. GROSS

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

1 MR. SANTOS: Oh, the second min second
2 max.

3 MR. REBSTOCK: Second min, second max,
4 yes. I call it second worst value --

5 CHAIR BROWN: Yes, you have that in the
6 discussion paragraph. Thank you.

7 MR. SANTOS: There is a design change on
8 the -- they are not going to propose that.

9 MEMBER STETKAR: Oh okay, I didn't -- I
10 have seen it. Anyway, okay. Maybe that's being treated
11 elsewhere.

12 CHAIR BROWN: Well, it's interesting, that
13 concept is an issue already in place in one of the
14 operating plants, so --

15 MR. REBSTOCK: But the purpose of this
16 paper wasn't to go back over designs that have already
17 been done. It was to look at it clean and say what do
18 we need?

19 MEMBER STETKAR: Going forward.

20 MR. REBSTOCK: Yes.

21 MR. SANTOS: And again, from a staff
22 perspective, there were too many definitions of what
23 independence meant. We are trying to improve upon
24 that.

25 At one end of the spectrum you get total

NEAL R. GROSS

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

1 isolation which is not necessarily the same thing. On
2 the other hand you only have people that independence
3 just meant I just need to deal with electrical and
4 communications independence.

5 And no regards for functional or data,
6 resource type issues.

7 CHAIR BROWN: That was the first comment
8 I got on one of the new design projects two months
9 after I got on this -- on the Committee. And I looked
10 at the -- I won't tell you the project.

11 MR. REBSTOCK: No I know that, but the
12 issue.

13 CHAIR BROWN: Well the issue, when I
14 looked at their setup on their reactor protection
15 system, I said you have put -- brought all these
16 signals together, and they said well, we meet the rule
17 because we have got electrical and physical
18 independence. They were electrically --= they had a
19 diode, or they used a fiber optic connector to send
20 their data stream through.

21 So they had to -- it was an optical data
22 stream but it still had to be converted at the other
23 end. So you start doing that, and the processor is
24 doing that, okay, because that's where the alogrithm
25 is.

NEAL R. GROSS

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

1 So as soon as you do that, you can stop
2 the whole thing, and if it will stop it in one voting
3 unit, it will stop it in the others. So and they said
4 well, we met the rules, so tough darts.

5 And they said well, we met the rule, so
6 tough darts.

7 MR. REBSTOCK: Well that's -- that's what
8 we are trying to get at, a ND that's what we are
9 talking about, know, the independence means that the
10 one channel does not influence the other.

11 CHAIR BROWN: And ISG 4 is the one the
12 talks about data communications independence as well
13 but it's not -- nobody -- it's just a guidance
14 document. It's not in the rule, and therefore they met
15 the rule, which is a little disturbing with the new
16 stuff.

17 If you went back a million years, when you
18 used relay logic, and you had four channels feeding a
19 relay and there were a bunch of contact, they didn't
20 -- there was no interference, no compromise at all.

1 MR. REBSTOCK: I would question whether
2 they meet the rule if they are crossing channels but
3 that's getting into second-guessing the design review
4 and I'm not even familiar with the --

5 CHAIR BROWN: I'll let you talk to the NRR

NEAL R. GROSS

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

1 staff on that or excuse me, the NRO staff, not me. So

2 --

3 All right, thank you Dan.

4 MR. SANTOS: Yes thanks.

5 CHAIR BROWN: John, you got anything else
6 right now, now that we have gotten -- we have vented?

7 (No response)

8 MR. REBSTOCK: Let me get back on track.

9 CHAIR BROWN: I will make one observation.
10 I agree with Dan that I think based on all the stuff,
11 and this is just my opinion, this is not either a
12 Committee opinion, Subcommittee or a Committee
13 opinion, it's just that the idea of what is
14 independence is not clearly understood amongst how we
15 are doing this. You get the stories that there's
16 various thought processes, and this is a useful tool
17 to get the whole issue back on the table along with
18 all the references to the Code of Federal Regulations
19 as well as the IEEE standards and your reg guides.

20 MR. REBSTOCK: That was the objective.

21 CHAIR BROWN: So I think that's -- and we
22 have just -- John just identified a couple of, a
23 little bit of what you could call inconsistencies and
24 I just enumerated or expanded on what those
25 inconsistencies meant.

NEAL R. GROSS

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

1 Now the whole point of the shared data,
2 you could have one piece of data coming in and going
3 to everybody.

4 MEMBER STETKAR: I come back to regulatory
5 kind of consistency in terms of what designers have to
6 understand they design to. This notion of a single
7 faulty bit stream hanging out multiple processors is
8 something that I would characterize as violation of a
9 single-failure criterion, because that's a single
10 failure.

11 However some of the stuff I read in the
12 paper seems to say that we need to design the systems
13 -- the single failure is a concept but we need to
14 think of multiple failures.

15 That is a fundamental change because that
16 says that we can't have -- you know, we can't have
17 plants that have four identical diesel generators in
18 them, because they are susceptible to multiple common
19 cause failures.

20 So you have to be careful --

21 MR. REBSTOCK: Yes, I am not sure where
22 that is in the paper that you are getting to that.

23 CHAIR BROWN: No, there is a point -- no,
24 John is exactly right. There was a point at which you
25 -- some might argue that the transmittal of inaccurate

NEAL R. GROSS

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

1 data and the failure to flag those data as inaccurate,
2 two things -- the transmittal of inaccurate data or
3 corrupt data, and the failure to flag those data as
4 inaccurate, constitute two failures. That's on --
5 that's the first sentence of the first paragraph on
6 page 15.

7 MR. REBSTOCK: Yes, I remember writing
8 that.

9 CHAIR BROWN: Under 4.1.

10 MR. REBSTOCK: I think it also says that
11 we don't buy that.

12 CHAIR BROWN: No, you are considering it
13 one failure.

14 MR. REBSTOCK: You're sending the wrong
15 information --

16 CHAIR BROWN: Now I don't know whether
17 everybody would agree with you on that, but now that
18 your little paper has been -- not little paper, excuse
19 me -- the paper has actually been signed or whatever,
20 final version, so I think that's what you are talking
21 about John, relative to this --

22 MEMBER STETKAR: Well, there's several --

23 CHAIR BROWN: That is the only one I
24 remember that --

25 MEMBER STETKAR: It's -- and I have to be

NEAL R. GROSS

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

1 careful because the revised version of the paper we
2 have today may be those words so --

3 CHAIR BROWN: Should I check those words
4 again?

5 MEMBER STETKAR: I'm out on the record. No
6 this is --

7 CHAIR BROWN: No, that's the same.

8 MR. REBSTOCK: I know that part didn't
9 change.

10 MEMBER STETKAR: Bear with me here because
11 I don't want to misquote something on the public
12 record here. Let's go on because the words have
13 changed enough that the quote that I pulled out has
14 been softened enough that you could -- well, let me --

15 CHAIR BROWN: Where is it John?

16 MEMBER STETKAR: This is in section 4.1 I
17 think it is, oh that's it. Let me just get the page
18 number correct. Yes, it's section 4.1 and I've lost
19 my place again.

20 In addition the requirements cited above
21 do not stop at the single-failure criterion. They work
22 together to require that redundant channels perform
23 the safety functions independently, and they do not
24 include provisions for mitigation of that requirement.
25 That sounds okay.

NEAL R. GROSS

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

1 Conformance to the single-failure
2 criterion is necessary to achieve this, but is not
3 necessarily sufficient, it says that you are now
4 requiring --

5 CHAIR BROWN: That's the sentence that's
6 right after the earlier one. Same paragraph.

7 MEMBER STETKAR: So there's a lot of
8 implications in here that says we are now going to
9 require people to think more than single failures in
10 terms of the licensing basis for these systems.

11 MR. REBSTOCK: Well, the issue
12 specifically is independence and what that is
13 referring to is the need for independence.

14 MEMBER STETKAR: Are four diesel
15 generators independent?

16 MR. REBSTOCK: If they are not connected
17 together. Independence and common cause failure are
18 two different things, or --

19 MEMBER STETKAR: Why is that?

20 MR. REBSTOCK: What we are talking about
21 if one of those four diesels has some problem, and
22 it's not connected to the other ones, then it won't
23 bring the other ones down.

24 MEMBER STETKAR: Suppose it's a common --

25 MR. REBSTOCK: If they all --

NEAL R. GROSS

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

1 MEMBER STETKAR: Suppose it's a common
2 problem?

3 MR. REBSTOCK: Then they will all come
4 down. That's --

5 MEMBER STETKAR: Unrelated problems such
6 that under those conditions all four of them fail.

7 MR. REBSTOCK: Right, and that's the same
8 issue that has existed for all eternity as far as
9 common cause failures are concerned. It has nothing to
10 do with digital.

11 MEMBER STETKAR: That's right, and that's
12 why our design and licensing -- our licensing criteria
13 say that common cause failures are beyond design basis
14 events, that the designers don't have to think of them
15 in design space, deterministic design space.

16 We have the single-failure criterion and
17 unavailability of the second train due to maintenance
18 -- as kind of a surrogate to get around a little bit
19 of that stuff but not address it completely, and my
20 question is, in terms of this paper, are we creeping
21 into that gray area between the single-failure
22 criterion and needing to design systems as resistant
23 to common cause failures, within the construct of a
24 part of the design. I am not talking about diverse
25 actuation systems, because that's a --

NEAL R. GROSS

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

1 MR. REBSTOCK: Yes, I understand what you
2 are saying.

3 MEMBER STETKAR: That's in a sense an
4 add-on to address that common cause issue.

5 MR. REBSTOCK: Yes.

6 CHAIR BROWN: One of the arguments the
7 designers, the applicant was making on these serial
8 data systems, is that they have checks on them, they
9 have -- what is it -- cyclic redundancy checks and
10 therefore the data is checked, and the answer in
11 reality is all you are doing is confirming that if you
12 send bad data, that you receive bad data on the other
13 end.

14 MR. REBSTOCK: That you receive the same
15 bad data, yes.

16 CHAIR BROWN: That's all they do. They --
17 so if it's corrupt, it's corrupt. And they say oh, I
18 got this great corrupt data that I'm not going to go
19 use, so that the argument falls apart, but yet where
20 is the dividing line on that single-failure criterion
21 mode as you have discussed here, I mean it can be
22 corrupt or it can be bad data or whatever, and the
23 idea that it brings down all four -- is that a common
24 cause because the data is corrupt and will bring them
25 all down? That's almost a single common cause failure

NEAL R. GROSS

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

1 because there is something within that set of data
2 that makes all the processors respond the same way.

3 MR. REBSTOCK: That wouldn't even be
4 common cause. That would be -- that would be just a
5 single failure.

6 MEMBER STETKAR: No, that's -- a single
7 failure.

8 MR. REBSTOCK: It's also a terrible
9 design.

10 CHAIR BROWN: And yet I would look at on
11 the diesel generator side, is that I've got four
12 independent diesel generators, they are all not
13 connected, there's no communication between them,
14 therefore I wouldn't -- common cause failures are not
15 as -- don't kill me when I say this --- are not as
16 likely in those circumstances, and all I'm saying is
17 in the digital systems when you --- it's more likely
18 when you are doing those things than it is in the
19 diesel generator case when there is no communication
20 between the various systems.

21 Now that doesn't mean you can't have a
22 shaft that is just waiting to break or what have you.

23 MR. REBSTOCK: You've got weak oil seals
24 but they still won't fail at the same time.

25 MEMBER SIEBER: Synchronous common-cause

NEAL R. GROSS

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

1 failures are very remote but if you have a defect of
2 a diesel or anything else, that's common to all
3 devices of that brand, sooner or later they are going
4 to fail but they won't fail simultaneously.

5 CHAIR BROWN: Well, you can make the same
6 argument relative to -- people tried to make the same
7 argument relative to the serial data stream.
8 Unfortunately they are being transmitted every 30 or
9 50 milliseconds so it's not -- they are all going to
10 see it within the time frame of having to respond and
11 you're going to corrupt all of them and none of them
12 will trip, you won't get them in time, so anyway. Now
13 that we have done it we will --

14 MR. REBSTOCK: I would seek to avoid that
15 design in that situation.

16 CHAIR BROWN: Okay, I don't disagree. You
17 can proceed on now.

18 MR. REBSTOCK: Okay, we pretty much, I
19 think, took care of a lot of this. Oh, one of the
20 claims also has been made is that systems are
21 dependent, one system needs information from another
22 but if it's not getting it, then it will execute the
23 trip immediately.

24 And my response to that is the system that
25 is supposed to be removing the information, if the

NEAL R. GROSS

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

1 line breaks and it gets nothing, then fine. But if it
2 is getting bad information it has no way of knowing
3 that it's bad information.

4 CHAIR BROWN: Well that was what we just
5 talked about, just now, the same issue.

6 MR. REBSTOCK: Yes, another aspect of it.
7 So what we say, if putting together the prior logic,
8 the regulations, the guidance the practical reasoning,
9 is that each independent channel has got to be capable
10 of performing its safety function without the
11 participation of anything outside and without the need
12 for anything from outside.

13 MEMBER STETKAR: This means that voting is
14 not allowed.

15 MR. REBSTOCK: Voting is a different
16 issue.

17 MEMBER STETKAR: I just don't understand
18 that. You are going to have to convince me why voting
19 is a different issue.

20 MR. REBSTOCK: How can you vote if you
21 can't get information from the other channels? The
22 whole reason you have got four channels --

23 MEMBER STETKAR: The issue is you can vote
24 but you have got to do it to maintain independence.
25 That's where the hangup is. You have got to maintain

NEAL R. GROSS

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

1 --

2 MR. REBSTOCK: Your data stream issue is
3 -- I will concede that. A system that can transmit a
4 data stream like that that can clobber the process or
5 is not a good thing. That's not a voting problem.
6 That's a communication problem, a system architecture
7 problem.

8 CHAIR BROWN: Exactly, but you don't have
9 to do that so my point being, and John's point I think
10 is you can make voting still independent based on the
11 way you transmit or the way you communicate the data,
12 and how you execute with that data. That's where the
13 hangup comes.

14 MR. REBSTOCK: In 1975, when we designed
15 the SNUPPS plants we had relay logic, and the relay
16 logic took relay outputs from all four channels in the
17 one channel and it either did or did not open the
18 reactor trip breaker.

19 CHAIR BROWN: Yes, but that couldn't
20 corrupt.

21 MR. REBSTOCK: It couldn't corrupt
22 anything.

23 CHAIR BROWN: That's right so there was
24 just --

25 MR. REBSTOCK: The corruption doesn't come

NEAL R. GROSS

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

1 from the voting. The corruption comes from bad
2 communications in your example.

3 CHAIR BROWN: No, in this case it was the
4 contacts were okay because you had two out of four
5 voting logic ladders out of the relay contacts.

6 MEMBER SIEBER: And the point of
7 combination was the voting relay itself and you could
8 also do the same thing in digital systems as long as
9 the communications channels were independent.

10 MR. REBSTOCK: Well of course you can.
11 That's what you need to do.

12 MEMBER SIEBER: That's the equivalent
13 digital system. And I think that's legal under --

14 CHAIR BROWN: Microprocessor-based voting
15 systems have been used. I have personally associated
16 with those, but yet not based on serial data streams.
17 They were based on equivalent of analog signals that
18 went into, you know, what I call AtoD regular AtoD
19 converters, it's like getting a switch contact.

20 MR. REBSTOCK: Yes, that's what the ISG 4
21 communications process essentially does.

22 CHAIR BROWN: Right, yes, except well I
23 don't want to go --

24 MR. REBSTOCK: But you are saying you know
25 somebody that doesn't use it.

NEAL R. GROSS

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

1 CHAIR BROWN: Yes.

2 MR. REBSTOCK: That's another story.

3 MEMBER SIEBER: That's a different issue
4 altogether.

5 CHAIR BROWN: John's point is, is that
6 voting -- why isn't voting included in the idea of
7 independence. That's the point we are trying to make
8 where you have kind of excluded that.

9 MR. REBSTOCK: I don't mean to exclude it.
10 The voters themselves need to be independent of one
11 another. The issue is the point of the logical
12 concept, the voting, means that you are looking at
13 inputs from all of the channels and deciding what to
14 do. That logical concept is inherently cross-
15 divisional. The two voters certainly shouldn't be
16 talking to one another.

17 CHAIR BROWN: Not the way your stuff is
18 worded.

19 MEMBER STETKAR: It doesn't necessarily
20 mean that and my concern is if the agency is adopting
21 this position of absolutely strict independence
22 required, that you have to think about what the
23 implications of that may mean in design space.

24 For example I can have four channels, each
25 channel has four of its own sensors.

NEAL R. GROSS

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

1 MR. REBSTOCK: Right.

2 MEMBER STETKAR: Because you are worried
3 about spurious signals, you are worried about
4 maintenance and things like that, so each channel can
5 vote two out of four of its sensors and say okay, I
6 have a channel A trip now. It doesn't communicate to
7 any of the other channels.

8 MR. REBSTOCK: Okay.

9 MEMBER STETKAR: It finally gets down to
10 a set of actuation devices for that pump that says I
11 need two out of the four of those other -- two out of
12 four channels.

13 MR. REBSTOCK: Okay.

14 MEMBER STETKAR: You're not cross-
15 communicating until you finally get to the circuit
16 breaker for the pump.

17 MR. REBSTOCK: So you have got 16 sensors
18 and 16 channels and four voters and everything in
19 parallel.

20 MEMBER STETKAR: That's right. Uh-huh.
21 Yes. Yes. Now --

22 MR. REBSTOCK: That's not the way we do
23 it. But -- I said that's not the way, that's not the
24 way we have been doing it for --

25 MEMBER STETKAR: You're right, it's not

NEAL R. GROSS

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

1 the way we have been doing it, but taken to an
2 extreme, that is much more independent than the way we
3 have been doing it, and that's a bit of the concern
4 that I have in terms of going forward with this sort
5 of --

6 MR. REBSTOCK: If this paper were to go to
7 the level of becoming law, we would need to reword
8 that issue of voting very carefully.

9 MEMBER STETKAR: Absolutely.

10 MR. REBSTOCK: The intent right now is to
11 get the concept out there.

12 MEMBER STETKAR: Yes, okay. Okay. Okay. I
13 think some of that -- some of the words are important
14 because this -- without the part that is on the screen
15 right now, without the participation of any component
16 means zero.

17 And without the need for information from,
18 connection to proper operation of any equipment
19 outside of its own safety division. That could be
20 interpreted as my sort of conceptual design is the
21 only acceptable conceptual design.

22 MR. REBSTOCK: Right, this is at the
23 sensing channel level.

24 MEMBER SIEBER: Right, and the over is not
25 part of that.

NEAL R. GROSS

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

1 MR. REBSTOCK: Is not part of the sensing
2 channel.

3 MEMBER SIEBER: Right.

4 CHAIR BROWN: And our point is the voting
5 needs to be included in some way, shape or form in
6 terms of of how you are going to accept it. You have
7 got to come to the conclusion as to what you are going
8 to allow.

9 (Simultaneous speaking.)

10 MEMBER SIEBER: -- control a single
11 component when you are done.

12 MR. REBSTOCK: Yes, ultimately there is
13 just one --

14 MEMBER SIEBER: The voter belongs to the
15 component as opposed to belonging to any or all --

16 MEMBER STETKAR: There are many different
17 ways to design it and I am not proposing designs, I am
18 trying to get what the basic philosophy of this white
19 paper is and how it may be interpreted in terms of
20 licensing requirements --

21 MR. REBSTOCK: Yes, it is looking at
22 sensing gaps --

23 MEMBER STETKAR: -- regardless of how
24 those licensing reviews are implemented.

25 MEMBER SIEBER: The intended philosophy

NEAL R. GROSS

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

1 may be different than the way it is interpreted.
2 That's really what you are trying to straighten out.

3 MR. REBSTOCK: Yes.

4 MEMBER SIEBER: So we have to be careful
5 with the words.

6 CHAIR BROWN: One other way of looking at
7 that okay in terms of future thought process, however
8 this paper gets utilized to develop the design space,
9 is if you are going to use microprocessors, and you
10 are going to use any type of a data stream which could
11 possibly corrupt the operation of the processors
12 themselves, stop them and lock them up, you have to
13 have a system where if all -- that's a design
14 consideration. All four voting units lock up, how do
15 you guarantee a trip.

16 MR. REBSTOCK: Personally I would rather
17 not see a system that --

18 CHAIR BROWN: I would rather not do that
19 but that was what we were forced to --

20 MR. REBSTOCK: that was possible, and as
21 far as what's already been reviewed, I --

22 CHAIR BROWN: I am just saying, what's
23 already been reviewed, we've found a method where that
24 happens. You can argue for good or for worse, it may
25 not be a good design in terms of my personal opinion,

NEAL R. GROSS

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

1 but it does have a second layer, call it defense-in-
2 depth if you want, but it's in the wrong place.

3 MR. REBSTOCK: The second layer is not a
4 bad thing --

5 CHAIR BROWN: That's right, it's just how
6 it's done is -- what you have to depend on is what you
7 would just as soon not. You would much rather have the
8 channels and the voting system be totally independent
9 so that one can't compromise -- any division voting
10 that says not voting but says trip, can't compromise
11 all four of the voting units.

12 MR. REBSTOCK: Right. That's a fundamental
13 principle that I'm trying to get across.

14 CHAIR BROWN: Well that's -- and we are
15 pointing out that that's not real clear when it comes
16 to the voting units side.

17 MR. REBSTOCK: I understand.

18 CHAIR BROWN: And the shared-data side is
19 another issue in itself. Anyway --

20 MR. REBSTOCK: If this goes to a next
21 step, we'll have to have a much bigger section on
22 voting.

23 CHAIR BROWN: Okay.

24 MR. REBSTOCK: I think that the conclusion
25 that we have drawn is reaffirmation of existing

NEAL R. GROSS

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

1 regulations. There's nothing new about it. There's not
2 a new regulatory position, and I don't see a need for
3 a new rulemaking.

4 I do think that --

5 CHAIR BROWN: New rulemaking, that's
6 interesting, because I think based on the discussion,
7 somehow that thought process and the rules that exist
8 today, are I mean, the rules today don't really cover
9 anything other than electrical isolation and separate
10 -- and physical isolation.

11 The other part of independence is not
12 covered at all so I would disagree with that statement
13 right now.

14 You have got reg guides, but they are not
15 rules.

16 MR. REBSTOCK: They are not -- that's
17 right. That's right.

18 CHAIR BROWN: I would disagree with that
19 based on just going to the digital systems period, or
20 the microprocessor-based systems, software control in
21 other words, as opposed to combinational logic --

22 MR. REBSTOCK: A sequentially-controlled
23 system raises issues. I think the independence
24 requirements as they are written are applicable.
25 Personally, I wouldn't mind seeing more specific rules

NEAL R. GROSS

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

1 --

2 CHAIR BROWN: Well, my point being that
3 the data communications aspect now is not part of the
4 rules.

5 MR. REBSTOCK: No, the -- there's no rule
6 specific on data communications. There is some motion
7 to make some but --

8 CHAIR BROWN: Right, but electrical
9 isolation was able to be met with the older analog
10 systems, and that meant you had data isolation as
11 well. That's the only point so there was -- one
12 captured both.

13 MR. SANTOS: This is Dan Santos, NRO. I
14 think -- correct me if I am wrong -- but what Paul is
15 trying to say that you can accommodate what some of
16 the points Paul is saying, under the existing rules.
17 Maybe we need to strengthen some of the words and
18 clarification, but to do what Paul is suggesting can
19 be accommodated under existing rules.

20 CHAIR BROWN: If you can get the
21 applicants to not call your hand by saying I meet the
22 electrical and physical isolation requirements of your
23 rule.

24 MR. SANTOS: And that's correct, and it
25 has been very --

NEAL R. GROSS

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

1 CHAIR BROWN: And if you are not -- if you
2 can't stand up and say wrong, then you have a problem
3 and today that is what's going on.

4 MR. SANTOS: And you will see later, I
5 don't know when you are going to see some recent
6 applications with EPR and ABWR where you are going to
7 see some of that very challenging dialogue going on
8 and applicants making design decisions based on those
9 interactions.

10 MR. REBSTOCK: One key thing that I would
11 like to say, I think that the existing rules do cover
12 what's needed. That doesn't mean that there's no room
13 for improvement. But I don't want to say if -- I am
14 not willing that the existing rules permit a
15 free-for-all in digital design. I don't think that's
16 true.

17 CHAIR BROWN: I got that twice, three or
18 four different meetings, where I was told they met the
19 specific rule and that's all they were required to do.

20 MR. REBSTOCK: Okay, I --

21 CHAIR BROWN: That's personal experience,
22 there's -- okay, and I will tell you outside the forum
23 of this meeting which projects they were if you want
24 to know although I said it in those meetings as well.

25 MR. REBSTOCK: I have a hunch I know what

NEAL R. GROSS

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

1 you are referring to so --

2 CHAIR BROWN: So anyway --

3 MR. REBSTOCK: Personally I am not sure
4 the they do meet -- but that's --

5 CHAIR BROWN: Let's get on with it. Thank
6 you Dan.

7 MR. REBSTOCK: Okay, some corollary
8 observations. We have seen cases where people claim to
9 have made some design feature that is supposed to
10 improve the system's performance but doesn't
11 necessarily support independence or causes complexity
12 in the design and so on.

13 I would say any provision that improves
14 the performance but also increase the probability of
15 system failure, should be viewed with skepticism. If
16 it works better when it's working that's great, but if
17 it's more likely to not work that is not so good.

18 I think we need to distinguish between
19 safety performance and economic performance. An
20 example, some feature may improve the accuracy of some
21 measurement, but at a cost of compromising
22 independence or compromising reliability.

23 The improved accuracy is certainly a good
24 thing. It's hard to argue against better accuracy in
25 your instrumentation. But the benefit to safety isn't

NEAL R. GROSS

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

1 necessarily there.

2 The less accuracy, the less accurate
3 system, if it's more reliable -- you can compensate
4 for the lack of accuracy by adding safety margin. So
5 you come out ahead.

6 (Simultaneous speaking.)

7 CHAIR BROWN: -- you don't really increase
8 the safety margin you just include the worse accuracy
9 in your analysis.

10 MR. REBSTOCK: That's what I mean by
11 safety margin. You move the set point further away
12 from --

13 CHAIR BROWN: If it's not accurate, you
14 can't really call it margin. Personal opinion again.

15 MR. REBSTOCK: Okay, okay, I'm talking
16 about the difference --

17 CHAIR BROWN: You compensated for the poor
18 nature of the instrumentation --

19 MR. REBSTOCK: Yes, bad things happen
20 here, if you have really accurate instruments you can
21 go to here. If you have not so accurate instruments
22 you can only go to --

23 CHAIR BROWN: Go to there, but the margin
24 stays the same.

25 MR. REBSTOCK: Okay, there's a difference

NEAL R. GROSS

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

1 in the use of the word margin.

2 CHAIR BROWN: I'm picking, I'm picking at
3 a few nits here. Every now and then I do that.

4 MR. REBSTOCK: Yes. But the point is that
5 the improved accuracy doesn't necessarily give you a
6 safety benefit, and it's the safety benefit that is
7 important in the issues that we are talking about
8 here.

9 I have also heard references to installing
10 things, digital systems under 50.59 and in my personal
11 opinion, I think that it can be rather difficult to
12 demonstrate that a digital system is necessarily a
13 one-for-one replacement for an analog system, and
14 doesn't introduce some new kind of failure mode or
15 some new kind of unexpected operation that would fall
16 under the screening of 50.59.

17 Digital systems are fundamentally
18 different. At the terminals, they may look very much
19 the same as an analog system they replace, but they
20 operate differently, they have different ways of
21 failing, and I would question how well it would -- how
22 easily a digital system would screen out under a 50.59
23 review.

24 As I say this is an observation, it's not
25 a conclusion of the paper, just something to think

NEAL R. GROSS

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

1 about.

2 And then some additional concerns that
3 came up in the process of working through this.
4 Hardware complexity. If you look at the input circuit
5 cards on a digital system, the input modules, or the
6 digital modules, not just the input modules but the
7 whole system itself, the circuit cards, much higher
8 parts count. They include programmable control
9 components, they use firmware. It means they have
10 software built into them. They have programming. They
11 are state-based systems.

12 The devices are much more complex than the
13 analog devices that they purport to replace and I
14 raise a question and I don't know the answer, but I
15 think it's something for further consideration, is
16 perhaps some of the concerns that we have about
17 software should also apply to some of these highly
18 complex hardware modules.

19 Adversity considerations also. If you have
20 got a system -- you have got two different systems
21 that provide two different ways of protecting the
22 plant. So they are diverse systems.

23 If you execute them on the same
24 microprocessor, the diversity is shot. So there can be
25 diversity considerations that are altered by the use

NEAL R. GROSS

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

1 of digital systems that were fine in the analog world.
2 More things to think about.

3 CHAIR BROWN: Okay. Any other questions?
4 Jack? John?

5 MEMBER SIEBER: No.

6 CHAIR BROWN: Joy?

7 (No response)

8 CHAIR BROWN: Thank you very much Paul for
9 another dynamic, interactive discussion.

10 MR. REBSTOCK: Interesting discussion.

11 CHAIR BROWN: Well, it's a --

12 MR. REBSTOCK: I'm going to write up
13 something on voting logics.

14 CHAIR BROWN: Yes.

15 MR. CONCEPCION: All right. My name is
16 Milton Concepcion. I am with the Office of Research
17 and I am going to spend a couple of minutes discussing
18 section 3.4 of the research plan which is knowledge
19 management. I am going to try to go as quickly as
20 possible and try to be on schedule.

21 What I am going to focus this afternoon is
22 on the first four research projects that are ont the
23 slide. Since Karl already briefed the Subcommittee on
24 operating experience so basically I am going to talk
25 about emerging technologies and what we are doing,

NEAL R. GROSS

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

1 collaborative and cooperative research, standards
2 development, reg guides and regulatory reviews, and
3 last but not least, organization of regulatory
4 guidance, which already created some interesting
5 discussions in the morning.

6 On the survey of emerging technologies, we
7 have this ongoing project that explores cutting-edge
8 technology and advancements in established technology
9 to keep up with the rapid pace of I&C systems, and
10 also to stay abreast of new methods and criteria
11 needed to assess the safety of I&C systems.

12 These reports identify and assess as I
13 said state of the art technology and provide high-
14 level discussions on specific emerging capabilities
15 and products in different technology areas including
16 capabilities that are likely to be included in safety-
17 related applications in nuclear plants, through
18 upgrades or through new reactor activities.

19 In addition, the surveys serve as a
20 vehicle to keep the staff abreast of evolving
21 technology and new industry initiatives, including new
22 tools and techniques and practices that apply to
23 design evaluation of I&C systems.

24 As stated on the slide, there have been
25 three NUREG/CR reports published, one in 2003, one in

NEAL R. GROSS

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

1 2006 and the latest in 2009. The focus of these
2 reports is varied and covered areas such as sensors
3 and measurements, communications, media and
4 networking, microprocessors and other integrated
5 circuits, computational platforms, surveillance,
6 diagnostics and prognostics -- you heard a little bit
7 of that also this morning -- human-system
8 interactions, integrity software and I&C architectures
9 in new plants.

10 We are using the results of these survey
11 reports as a starting point for identifying research
12 opportunities in situations where there is an emerging
13 technology that we feel could migrate into the nuclear
14 field in nuclear power plants.

15 CHAIR BROWN: Is the purpose of this to
16 make sure you are all aware of, or have some
17 capability of evaluating --

18 MR. CONCEPCION: Correct.

19 CHAIR BROWN: how to handle these when
20 applicants present them as part of their -- you know,
21 build their systems from these?

22 MR. CONCEPCION: That's correct. And
23 finally on this slide, the next survey report is
24 scheduled for Fiscal Year 2013. We typically do a
25 three- or four-year cycle on these reports, and that's

NEAL R. GROSS

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

1 the next one coming up in 2013.

2 Collaborative and cooperative research. We
3 want to say that we are doing a lot of cooperative
4 activities, I believe more than we use to, as I heard
5 before that I guess we were highly criticized of not
6 reaching out and collaborating with either nuclear and
7 non-nuclear stakeholders.

8 Dr Birla's presentation also mentioned the
9 expert elicitation process which has allowed us to
10 maintain and expand our working relationships with
11 domestic and international entities with a substantial
12 amount of experience, developing and using I&C
13 systems.

14 These entities include nuclear regulatory
15 -- industry organizations, regulatory authorities,
16 federal agencies, academic institutions and National
17 Laboratories and intergovernmental organizations such
18 as the Nuclear Energy Agency and the International
19 Atomic Energy Agency.

20 What we are trying to do with this project
21 is maintain openness and continuously expand
22 cooperation efforts, exchange information and learn
23 from different sources outside the nuclear industry
24 and evaluate its relevance to the nuclear industry,
25 and also develop additional technical basis for

NEAL R. GROSS

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

1 decisions regarding current and new digital system
2 designs and technologies for safety-related
3 applications.

4 And as you can see on this slide, it's a
5 little busy, but, and some of these organizations have
6 been already in previous presentations, but I will
7 provide specific examples from some of the activities
8 where collaboration efforts are ongoing.

9 For example, we mentioned the NASA and the
10 Jet Propulsion Laboratory cooperation with -- related
11 to operating experience events, and data-exchange.
12 There's also the Networking Information Technology
13 Research and Development, which is also cooperating
14 with us in the area of operating experience, as well
15 as COMPSIS.

16 Also we have cooperations with the Halden
17 research project which is a project sponsored by
18 research. They have established a software engineering
19 laboratory which provides systems and resources needed
20 to support research and development assessment,
21 consultancy and training related to safety-related I&C
22 systems and safety-oriented software engineering.

23 Also, the French Institute of Radiological
24 Protection, IRSN, as you heard from Luis this morning,
25 IRSN and the NRC began exchanging information and

NEAL R. GROSS

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

1 cooperation in I&C last year.

2 We identified an interest in sharing
3 understanding of digital I&C system fault modes
4 attributable to computer logic in I&C systems for
5 safety functions and the NUREG-0254 is an example of
6 those cooperation activities as you saw in Luis'
7 presentation this morning.

8 Two more examples, one of them is the
9 Safety-Critical Software Task Force. This task force
10 is trying to improve technical consistency in safety
11 assessments of software and digital I&C systems.

12 Participants include regulatory bodies
13 from UK, Belgium, Spain, Sweden, Germany, Finland,
14 France and the U.S. We have representation from from
15 Research as well.

16 Collaborations include comparisons of the
17 countries' respective licensing approaches,
18 identifying areas where consensus already exist, and
19 explore how greater consistency and more mutual
20 acceptance could be introduced into the current
21 licensing practices.

22 Last example I have to show here is the
23 Software Certification Consortium. This consortium
24 attempts to understand certification issues with
25 respect to systems that contain significant software

NEAL R. GROSS

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

1 components and make recommendations on processes and
2 standards that have an impact on the certification of
3 such systems.

4 The consortium is particularly interested
5 in certification of systems in medical devices,
6 nuclear power plants, automotive and aerospace
7 industries and they have representation from each of
8 these sectors.

9 These interactions have allowed us to look
10 at industry-specific issues and share ideas between
11 the different domains and levels of regulation.

12 And as always we continue to pursue and
13 expand potential opportunities for collaborative
14 efforts and pilot projects with parties that have
15 shared safety interests with the NRC.

16 In the area of standards, development and
17 -- before I move in, I want to say that in the short
18 term, some of the things that we will be doing short
19 term for collaborative and cooperative activities,
20 there's a publication of the NUREG-0254 as mentioned
21 this morning, continue the in-depth analysis of
22 operating experience as presented by Karl, and
23 initiate research collaboration with IRSN on criteria
24 for evaluation of software for systems of the highest
25 safety classification. Forgive the lengthy title but

NEAL R. GROSS

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

1 --

2 In terms of long-term activities, we will
3 continue with the publication of this RIL series of
4 technical reports. We will pursue additional joint,
5 technical reports as well as joint workshops with
6 industry and the NRC, and enable the structures for
7 potential migration of the results of these reports
8 into standards-development organizations which is my
9 next slide.

10 So what we are doing with the
11 standards-development, basically we are trying to
12 enhance the consistency of existing regulatory
13 guidance by leveraging cooperation among standard
14 development organizations who are responsible for
15 coordinating and maintaining consensus standards.

16 CHAIR BROWN: Is that within the U.S. or
17 is this including -- I mean you use U.S. standards for
18 the most part I guess.

19 MR. CONCEPCION: Yes, and I will get into
20 both domestic and international activities. But there
21 is an OMB, Office of Management and Budget circular,
22 A-119 that basically establishes the policies on the
23 federal use and development of voluntary consensus
24 standards.

25 And what we are doing in research is we

NEAL R. GROSS

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

1 are evaluating our staff participation in domestic and
2 international consensus standards and providing
3 recommendation to the licensing offices to maximize
4 such participation.

5 We have developed a draft strategic plan
6 for improved use of consensus standards in order to
7 strengthen that participation. NRR and NRO already
8 provided comments. We sought comments from -- and we
9 are in the process of potentially piloting that plan
10 in future activities.

11 What we are trying to get out of this
12 project is to continue to evaluate national standards,
13 improve the efficiency of the regulatory process and
14 gain knowledge from other application sectors and
15 standards outside the nuclear industry, establish
16 priorities and identify opportunities to expand
17 interactions with standard development organizations,
18 identify our own needs for standards, to address
19 specific technical issues, new technologies or new or
20 revised regulatory guidance, develop initiatives for
21 timely endorsement of standards in regulatory guides,
22 create and support partnerships to leverage
23 opportunities and promote compliance with
24 international consensus standards where applicable,
25 and along those lines, I have two examples to provide.

NEAL R. GROSS

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

1 We maintain participation in IEEE Working
2 Group 6.4 which is responsible for IEEE 7432, which
3 provides criteria for digital computers in safety
4 systems of nuclear power plants.

5 We are also maintaining staff presence and
6 participation in IEEE 603, which provides functional
7 design criteria for safety systems.

8 Now expanding it to international
9 activities, we will continue to participate and
10 leverage that knowledge collected with our
11 participation in international activities.

12 It is well known that foreign utilities
13 use I&C technology and they are gaining approvals
14 under their regulatory processes, often using
15 international standards and what we are trying to do
16 is to review those international standards and
17 leverage cooperation with those international entities
18 to apply that knowledge into our own regulatory
19 process.

20 I have two examples of those as well. We
21 have provided comments to one, IAEA working group
22 response responsible for the update of a guide, and I
23 guess I can provide a title, instrumentation and
24 control systems important to safety in nuclear power
25 plants.

NEAL R. GROSS

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

1 And we also provided comments to an IEC
2 standard. The is the one that was mentioned earlier
3 about FPGAs. It's IEC 62566, which discusses --
4 provides guidance for the selection and use of complex
5 electronic components for system-performing category
6 A functions, which is basically safety-related
7 functions.

8 No questions so far.

9 CHAIR BROWN: I haven't gotten to it. I'm
10 letting you finish.

11 MR. CONCEPCION: Oh, okay. Okay. Last but
12 not least, I happen to be the project manager of this
13 effort and I guess I will get questions from it.
14 Basically what we are doing is we are reviewing our
15 existing regulatory framework and Oak Ridge is helping
16 us all of the guidance associated with I&C and do a
17 correlation of regulatory requirements all the way
18 down to regulatory guides and including standards that
19 are being endorsed by those regulatory guides.

20 As I said, Oak Ridge is working with us.
21 We just had a kick-off meeting last week. We discussed
22 our expectations. They discussed a preliminary plan
23 that attempts to do the review in the next couple of
24 months.

25 But the review, and I don't want to I

NEAL R. GROSS

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

1 guess over-promise and under-deliver, the review has
2 not taken place. This effort started in March of this
3 year. We just had a kick-off meeting. And the goal is
4 to have a comprehensive report that will feed into
5 what we will call an electronic database for technical
6 reviewers to have access, or I guess more
7 accessibility to the regulatory requirements and
8 guidance related to digital I&C, I&C in general,
9 Chapter 7, includes -- chapter 7 as I said all of the,
10 Branch Technical Positions, reg guides associated with
11 I&C, NUREGs, SECY papers, generic letters, Regulatory
12 Information Notices, ISGs and industry standards.

13 But yes --

14 CHAIR BROWN: Just tell me when you are
15 finished.

16 MR. CONCEPCION: But the review has not
17 started. The goal -- we have engaged with the Office
18 of Information Services which will help us develop
19 this electronic tool, but as I said, we are just in
20 the beginning phases of this effort.

21 CHAIR BROWN: Now are you ready?

22 MR. CONCEPCION: I'm ready.

23 CHAIR BROWN: okay, my concept of
24 knowledge management has always been, based on some
25 other applications, some other work, has been the

NEAL R. GROSS

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

1 ability to correlate and focus in specific areas, pick
2 you area, whatever it is, what information is
3 available and the type of information available in
4 whatever little packet you've got, of whatever the
5 knowledge is you want to deal with -- area knowledge.

6 And I can only this as being a new member
7 three years ago and walking in here and trying to
8 figure out what in the world I was supposed to use,
9 and where to access it, and there was absolutely zero
10 index or table of contents and people said well,
11 here's a bunch of ML numbers. Well, what are those?
12 There's no titles with them. Here's some reg guides.
13 Well, which ones are those, there were no titles.

14 I didn't even -- where do I find the reg
15 guides, what sets out an overall hierarchy that says
16 the Code of Federal Regulations, Part 50.55(a)(h) or
17 whatever the heck it is, that says okay, here's the
18 general design criterion, under that there's four of
19 them, or five them, or six of them that have
20 particular relevance to the instrumentation control.

21 Forget digital versus analog and then from
22 that you branch down to reg guides, ISGs, NUREGs with
23 a squib --m by squib I mean a little blurb, by blurb,
24 I mean written word, words plural. That give you some
25 idea what that reg giude or NUREG or whatever did.

NEAL R. GROSS

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

1 And my brain is so old and overtaxed, and
2 the locator bits keep getting lost, that every time I
3 learn one of them, I am not even sure I got the Code
4 of Federal Regulations number right when I just stated
5 that it was -- maybe the AH was right, but I'm not
6 sure of those other numbers or letters were correct.

7 And I am still struggling with that and I
8 have written letters on five different reg. Guides and
9 I even have trouble remembering what those are. I have
10 to say that with a little bit of tongue in cheek, but
11 you know, it's 5:10 AND --

12 so that's what I was kind of looking for
13 when I saw the knowledge management ticket in rhere,
14 and knowledge management like ever y-- and I'm not
15 talking about giving details of everything. It's just
16 where do you find relevant to the technical areas for
17 which you are going to be -- you know, going to be
18 working, not that you won't work on others, but -- and
19 that the organization of all the data in the database
20 for the NRC is -- personal opinion -- is a mish-mash.
21 It's all over the p0lace, either that or I still
22 haven't figured it out which is also possibly the
23 case.

24 MR. CONCEPCION: There is a big matrix, I
25 believe is Table 7A-1. I don't know if my memory

1 serves me right at this point --

2 CHAIR BROWN: Where?

3 \ MR. CONCEPCION: But the SRP has an
4 appendix that has a very large matrix of --

5 CHAIR BROWN: The SRP?

6 MR. CONCEPCION: The SRP, the --

7 CHAIR BROWN: I didn't even know what the
8 SRP was until about 10 months later so it didn't help.

9 MR. CONCEPCION: Okay, so that first
10 chapter of the SRP on -- Chapter 7 -- has a large
11 matrix that presents all of the subchapters of chapter
12 7, and also provides regulatory requirements
13 associated with each of those subsections and provides
14 a pointer to certain regulatory guides that are
15 associated with the concept that is being discussed in
16 each and every subchapter.

17 CHAIR BROWN: Is there a title and a brief
18 description for each one?

19 MR. CONCEPCION: Yes there is and I
20 believe -- I don't recall if that was prior to 2007,
21 which was the last time the SRP was updated, but I
22 know that exists right now, and that can be accessible
23 online, on our website.

24 But we are expanding that matrix and
25 providing specific content that is buried in those reg

NEAL R. GROSS

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

1 guides, buried in NUREGs, and some NUREGs are not
2 referenced in what part --

3 CHAIR BROWN: Neither are the ISGs.

4 MR. CONCEPCION: Well, the ISGs are now
5 posted online but we are trying to take it a step
6 further and I guess, bring that content and relay it
7 to the actual topic that is under discussion and for
8 review. Yes.

9 MEMBER STETKAR: Milton, have you seen
10 what the fire people have done?

11 CHAIR BROWN: I have not. The fire
12 protection?

13 MEMBER STETKAR: Take a look at what they
14 have done. They have actually done a lot of what I
15 think I hear you saying and it kind of got a neat
16 organization so go talk to Mark Henry Sally. They have
17 -- yes it might be a nice template for you to organize
18 stuff because they have done a lot of that, linking
19 all the way back through to NUREGs, and you know,
20 whatever other references are out there.

21 MR. CONCEPCION: Okay, good.

22 MEMBER STETKAR: Whether it's complete or
23 not I don't know, I didn't try to trace every line,
24 but they have --

25 MR. CONCEPCION: Well the good thing is

1 that we are just starting the process.

2 MEMBER STETKAR: They have done quite a
3 bit and in the sense of consistency, you know, among
4 the different organizations, it might be a place to at
5 least go talk to them and take a look at it.

6 MEMBER SIEBER: All the reg guides are on
7 the NRC's website.

8 MEMBER STETKAR: I mean this has gone
9 further --

10 (Multiple speakers)

11 MEMBER STETKAR: It's buried information
12 down at the next level, often is not very easy to
13 find.

14 MR. CONCEPCION: Well, with this
15 electronic tool, what we are trying to do is not just
16 the information accessible to reviewers so they can do
17 a couple of clicks and find a NUREG for example.

18 We are trying to bring the context based
19 on the review they are performing, and bringing that
20 text to them so they make it available for their
21 safety assessments, we are taking it a step further.

22 MEMBER STETKAR: I might be a little even
23 more ambitious.

24 CHAIR BROWN: I understand the idea and
25 that's what some of the folks I dealt with. We had an

NEAL R. GROSS

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

1 area that a couple of people were working on as a
2 project for a client and it gets very complex when you
3 get down to that level so they can pull information
4 from a whole bunch of different sources, but what
5 people were pointing at is just -- here, I mean even
6 finding SECY papers or SRMs with -- that are related
7 to I&C subjects, unless I can find somebody that oh,
8 yes, I remember back in 2006 there was an SRM and I
9 think it was -- and then trying to -- and then you go
10 look in their list of SRMs with ML numbers and there's
11 no titles on them, there's some dates, but --

12 MR. CONCEPCION: What we are trying to do
13 -- Oak Ridge is helping us compile that information
14 that it is not necessarily obvious in the SECY papers
15 or any Generic Letters or information letters, and
16 bring it to context based on a particular review.

17 They are helping us with that. Russ? Do
18 you have another comment?

19 MR. SYDNOR: I was just going to comment
20 that the driver for this project really came from the
21 user offices, it was very much your same experience.
22 One of the drivers was the new engineers suffered the
23 same issue. The reason this got added to the research
24 bank, because this is not classical research, it's
25 more organization --

NEAL R. GROSS

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

1 MEMBER STETKAR: But it is important.

2 MR. SYDNOR: It is vitally important.

3 (Multiple speakers)

4 MEMBER STETKAR: It's been a while, it's
5 been like a year and a half since I looked at it, or
6 two years because I looked at for the two years ago
7 research, our report, and it was pretty slick. I don't
8 think it quite goes as far as you are talking about
9 and

10 5:14:55 PM tailor those better in terms of bringing
11 specific context out of those documents, but it does
12 provide that --

13 MR. CONCEPCION: We envision this as more
14 than just a knowledge management tool. If we are able
15 to achieve what we are shooting for with the tool, it
16 would actually be -- bring more efficiency to the
17 licensing reviews, because it would tailor those
18 better.

19 CHAIR BROWN: Yes, just even -- there's a
20 limit. First of all it's just the general organization
21 and layout and what the subjects are of the reg
22 guides, and then after that, you can develop -- at
23 least somebody knows where to go and hit two or three
24 of them that would have the information and then you
25 would go from there. I mean there's a -- and you can

NEAL R. GROSS

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

1 expand after that, once you lay in a fundamental
2 framework, and whether the fire protection folks have
3 got that fundamental framework or not is -- Christina
4 you are interrupting me while I am talking to Russ
5 here. Should I wait?

6 MR. CONCEPCION: Can I make another point
7 while Christina is talking? Another question that came
8 up from one of the members that I recall was that gaps
9 in our existing regulatory guidance. One of the
10 sub-tasks of the organization part that Oak Ridge is
11 helping us with is to identify gaps in our existing
12 regulatory guidance, and they will give us a list of
13 things that we should consider, adding items, and that
14 is also covered as part of the project, I just wanted
15 to mention.

16 CHAIR BROWN: Okay, I got, other than
17 that, any other comments? Jack? John?

18 MEMBER REMPE: No. I'm good

19 CHAIR BROWN: Okay, thank you very much.

20 MR. CONCEPCION: No acronyms?

21 CHAIR BROWN: I don't need -- if you just
22 give me the basic stuff I don't think we need to go
23 through any of this. We have covered a large number of
24 the --

25 MR. SYDNOR: I have captured all your

NEAL R. GROSS

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

1 requests and action items and I will work with
2 Christina to get what you need.

3 CHAIR BROWN: I'd appreciate that. I would
4 like to say thanks. I wanted to compliment the
5 presentations. I thought we had some very thorough,
6 comprehensive presentations and discussions, and it
7 was very, very useful in terms of number one, it
8 allowed me to get this other thing done, ubt aside
9 from that, the general background and getting into a
10 couple of these other technical areas, I think is
11 useful for the overall picture is how you all go down
12 and get various agreements on where we are going in
13 the digital I&C world. It's definitely different and
14 it needs to have a consistent focus in terms of how
15 it's going to be evaluated across all the program
16 offices and right now it's -- raises some issues based
17 on what we have been seeing so I think that would be
18 useful.

19 Anyway thank you very much. If there's no
20 more comments or questions?

21 MEMBER STETKAR: I would just like to
22 mention one thing, and that is I guess I am still a
23 bit concerned about this notion of failure modes, and
24 from a more -- and obviously I am not going to rehash
25 several things, I am a little bit concerned about it

NEAL R. GROSS

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

1 in the sense that from what we heard today, there
2 seems to be a conclusion that it's either not feasible
3 or certainly not practical to try to identify failure
4 modes, so that's sort of an abandoned notion.

5 Whereas over in the PRA group they have
6 concluded that not only is it possible, feasible, they
7 are actively pursuing a program according to a
8 specific methodology to identify failure modes and use
9 those.

10 So I see within Research now sort of two
11 diverging approaches with inputs from expert groups,
12 both of them used in expert, you know, if you want to
13 call it elicitation, both of them convened groups of
14 nominal experts who were asked questions about is this
15 a useful exercise or not.

16 One group concluded apparently no, the
17 other group concluded apparently yes, and I'm a bit
18 concerned about was there any -- I don't want to use
19 the term bias -- but was there a bit of self-serving
20 going on in terms of how those groups were convened
21 and how they were queried, more importantly, and how
22 the results of those exercises are now being used to
23 formulate research programs going forward in the
24 future.

25 I -- it's hard for me to get a handle on

NEAL R. GROSS

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

1 it, and I don't know quite honestly whether the full
2 Committee might feel it is important enough to write
3 a letter on. I just don't know yet. I think we need to
4 discuss it with ourselves.

5 But I just, I wanted to get that kind of
6 unease on the record regardless of the fine structure
7 detail that I was talking about earlier, it's this
8 notion of a bit of divergence and not clear what the
9 basis for that is, and I know you want to --

10 MR. BIRLA: Sushil Birla. You mentioned
11 the the PRA work performed by BNL is proceeding with
12 failure modes as a basis. I would like to refresh your
13 memory on what you heard on June 7. They basically
14 abandoned that approach. They presented to you two
15 alternatives. One was based on information from the
16 development process. And the second was based on
17 information from testing.

18 And they are -- they proposed to you a
19 research plan here onwards, that is favoring the
20 testing-based approach.

21 MEMBER STETKAR: And I'll refresh your
22 memory that they were talking about deriving
23 information to support quantification. They were not
24 talking about information to support failure modes.
25 It's a different issue.

NEAL R. GROSS

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

1 Their failure modes, they are still
2 pursuing the use of essentially a simulation type
3 technology to look at ways -- and it's not clear how
4 they are going to do that yet because they sort of
5 left that hanging -- to identify failure modes.

6 What we heard about on June 7th, was
7 primarily focused toward deriving information to
8 support quantification so that the two approaches that
9 they are talking about, both the Bayesian belief
10 network approach to generate a prior with do you use
11 testing, do you use some other sort of approach to
12 specialize that, was focused primarily in terms of
13 trying to come up with numbers to fit into a context
14 of failure modes.

15 Part of our criticism of June 7th was you
16 are embarking on a program now to derive numbers
17 without having yet defined the failure modes and they
18 said well yes, that's something that we still need to
19 work out.

20 But they hadn't abandoned the notion of
21 failure modes as a fundamental notion of something
22 going forward, at least not to my knowledge. If they
23 have, that's I guess a fundamental misinterpretation.

24 MR. BIRLA: Well, as a basis for
25 quantification, that's not what they are pursuing, and

NEAL R. GROSS

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

1 they said so on the 7th of June, and as far as the
2 last formal documentation on the work, that's from the
3 Brookhaven workshop held in May of 2009, and the
4 function-oriented failure modes that they had
5 identified we showed you those this morning.

6 MR. RICHARDS: This is Stu Richard with
7 the Office of Research. We understand your concern and
8 I think what we --

9 MEMBER STETKAR: There at least seems to
10 be some misinterpretation you know --

11 MR. RICHARDS: You know, it is something
12 we have had some dialogue about internally.
13 Unfortunately I don't think Alan Kuritzky is still
14 here today. But we will go back and talk it over with
15 Alan and review where we are at.

16 CHAIR BROWN: I would suggest that we --
17 I'm not going to write a letter referencing to this
18 meeting, but I would think we would put that in the
19 hopper of subsequent meetings to try to coalesce this
20 thought process and where we go, because it's
21 applicable to your -- you know, the PRA world as well
22 as the software evaluation world, and see, get at
23 least a consistent --

24 MEMBER STETKAR: It's a question on, you
25 know, the direction for Research.

NEAL R. GROSS

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

1 CHAIR BROWN: Right, exactly.

2 MEMBER STETKAR: That's sort of the
3 general topic of this meeting but it is related to the
4 integrated direction of Research, and out in the PRA
5 world also.

6 CHAIR BROWN: Okay. One last round, Jack
7 do you have any final comments?

8 MEMBER SIEBER: No I don't.

9 CHAIR BROWN: John anything else? Joy?

10 MEMBER REMPE: Just to emphasize what
11 John's brought up, I think somehow or other the
12 discussions today about the fact that some information
13 from John and Dennis would be provided to the staff,
14 and that they would reconsider that information, at
15 the next meeting we should definitely hear some of the
16 results of what they have done.

17 CHAIR BROWN: Yes, and Dennis and John, I
18 asked them both, they said they were going to take
19 actions to get that, I guess give it to Christina and
20 she can forward it on to them or whatever it is, and
21 --

22 MEMBER REMPE: I think it's something --
23 some response is due back.

24 CHAIR BROWN: Oh yes, that's our action to
25 get something at least the examples that were talked

NEAL R. GROSS

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

1 about to you guys and we will do that.

2 I just lost my -- there are no public --
3 I take it there's been no change in the public
4 comments? I mean I -- do I have to wave at anybody?

5 I think we are clean. Other than that I
6 will say the meeting is adjourned. Thank you all very
7 much.

8 (Whereupon the meeting

9 adjourned at 5:24 p.m.)

10

11

12

13

14

15

16

17

18

19

20

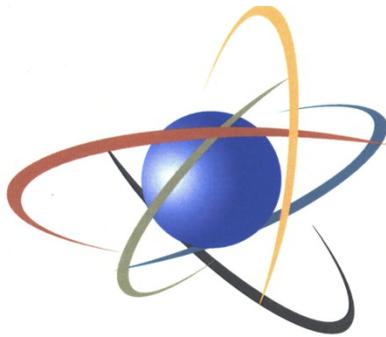
21

22

23

24

25



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

**NRC DIGITAL SYSTEM RESEARCH
FY 2010 THROUGH FY 2014
Status/Update**

**Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
June 22, 2011**

Russell Sydnor

**Division of Engineering
Office of Nuclear Regulatory Research
(301-251-7405, russell.sydnor@nrc.gov)**

- **To present status and results of NRC Digital System research activities of interest to the ACRS**
 - **Input for ACRS biennial review**
- **To discuss and obtain insights from ACRS members on the results and direction of Digital System Regulatory Research**
- **No letter is requested**

FY 2010 – FY 2014 Digital Systems Research Plan (ML093080383)

- Major update of the FY 2005 to FY2009 Plan**
- ACRS Digital Systems Subcommittee reviewed – August 2009**
- ACRS reviewed – September 2009**
- ACRS Letter – October 2009**
- Program Offices concur – February 2010**
- Issued by Office of Nuclear Regulatory Research – February 2010**

DI&C Research Program



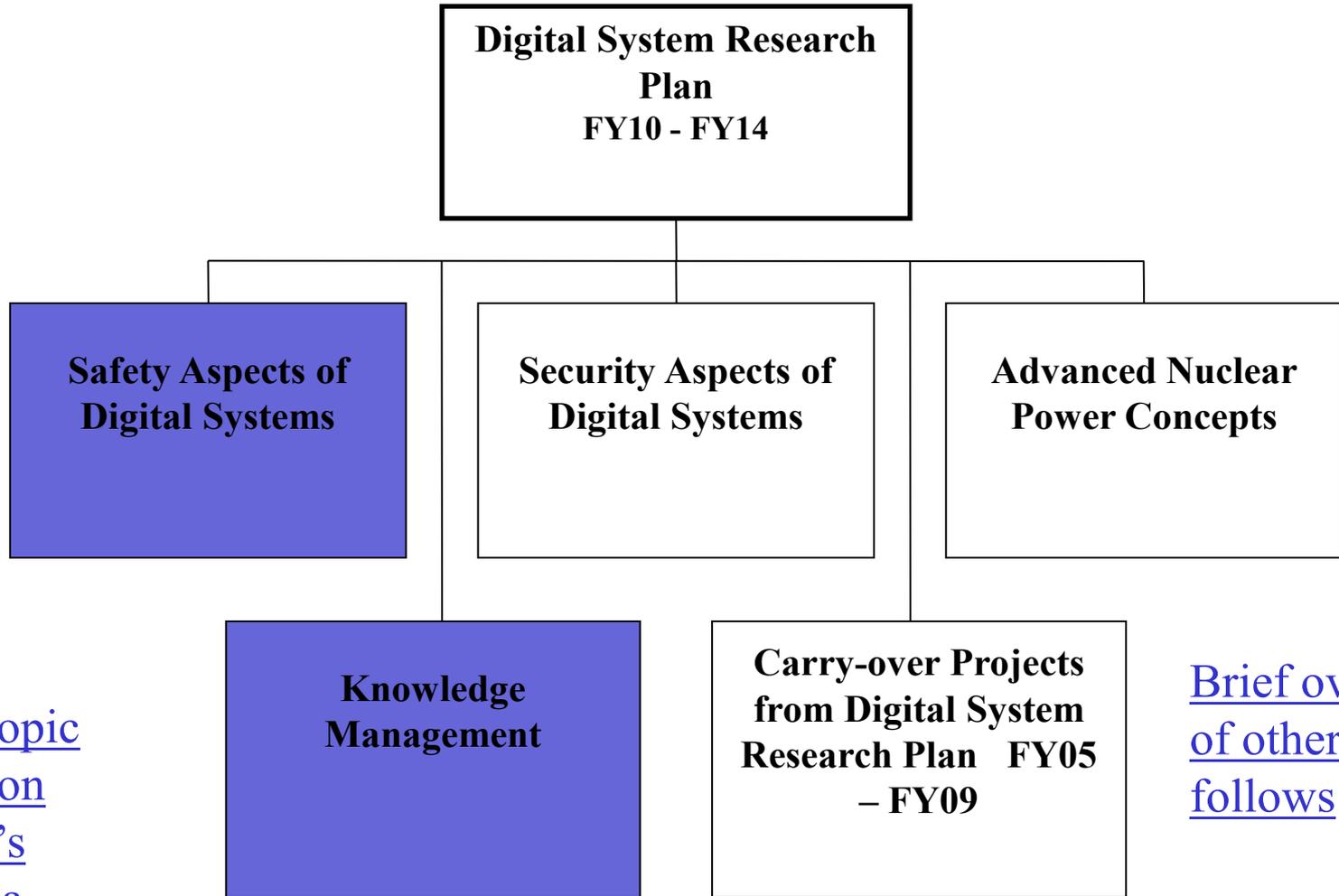
Completing 7 Projects from
05-09

Transition from 2005-2009 plan to 2010-2014 plan

- **FY 2010 – FY2011 transition period**
- **FY2005- FY2009 Digital Systems Research Plan**
 - 7 research programs made up of 29 research projects and tasks
 - In 21 of 29 areas - significant research progress
 - In progress research - continued to completion
 - Research not initiated - reviewed for incorporation into 10 -14 Plan
- **05-09 DI&C research targeted:**
 - Regulatory guidance improvements
 - Development of new methods e.g. PRA, assurance, testing, etc.
 - Regulatory implications of new technology
- **05-09 plan supported DI&C Project and ISG development**

Digital Research Publications

- **From 05-09 Plan**
 - **NUREG/CR – 7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems-** (technical basis for ISG-3, future BTP 7-19 update)
 - **NUREG/CR – 7006, Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems Plant –**(technical basis for a future Regulatory Guide)
 - **NUREG/CR – XXXX, Large Scale Validation of a Methodology for Assessing Software Quality** (exploration of software metrics for software assurance use)
 - **RG 5.71, Cyber Security Programs for Nuclear Facilities-** (guidance for 10CFR 73.54)
- **From 10-14 Plan**
 - **NUREG/IA – 0254, Suitability of Fault Modes and Effects Analysis for Regulatory Assurance of Complex Logic in Digital Instrumentation and Control Systems** (interim research results for DI&C failure modes)
 - **Research Information Letter 1001: Software-Related Uncertainties in the Assurance of Digital Safety Systems – Expert Clinic Findings, Part 1**
- **Additional details in handout provided**



Two topic areas on today's agenda

Brief overview of other topics follows

Research projects underway

- **Digital System PRA (Discussed at June 7 meeting)**
- **Fault Injection Test Methodology Development**
 - Platform testing complete
 - Drafting NURGEG/CR for publication

New research Projects

- **Developing project SOW and Contract**
 - Safety Assessment of Tool Automated Processes
 - Diagnostics and Prognostics
- **Defining scope**
 - Communications Among Plant-wide systems
 - Integrated Plant & DI&C System Modeling

- **Part of NGNP/HTGR research Plan**
 - **ACRS reviewed HTGR Research Plan in May 2011**
 - **Goal - Identify unique HTGR I&C aspects, identify regulatory knowledge/guidance gaps**
- **Interim results report to NRO – June 28, 2011**
- **Next Steps – incorporate NRO feedback complete and publish results, update guidance as needed.**

Cyber Security Research

- **Digital platform cyber vulnerability assessments by Sandia Labs (Common Q, Teleperm, Tricon)**
- **Digital system networks and wireless network security studies**
- **Support Cyber Security guidance development and knowledge management**

EMP/RHF Research

- **Sandia reanalyzed EMP/HRF impacts on NPPs with focus on new digital systems**
- **Solar Storm impacts study**
- **Exploratory research to determine regulatory impacts**

Lower priority 05-09 plan carryover projects (Research projects have not started)

- **Electromagnetic Compatibility**
- **Operating Systems**
- **Electrical Power Distribution System
Interactions with Nuclear Facilities**

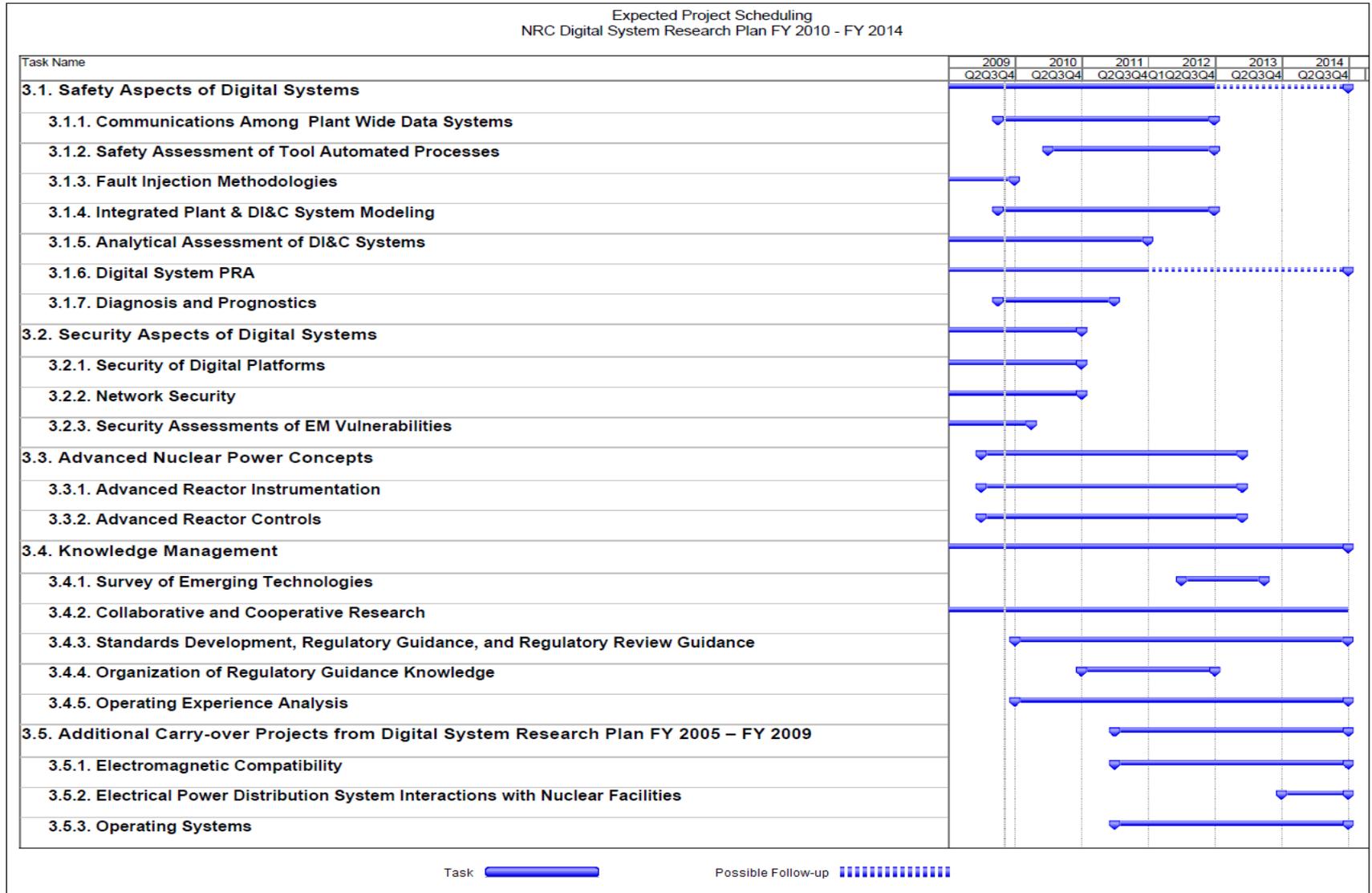
Digital System Research Summary-

- **Research is targeted to:**
 - **Answer specific regulatory questions**
 - **Improved regulatory guidance**
 - **Knowledge management**
- **Need improved interface with Program Offices**
 - **Program Office involvement to improve SOW's.**
 - **Program Office interim review and feedback**
 - **Program Office review of research results**

- **ACRS – Advisory Committee on Reactor Safeguards**
- **DI&C – Digital Instrumentation and Controls**
- **EMP/HRF – Electromagnetic Pulse/High Radio Frequency**
- **FPGA – Field Programmable Gate Array**
- **FY – Fiscal Year**
- **HTGR – High Temp Gas Reactor**
- **I&C – Instrumentation and Controls**
- **NGNP – Next Generation Nuclear Plant**
- **NRC- Nuclear Regulatory Commission**
- **NRO – Office of New Reactors**
- **OpE – Operational Experience**
- **PRA - Probabilistic Risk Assessment**
- **R&D – Research and Development**
- **SOW – Statement of Work**
- **UVA - University of Virginia**

Backup Slides

Project Scheduling



- **Analytical Assessment of DI&C Systems**
 - **Develop an inventory, classification, and characterization of DI&C systems for use in nuclear safety applications**
 - **Identification of credible systematic failure and fault modes typical of software-intensive DI&C systems**
 - **Initial focus is an analysis of 3 pre-approved platforms in highly integrated environment**
 - **Gain a better understanding of DI&C failure modes and of the feasibility of applying failure analysis in risk quantification**

- **Survey of Emerging Technologies**
- **Collaborative and Cooperative Research**
- **Standards Development, Regulatory Guidance, and Review Guidance**
- **Organization of Regulatory Guidance Knowledge**
- **Operating Experience Analysis**



U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

NUREG-I/A-0254:

**Suitability of Fault Modes and Effects Analysis
for Regulatory Assurance of Complex Logic in
Digital Instrumentation and Control Systems**

**Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
June 22, 2011**

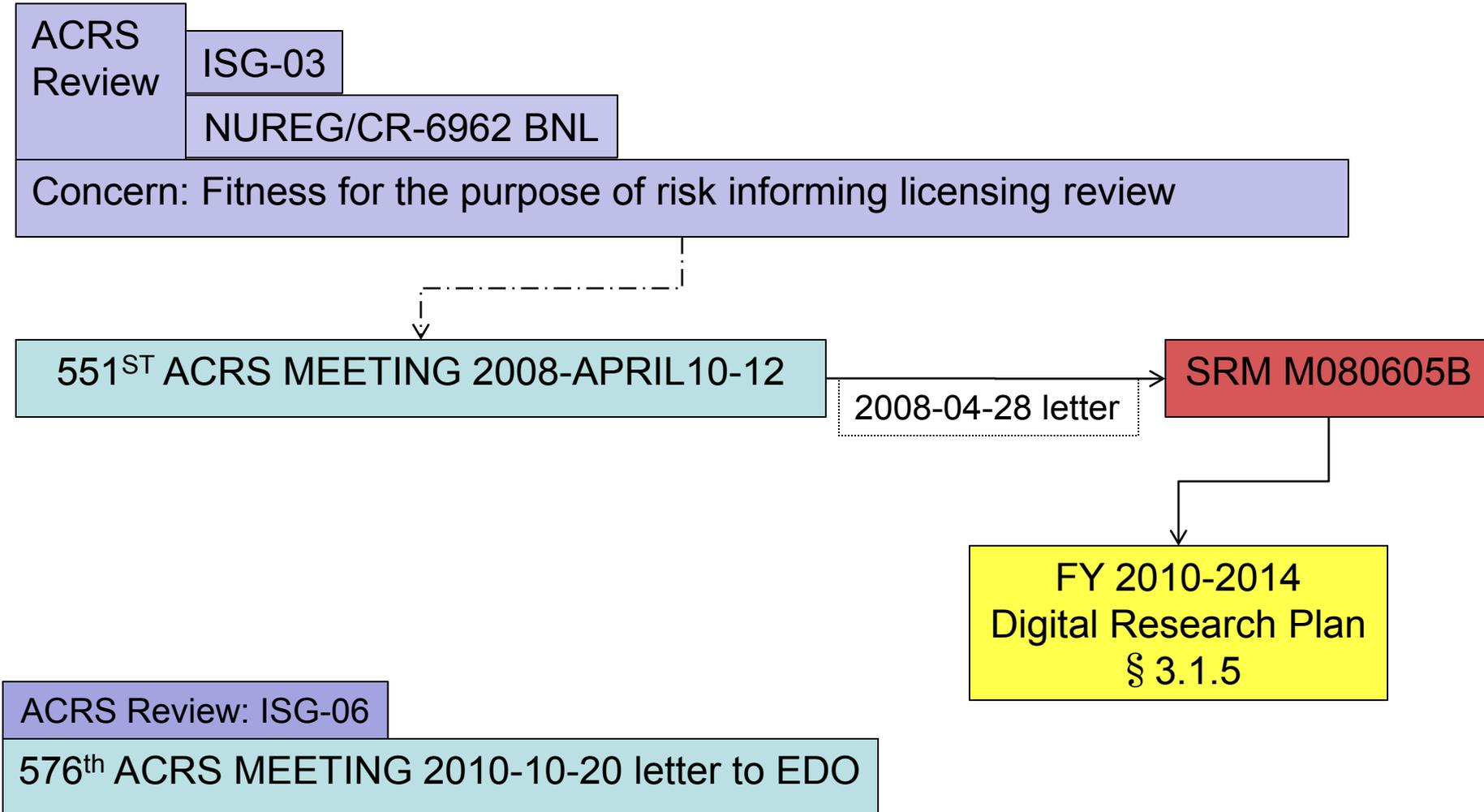
**Luis Betancourt / Sushil Birla
Division of Engineering
Office of Nuclear Regulatory Research**



Outline

- Background
- Research method
- Preliminary Results
- Path Forward

Background – Flow of concerns



Background – SRM M080605B

Staff Requirement Memoranda (SRM)-M080605B dated July 2008 (ML081780761): “At the next Commission briefing on digital I&C, the staff should

...report the progress with respect to identifying & analyzing DI&C failure modes

RIL-1001

NUREG/IA-0254

2nd RIL

and discuss the feasibility of applying failure mode analysis to quantification of risk associated with DI&C...”

3rd RIL

Software FMEA

- Literature review revealed that:
 - Some researchers or organizations call it software fault modes and effects analysis (FMEA), but use the technique for the system-internal hazard analysis to discover consequences of some hardware malfunction, and identify requirements to mitigate the effect through software
- Two types of Software FMEAs found:
 - System Level Software FMEA
 - Detailed Level Software FMEA

Purpose

- Purpose of NUREG-I/A-0254
 - Examine FMEA role in regulatory assurance of Complex Logic in DI&C safety systems
- For software, the corresponding concepts are faults and fault modes
- Scope of the study:
 - Broadened from “Software” to “Complex Logic
 - Narrowed the role in “regulatory assurance”

NUREG-I/A-0254

Development Process

- Serves as a repository and record for information received from a foreign source, as part of a bilateral or multilateral information exchange agreement
- Captured information from the experience of the French Institute of Radiological Protection and Nuclear Safety experts – Pascal Regnier and Jean Gassino
- Performed literature review of “Software FMEA”

Research method

- Characterize the differences between traditional hardwired systems and current Complex Logic-intensive systems
- Analyze validity of applying traditional FMEA to Complex Logic
- Validate analysis with examples from experience
- Find and analyze opposing viewpoints
- Draw conclusions
- Formulate direction of further investigations

Characterization of Fault Modes

Traditional Hardwired	Complex Logic
Most faults caused by physical degradation	Faults caused by engineering mistakes
Simpler system; mature practice → Engineering & manufacturing defects easier to eliminate	Complex system; immature practice → Undetected engineering defects likely
Limited number of fault modes; well understood	Number of potential faults very high; not well understood. In a high-quality process actual number of faults is smaller
Fault propagation paths (functional ↔ physical) well understood	Many possible, unknown propagation paths; not well understood
Engineering process can reduce frequency of occurrence but cannot eliminate faults	Engineering process can eliminate all known faults; otherwise, they would be corrected

Extending FMEA to Complex Logic

Issues and limitations

- Combination of inputs
 - Number of potential faults in Complex Logic cannot be bounded in general
- Defects internal to a software unit
 - Small fraction are detected by “brute force”
 - System fails because of logic, it had some fault from the time of introduction
- Propagation of faults across units
 - Very large and not well understood
 - Appendix B – Other Sources of Uncertainty when Complex Logic is implemented in Software
 - Unpredictable in software with known and hidden dependencies

Fault Modes from the Effect Perspective

Fault modes of a module are characterized in terms of the effects of module's function on the system:

- Failure to perform the module function in time (i.e., in time domain)
- Failure to perform the module function with correct value (i.e., in value domain)
 - AT&T's #4ESS toll switching systems
 - Ariane 5 Launcher
- Performance of an unwanted function by the module
- Interference or unexpected coupling with another module
 - Canadian Bruce-4 nuclear Reactor

Literature Review

- Literature review of Software FMEA
 - Useful in hazard analysis leading to the discovery or identification of safety requirements
- Reported beneficial uses of Software FMEA :
 - Herb Hecht, SoHaR
 - Robyn Lutz, Iowa State University
 - Pete Goddard, TRW ← Raytheon ← Hughes Aircraft Co

Preliminary Results

- Contribution of FMEA to regulatory assurance of Complex Logic, especially in software, in a NPP safety system is marginal
- Pursue improvement in other assurance techniques
- Clarify appropriate use of FMEA in safety analysis of Complex Logic
- No related changes in DI&C-Interim Staff Guidance-06 are recommended

Path Forward

- Continue learning from “contrarian” viewpoints

2ND Research Information Letter (RIL) — Build on the findings of RIL-1001 and NUREG-I/A-0254

- Complete 2nd RIL – Identification of DI&C fault modes attributable to software, contributing to:
 - SRM-M080605B
 - Recommendation #4 from the ACRS 576th meeting
- Discussions related to the:
 - Role of FMEA in safety analysis of Complex Logic
 - Software defect classifications

Some open questions

Related-research questions:

- Under what verifiable conditions can design information be deemed dependable for use in safety assurance?

Examples of concerns:

- Incomplete, inconsistent, ambiguous requirements
- Inadequate or unverifiable architectural constraints

Acronyms

- ACRS – Advisory Committee on Reactor Safeguards
- DI&C – Digital Instrumentation and Control
- DICB – Digital Instrumentation and Control Branch
- EDO – Executive Director for Operations
- FMEA – Fault Modes Effects and Analysis
- IRSN – Institut de Radioprotection et de Sûreté Nucléaire
- ISG – Interim Staff Guidance
- NRC – U.S. Nuclear Regulatory Commission
- NPP – Nuclear Power Plant
- RIL – Research Information Letter
- RES – Office of Nuclear Regulatory Research
- SRM – Staff Requirement Memoranda



Backup Slides

551st ACRS Comments

- 551st Advisory Committee on Reactor Safeguards (ACRS) Letter — Dated April 29, 2008 (ML081050636)
 - “...emphasize importance of identification of failure modes...”
 - “...DI&C may introduce new failure modes that are not well understood.”
 - “The SW failure probabilities...do not have a sound technical basis.”
 - “These probabilities cannot be very meaningful in the absence of a good understanding of the failure modes”

576th ACRS Comments

- 576th ACRS Meeting Letter: Recommendation #4 —
Dated October 20, 2010 (ML102850357)

“Software Failure Modes and Effects Analysis (FMEA) methods should be investigated and evaluated to examine their suitability for identifying critical software failures that could impair reliable and predictable DI&C performance”

- EDO response — Dated December 7, 2010
(ML103130193)

“As part of ongoing research under the FY2010-2014 Digital Systems Research Plan, RES/DICB is investigating the efficacy of Software FMEA as a method for identifying faults leading to system failures impairing a safety function. This effort has involved expert elicitation from numerous international software system engineering experts from both nuclear and non-nuclear domains. The Staff intends to brief the ACRS DI&C Subcommittee on the outcomes and findings of this research.”



**Software-related Uncertainties in Assurance
of Digital Safety Systems**
findings through
Expert Judgment Process

Briefing by RES to ACRS on 2011-06-22

Presenter: Sushil Birla

Outline

- Background
- Research approach:
 - Expert judgment process (custom-tailored)
- Findings concerning software assurance
- Path Forward

Project basis

Staff Requirement Memorandum

M080605B dated July 2008 (ML081780761)

At the next Commission briefing on digital I&C, the staff should

Report the progress made
with respect to
identifying and analyzing
digital I&C failure modes

&

Discuss the feasibility of
applying failure mode analysis
to quantification of risk
associated with digital I&C

Mapping into research plan

Staff Requirement Memorandum

M080605B

Report the progress made with respect to identifying and analyzing digital I&C failure modes

Discuss the feasibility of applying failure mode analysis to quantification of risk associated with digital I&C

Analytical assessment of DI&C systems (3.1.5)

Digital system PRA (3.1.6)

Knowledge management (3.4)

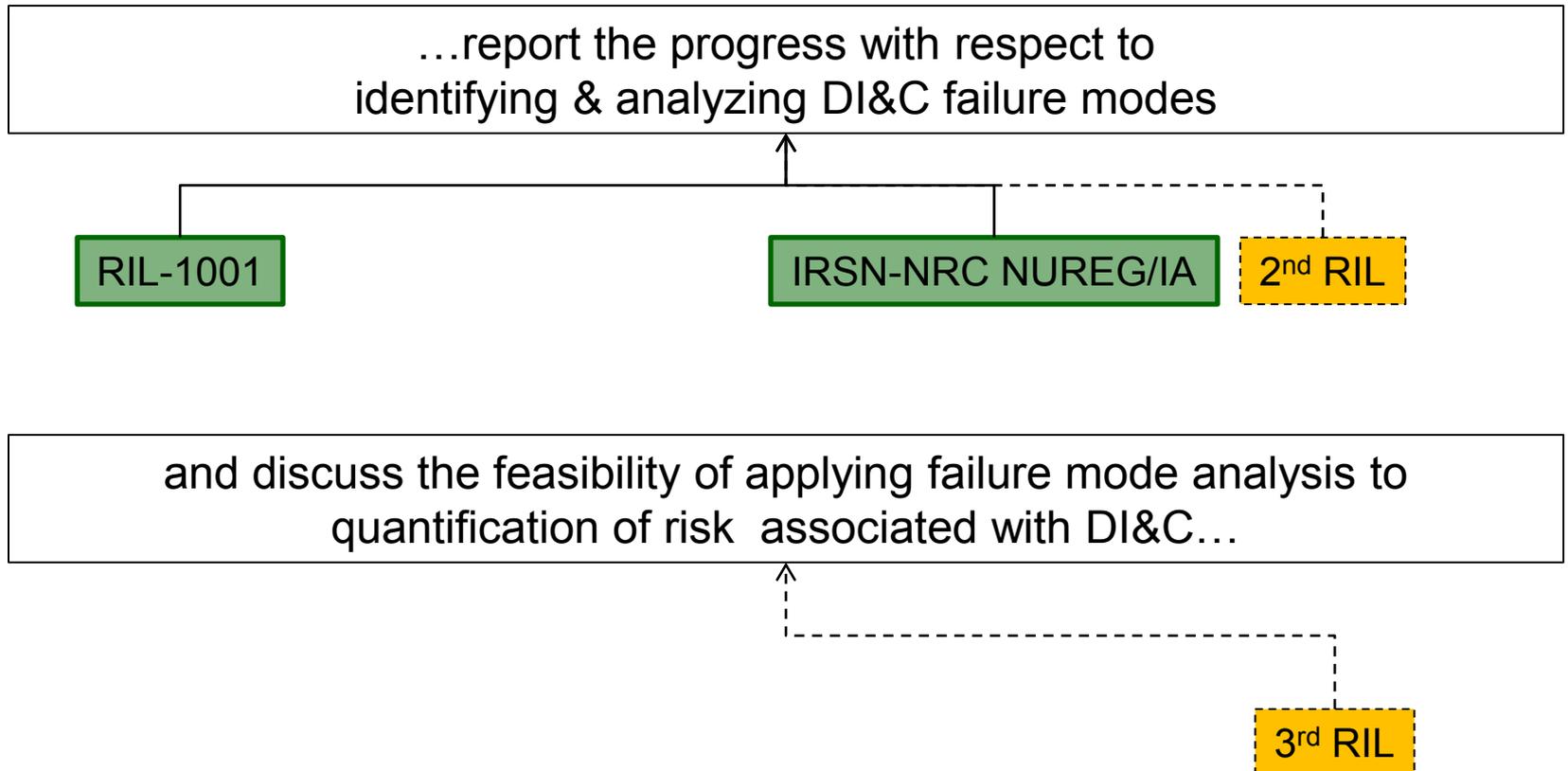
DI&C OpE (3.4.5)

Expert elicitation

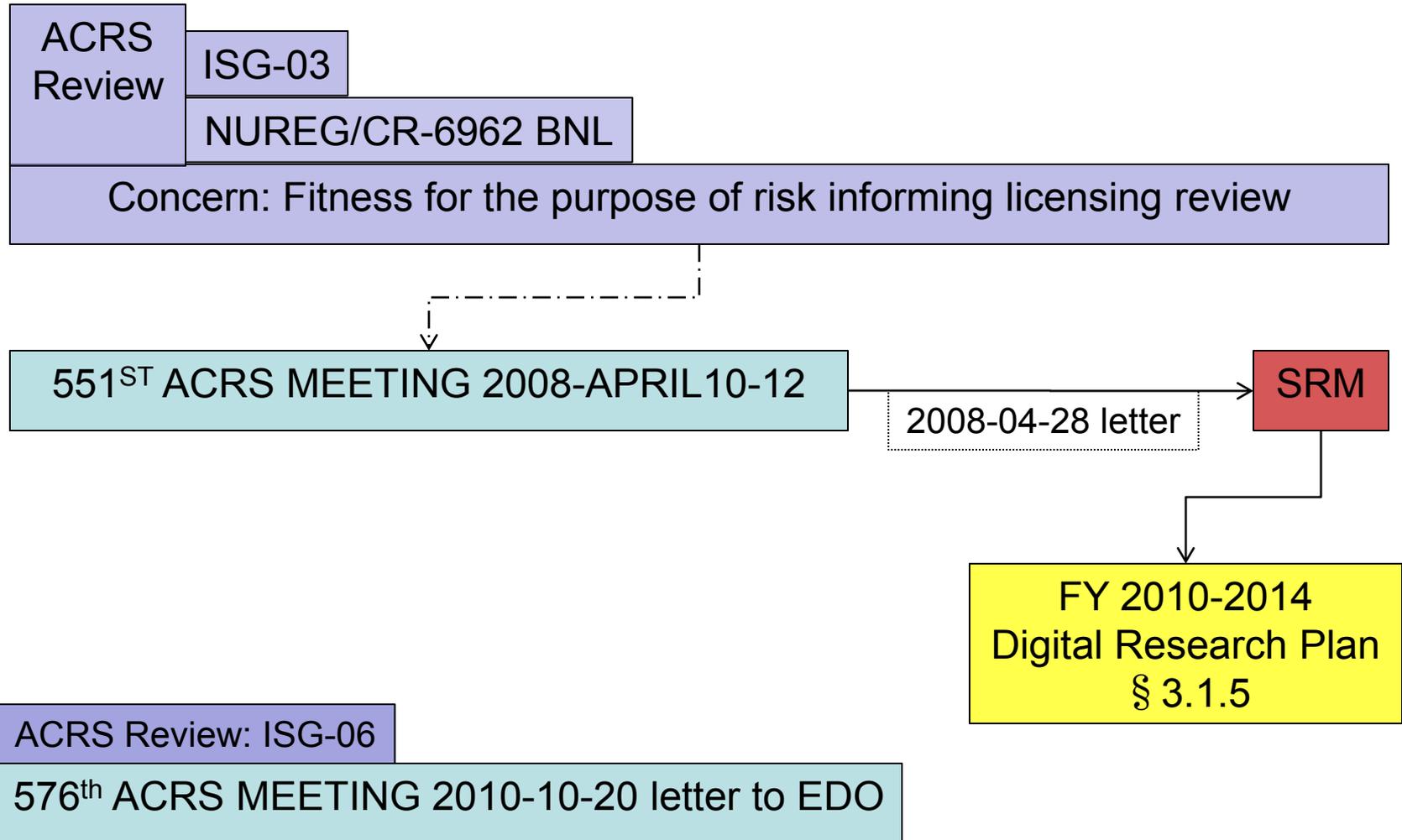
FY 2010-2014 DI&C research plan

SRM M080605B

SRM M080605B dated July 2008 (ML081780761) “At the next Commission briefing on digital I&C, the staff should



Flow of concerns



DI&C Assurance

~ 70 Sections in NRC regulations

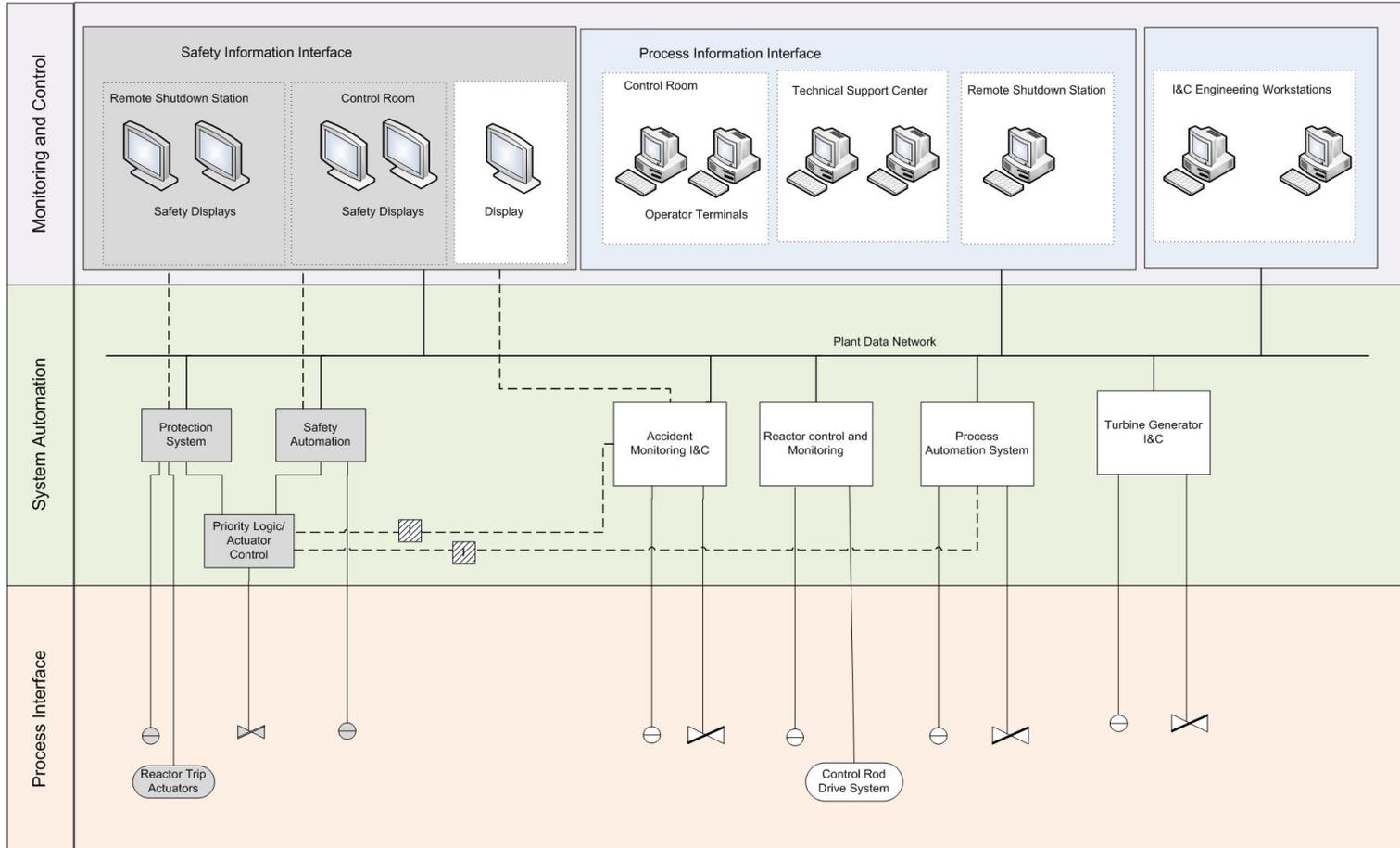
{ ~ 200 Relationships at section level }

~ 10 Regulatory guides

~ 10 voluntary consensus standards

~ Various references

System complexity

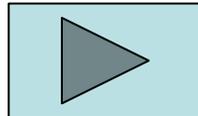


NOTE

- Shaded items are safety related equipment
- Unshaded items are non-safety related equipment
- Safety isolation barrier

Research approach

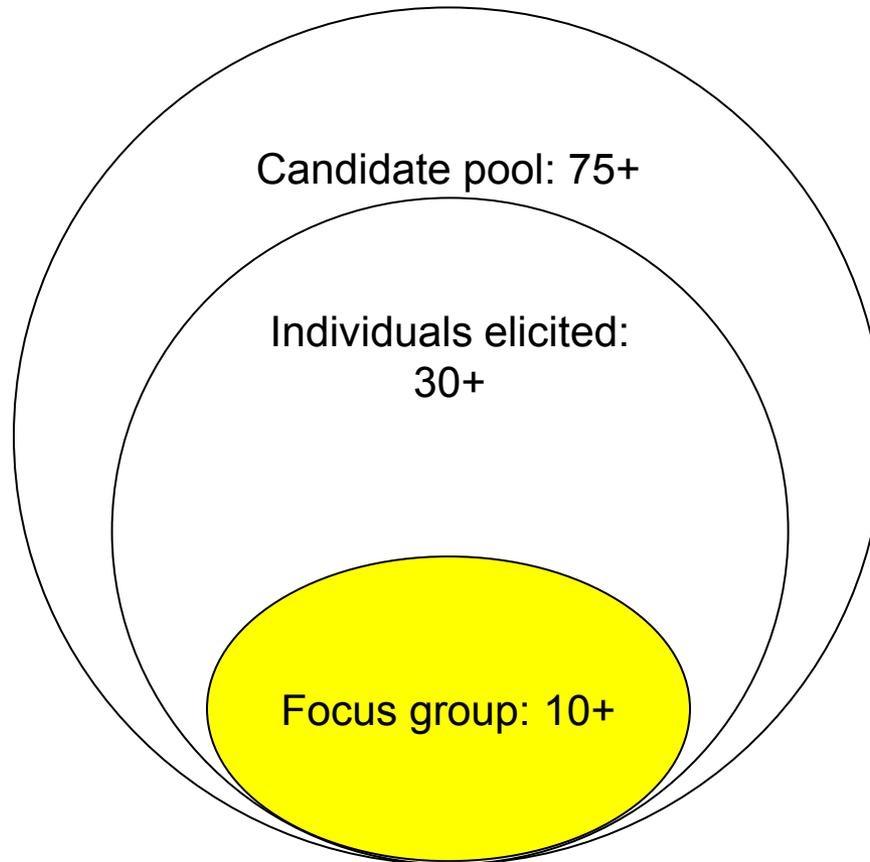
Acquisition of knowledge outside the NPP industry
&
Utilization of Expert Judgment Approach
in research
to improve regulatory guidance



Expert judgment process: overview

1. Derive initial scope and questions from SRM M080605B
2. Build search criteria and commensurate candidate pool of experts
3. Screen for individual elicitation
4. Pre-brief experts selected for individual elicitation
5. Interview experts for individual elicitation
6. Analyze and integrate elicited information
7. Develop consensus position (reference position document)
 - Iterate through sources of information
8. Select topics or issues for (face-to-face) focus group
9. Select focus group members
10. Execute two-day Clinic
11. Develop the first RIL (RIL-1001)
 - Iterate through clinic participants
12. Organize information for the 2nd and 3rd RILs
13. Seek feedback on the process

Multistage engagement of experts



Initial scope boundaries

Context given to experts:

In DI&C systems for NPP safety functions, contribution to failure from systemic causes (i.e. systematic failures), esp. failures attributable to software

Some initial questions for individual elicitation:

What is meant by “failure modes” in this context?

How to identify & analyze “failure modes” attributable to software?

Feasibility of applying failure mode analysis to quantify likelihood attributable to software?

Using risk insights, how to reduce variation in safety assessment, rooted in uncertainties from software assurance?

Expert screening criteria

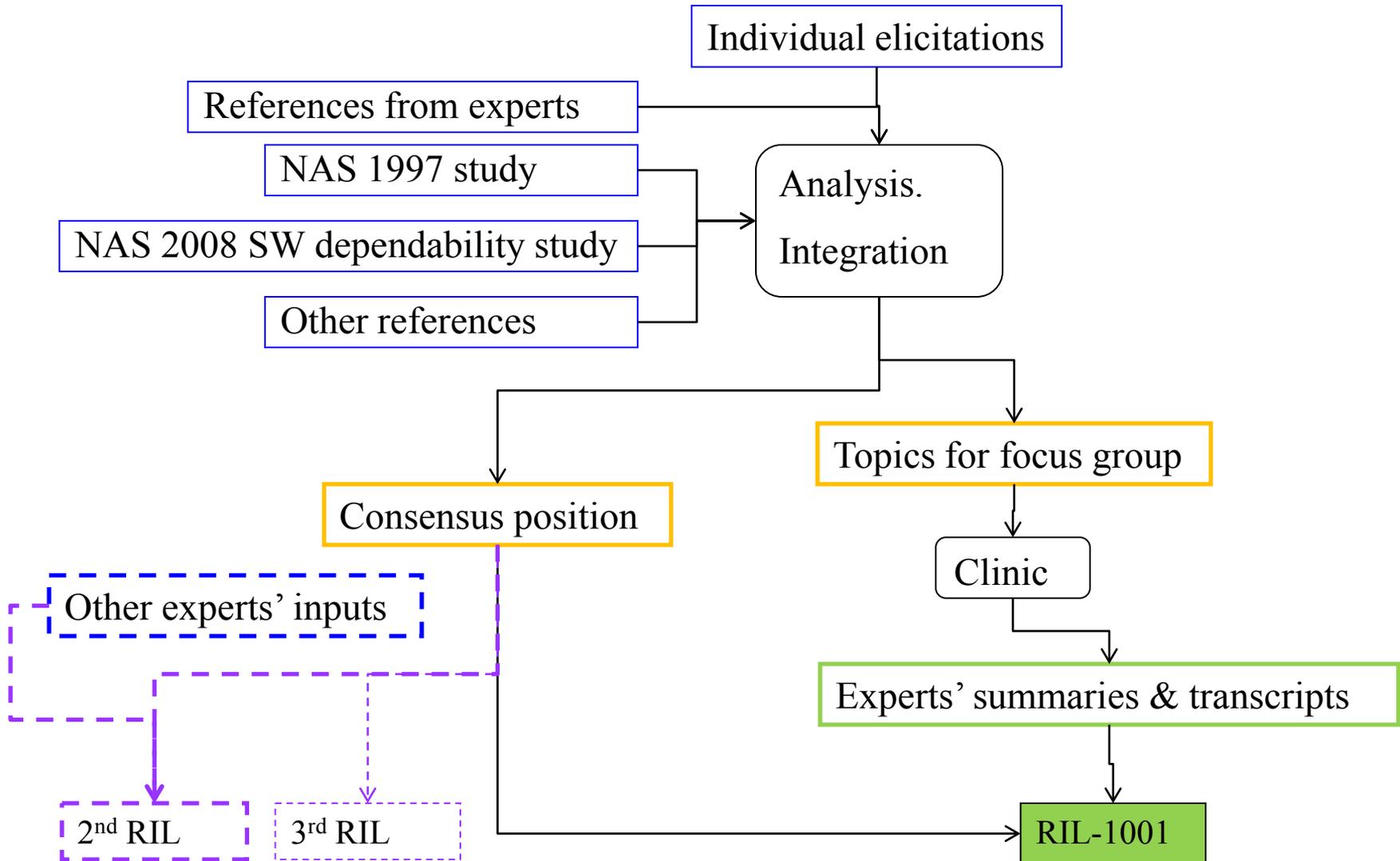
General:

- No conflict of interest
- Availability
- Match of interest

Match of interest (NRC side):

- Significant knowledge and experience contributing to project objectives
 - Safety-/mission-critical DI&C systems
 - Elements of the NPP application domain
- Broad and integrative rather than narrowly specialized
- Ability to identify influencing factors and their inter-relationships
- Ability to identify failure modes, their causes, and their interrelationships

Analysis and integration process



Results from Individual elicitations

Context: Risk-informing licensing review for software assurance

Identifying & analyzing digital I&C failure modes (software focus)

- No compact set of failure modes attributable to software could be found
 - [topic of 2nd RIL]

Feasibility of applying failure mode analysis to quantification of risk

- Negative
 - [topic of 3rd RIL]

Refocused clinic themes

Shifted discussion

From: Difficulty in characterizing failure modes, fault modes

To: Understanding causes of difficulties:

Uncertainties.

Large potential fault space

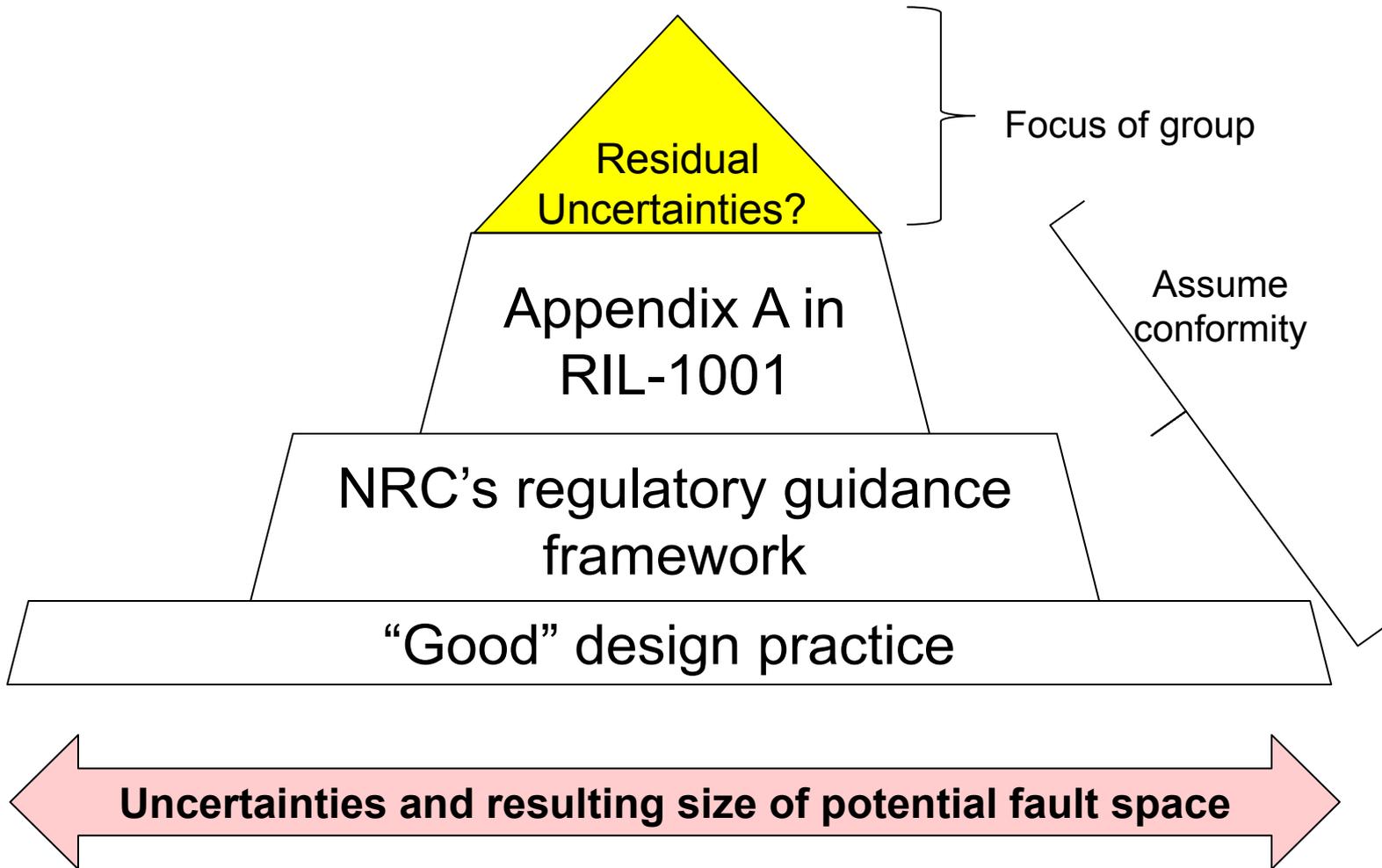
Clinic themes:

Sources of uncertainties in software assurance?

Evidence needed to reduce these uncertainties?

Knowledge gaps?

Starting point given to focus group



Focus group forming criteria

- Assemble complement of expertise required for the selected topics
- Maximize objectivity through independence
 - diversity in different dimensions:
 - Theory ⇔ Practice
 - Application domain
 - Product: Platform. Application. Integrated system
 - Process: {Systems; Software; Safety} engineering
 - Problem-solving paradigm: Different schools of thought...cultures

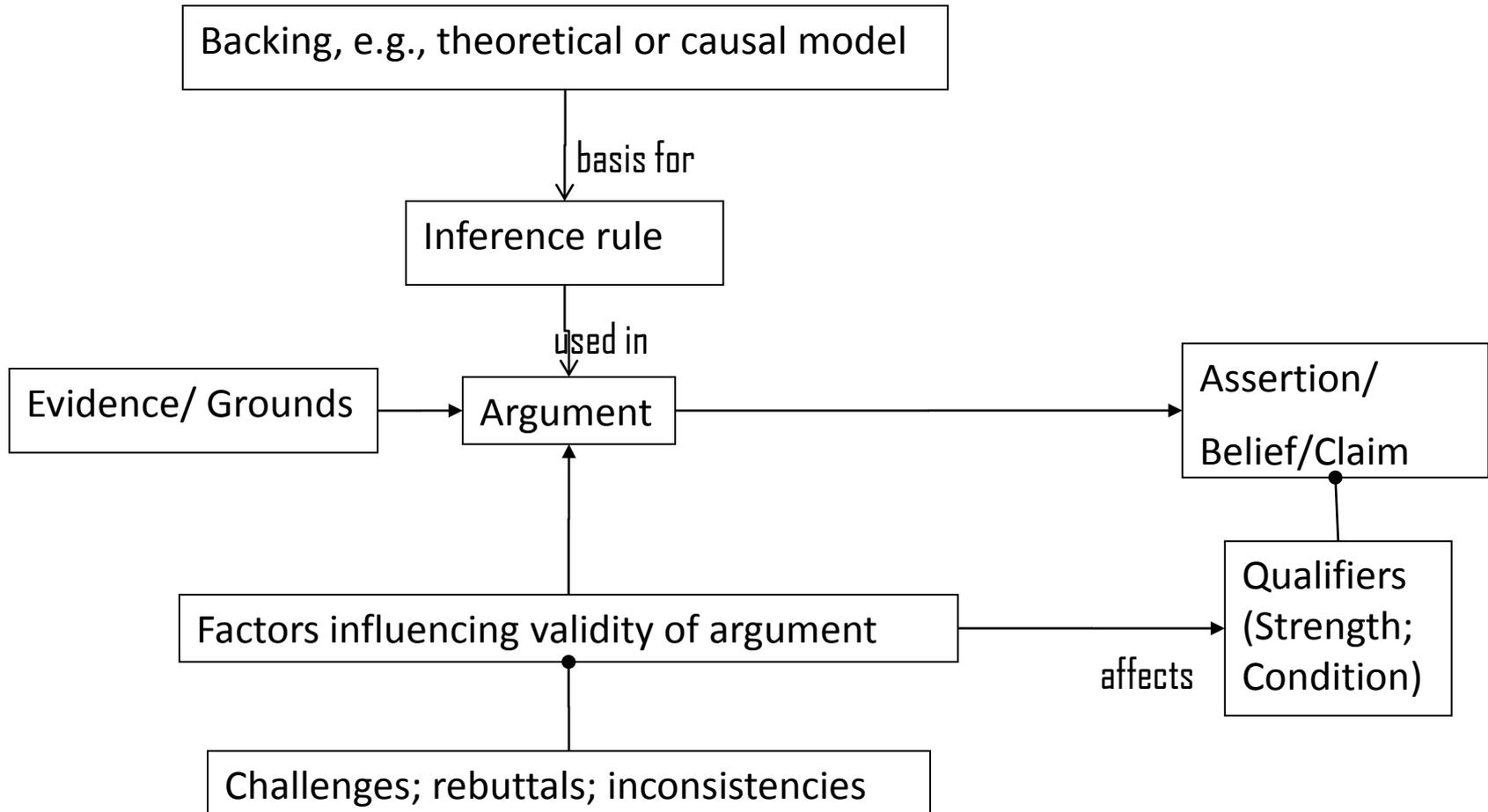
Diversity realized

- Sub-fields:
 - Requirements, Architecture, Methods & Tools, Assurance
- Application Domains:
 - Defense, Space, Aviation, Auto, Rail, Telecom, Medical, NPP
- Schools of thought:
 - {Formal methods} ←.....→ {Expert judgment}
- Culture/Country:
 - UK, Germany, Sweden, Canada, US
 - (New Zealand and Australia also covered in individual elicitations)

Actual focus group

Expert	Country	Distinguishing dimension
John McDermid	UK	Safety systems & SW research
Gerard Holzmann	USA	Software reliability; Tools
Manfred Broy	Germany	Systems & SW engrg research
Jorgen Hansson	Sweden	Systems & SW architecture
David Ward	UK	Automotive safety assessment
Paul Miner	USA	Formal methods
Darren Cofer	USA	Flight controls industry
John Knight	USA	Assurance case research
Alan Wassying	Canada	Software certification; NPP
Michael Holloway	USA	Expert judgment

Validity vetting model

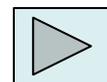


Clinic topics

1. Verification and Validation: Coverage gaps
2. Framework for Safety Demonstration
3. Tool-automated or tool-assisted processes
4. Change Impact Analysis
5. Combined effect of seemingly “small” defects

Expert judgment process: Feedback

1. Derive initial scope and questions from SRM M080605B
2. Build search criteria and commensurate candidate pool of experts
3. Screen for individual elicitation
4. Pre-brief experts selected for individual elicitation
5. Interview experts for individual elicitation
6. Analyze and integrate elicited information
7. Develop consensus position (reference position document)
 - Iterate through sources of information
8. Select topics or issues for (face-to-face) focus group
9. Select focus group members
10. Execute two-day Clinic
11. Develop the first RIL (RIL-1001)
 - Iterate through clinic participants
12. Organize information for the 2nd and 3rd RILs
13. **Seek feedback on the process**



Impact of Expert Clinic

Influence on licensing reviews

- Boosted Confidence in many positions held by NRC staff
- Increased awareness → Improve exercising judgment

Influence on FY 2010-2014 research plan

- Framework for Safety Demonstration
- Tool-automated or tool-assisted processes
- Change Impact Analysis
- Verification and Validation: Coverage gaps
- Combined effect of seemingly “small” defects

Some next steps

- Publish NUREG on experience from expert clinic
 - Include recommendations relevant to SRM COMGEA-11-0001
- Follow on use of expert judgment process in research projects:
 - Safety demonstration framework
 - Tool automated processes
 - Impact of change
 -



Software-related Uncertainties in Assurance of Digital Safety Systems

RIL-1001

Clinic topics

1. Verification and Validation: Coverage gaps
2. Framework for Safety Demonstration
3. Tool-automated or tool-assisted processes
4. Change Impact Analysis
5. Combined effect of seemingly “small” defects

Template for each topic

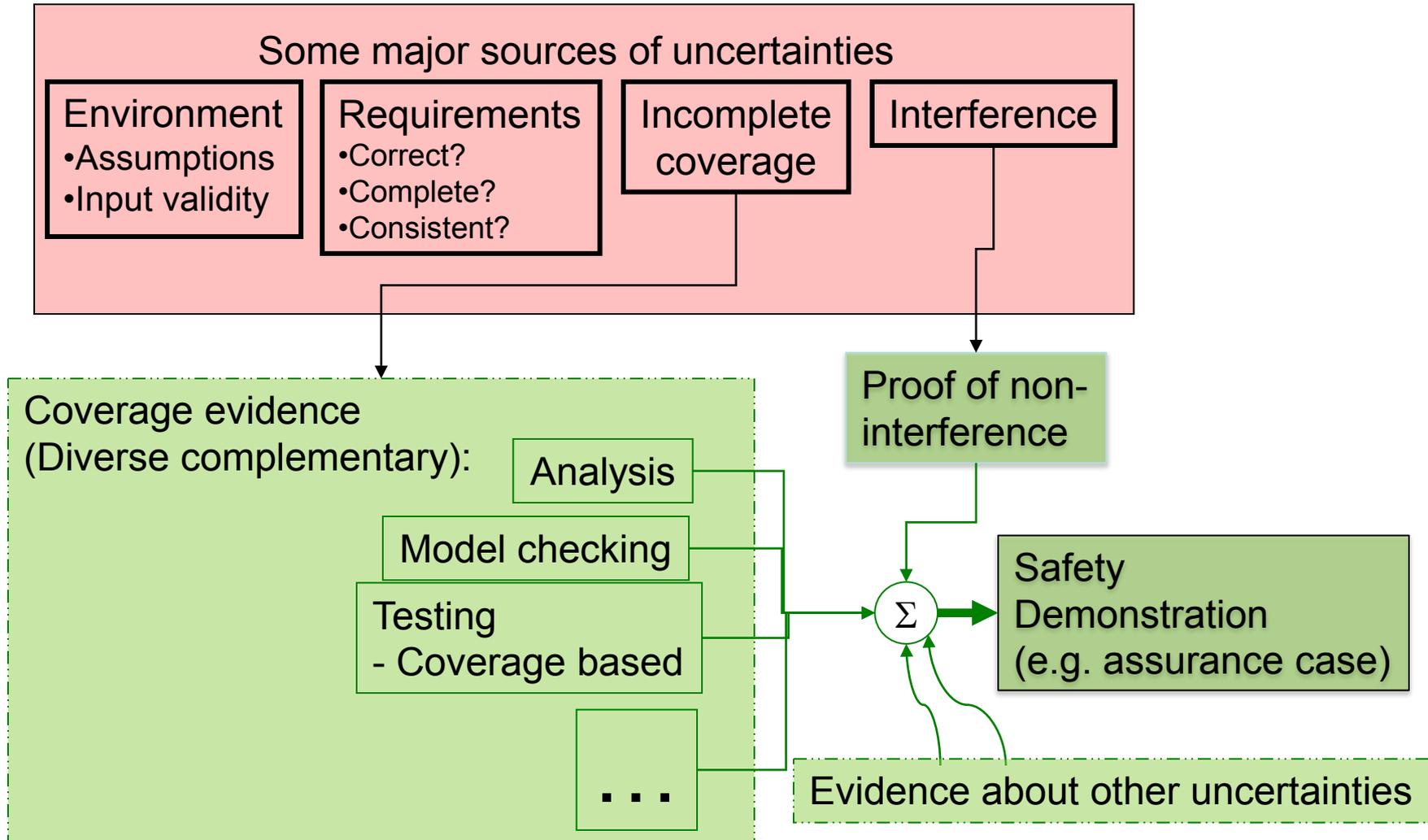
1. Discussion-trigger:
Question on topic-specific uncertainties
2. What evidence could reduce these uncertainties?
3. Knowledge gaps?
4. Degree of strength of validity of conclusions?

Clinic topic 1

Verification and Validation (V&V)

1. Q: “Complete V&V” claim credible?
2. What evidence could reduce the uncertainties?
3. Knowledge gaps?
4. Degree of strength of validity of conclusions?

V&V Uncertainties: Evidence needed



Clinic topic 5 kickoff

Combined effect of seemingly “small” defects



1. Trigger: Likelihood more in software?
2. Evidence to reduce likelihood?
3. Knowledge gap?
4. Degree of strength of conclusions?

Clinic topic 5 outcome

Template question

Likelihood more in SW?

Evidence needed?

Knowledge gap?

Degree of strength of validation?

Outcome

Proposition: More in complex systems

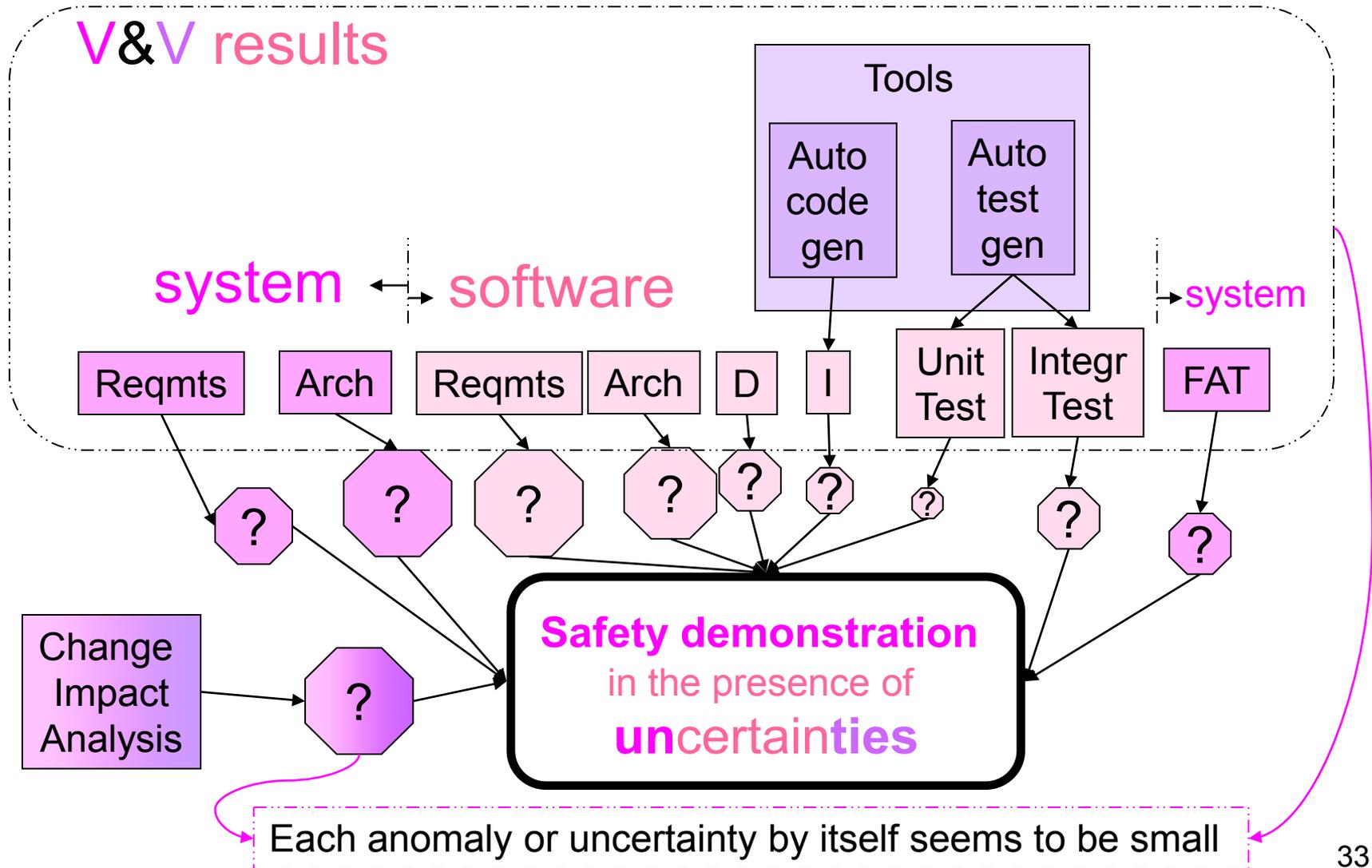
(Implied): Low complexity

Outside the experience of most experts

Low on initially implied proposition.

High in conclusion “Research needed”

Integrating effect of uncertainties



Clinic topic 2

1. Verification and Validation: Coverage gaps
- 2. Framework for Safety Demonstration**
3. Tool-automated or tool-assisted processes
4. Change Impact Analysis
5. Combined effect of seemingly “small” defects

Safety demonstration framework session

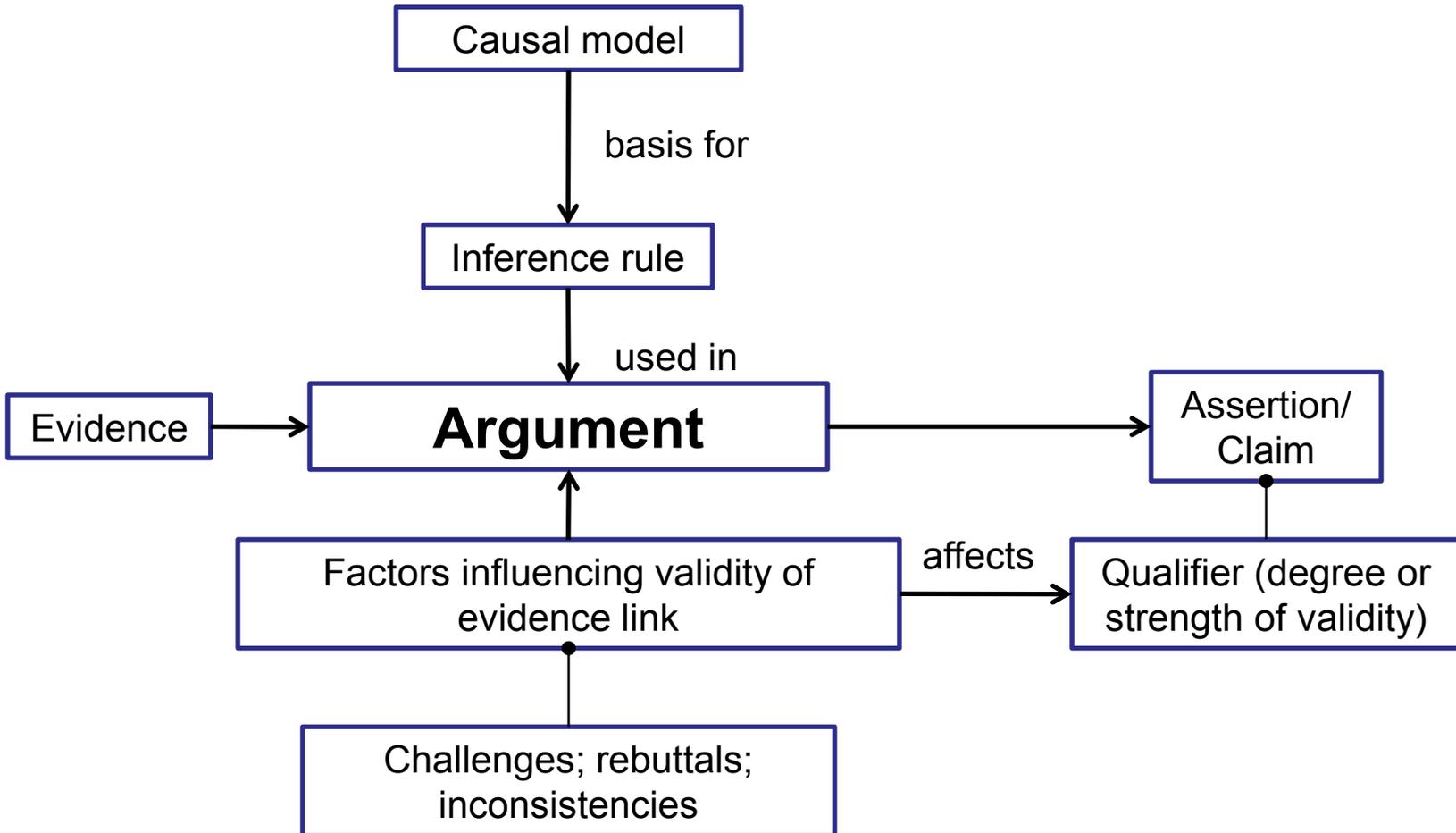
Q: How to evaluate integrated effect of all the uncertainties?

A: Develop a safety demonstration to evaluate effect of uncertainties

What is a safety demonstration?

- Structured argument integrating complementary evidence items
- Shows safety goals are met despite the presence of uncertainties
- Makes explicit the impact of known uncertainties

Argument structure



Safety demo framework – session outcomes

Q: What is needed to reduce uncertainties

A: Argument structure integrating evidence:

Complementary

Diverse redundant

Q: Gaps: Mathematical logic based arguments not always feasible

A: Integrate techniques from different disciplines:

Philosophy; Law; Linguistics;...

Q: Degree of strength of conclusions?

A: High

Clinic topic 3

1. Verification and Validation: Coverage gaps
2. Framework for Safety Demonstration
- 3. Tool-automated or tool-assisted processes**
4. Change Impact Analysis
5. Combined effect of seemingly “small” defects

Clinic topic 3: Tools...

Template question

What new sources of uncertainties...?

Evidence to reduce uncertainties?

Knowledge gaps?

Degree of strength of conclusions

Outcome

[Table 4](#)

Recommendations: Section 5

Conditions: Appendix A.5. [Table 8](#)

Section 7

High

Clinic topic 4

1. Verification and Validation: Coverage gaps
2. Framework for Safety Demonstration
3. Tool-automated or tool-assisted processes
- 4. Change Impact Analysis**
5. Combined effect of seemingly “small” defects

Change impact - summary

Remaining sources of uncertainty?

Many identified: Section 6. Table 5

Evidence to reduce uncertainties?

Many identified. [Table 6](#)

Knowledge gaps?

Indirect, through: Architecture;
Complexity

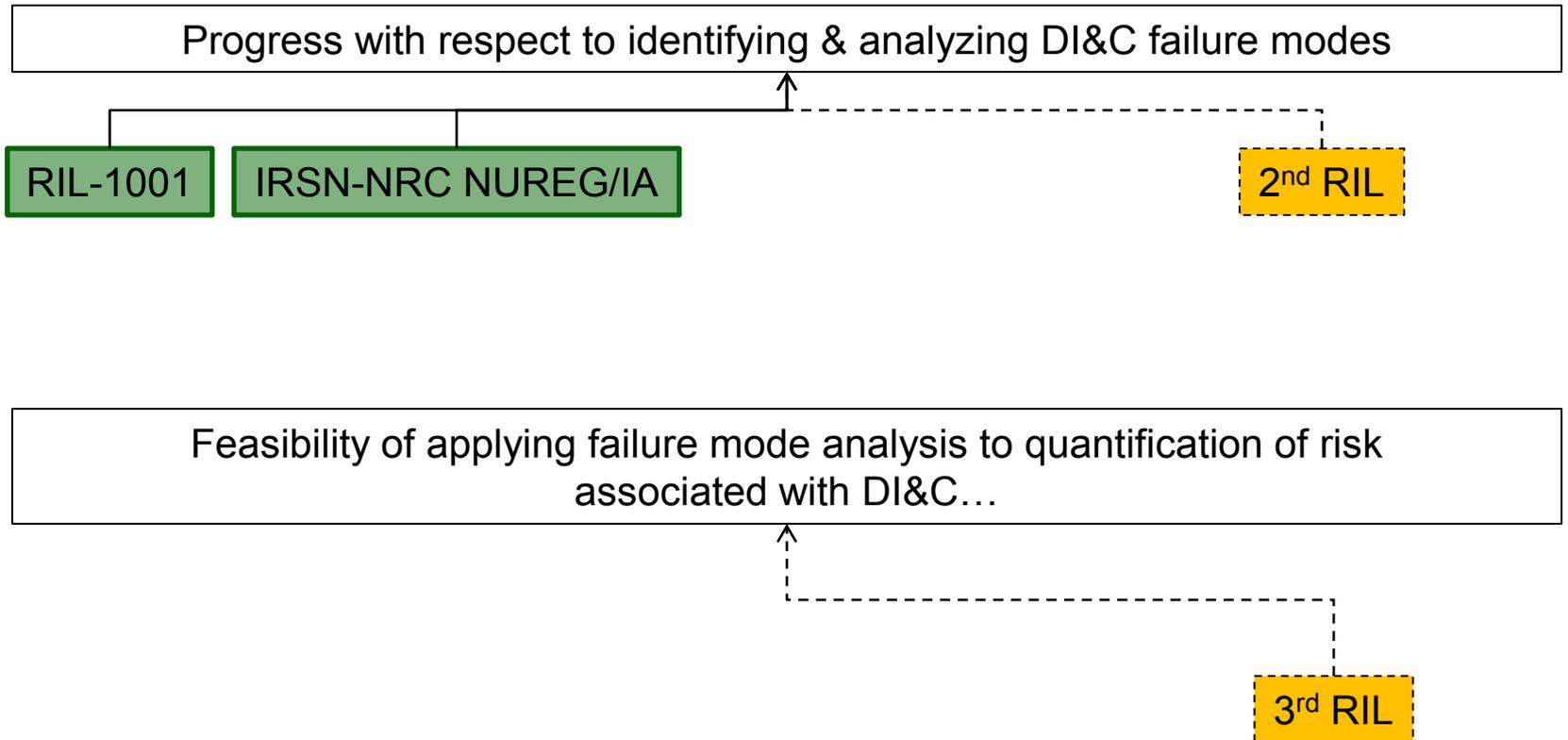
Degree of strength of conclusions?

High

Some other topics

Topic	Reference in RIL-1001
Valid requirements	Appendix A.3, especially Condition #5: Hazard analysis
Architecture <ul style="list-style-type: none"> •Verifiability •Complexity •Freedom from interference 	<ul style="list-style-type: none"> •Executive summary: Items 3, 4 •Section 7 •Appendix A.4

Status summary



Some next steps

- Validate information for 2nd RIL
 - Follow-on interviews of previously identified experts
 - Interview people with industrial experience
- Complete 2nd and 3rd RILs
- Research projects:
 - Safety demonstration framework
 - Tool automated processes
 - Impact of change
 -

Acronyms – 1/3

Acronym	Meaning
ACRS	Advisory Committee on Reactor Safeguards
Arch	Architecture
Auto	Automated
BNL	Brookhaven National Laboratories
D	Design
Demo	Demonstration
DI&C I&C	Digital Instrumentation & Control Instrumentation & Control
EDO	Executive Director of Operations
FAT	Factory Acceptance Testing

Acronyms – 2/3

Acronym	Meaning
FY	Fiscal Year
FSAR	Final safety analysis report
gen	Generation
I	Implementation
Integr	Integration
IRSN	Institut de Radioprotection et de Sûreté Nucléaire
ISG	Interim Staff Guidance
NAS	National Academy of Sciences
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission

Acronyms – 3/3

Acronym	Meaning
OpE	Operational experience
PRA	Probabilistic Risk Assessment
Q A	Question Answer
Reqmts	Requirements
RES	Office of Nuclear Regulatory Research
RIL	Research Information Letter
Σ	Combination, in the sense of integrated effect
SRM	Staff Requirement Memorandum
SW	Software
Typ	Typically
V&V	Verification and Validation

Optional presentation items

SUPPLEMENT CONCERNING BACKGROUND

...emphasize importance of identification of failure modes...

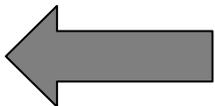
...DI&C may introduce new failure modes that are not well understood.
The SW failure probabilities...do not have a sound technical basis.
These probabilities cannot be very meaningful in the absence of a good understanding of the failure modes.

Examples of DI&C platform failure modes:

Operating-system-task {crash; hang; late response; early response; incorrect response; no response}

Processor (platform?) crash

Input corrupted



ACRS 2010-10-20 letter to EDO

Recommendation #4:

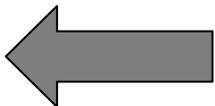
Software Failure Modes and Effects Analysis (FMEA) methods should be investigated and evaluated to examine their suitability for identifying critical software failures that could impair reliable and predictable DI&C performance.

EDO response:

As part of ongoing research under the FY2010-2014 Digital Systems Research Plan, RES/DICB is investigating the efficacy of Software FMEA as a method for identifying faults leading to system failures impairing a safety function.

This effort has involved expert elicitation from numerous international software system engineering experts from both nuclear and non-nuclear domains.

The Staff intends to brief the ACRS DI&C Subcommittee on the outcomes and findings of this research.



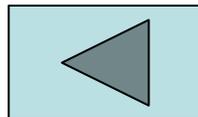
SUPPLEMENT CONCERNING EXPERT JUDGMENT PROCESS

Expert judgment approach

Defined in SRM COMGEA-11-0001:

...the process used to
elicit information from experts,
analyze this information to develop results, and
determine the implications of the results to
support regulatory decision making

“results to support regulatory decision making” includes
decisions about research paths to develop the technical basis for regulatory guidance



Evaluation feedback solicited

1. ...one thing that you liked best about the clinic...
2. In what ways do you feel the clinic was successful?
3. ...an outcome of the clinic that surprised you?
4. ...a topic that you think needs greater consideration?
5. ...a follow up activity that you would recommend?
6. ...facilities and arrangements?
7. Any additional comments?

Extracts from experts' written answers

- Little friction to reach broad consensus (surprising)
- Wish... had more on certification than development
- Follow up engagement of experts on specific topics
- Example of research topic suggested:
 - Validation of requirements (**connects with hazard analysis**)
- Example of collaborative research suggested:
 - Evaluating the strength of safety arguments

Participants' perceptions (heard)

- Participating experts said: “Best ever” experience, e.g.:
 - Method of interaction with experts
 - Complement of experts brought face to face
 - Supporting facilities
 - Facilitation
 - Efficiency of execution
- NRC Observers said: “Best ever”, e.g.:
 - Wealth of information acquired
 - Speed of acquisition (lots of information acquired in short time)
 - Speed of vetting

Expert pool: Follow up activities

- **Candidate pool of 75 experts (starter set)**
 - Profiles available
 - Able to expand resource pool through their referral chains
- **Sample engagements with external experts**
 - Dr. Gerard Holzmann, JPL, at Feb 1 Commission briefing
 - Dr. Alan Wassying, McMasters University, at RIC 2011
 - Dr. John Knight, University of Virginia, 1-day visit
 - Dr. David Parnas, 2-hr teleconference; email discussion
 - Pete Goddard, teleconference; email discussions
 - Herb Hecht, SoHaR , teleconferences; email discussions
- **Experience can be applied in certain research projects**

Lessons learned: What worked well

Tremendous pre-work was key contributor to success

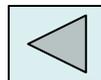
- Initial selection of scope, topics, questions, and issues
 - Known, cross-industry trouble areas (from NAS studies)
 - Relevant to issues experienced in licensing offices
- Matched selection of complement of experts
- Tailored method: Investment in filling experts' gaps
- Final narrowing down to seek a few useful outcomes
 - Significance to licensing offices
 - Need for vetting by group
 - Reachability of broad consensus

No scoring (quantitative synthesis of experts' positions)

- Elicitation of reasoning behind an assertion or belief

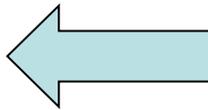
Lessons learned: Limitations

- Method is not a “cookie-cutter” template
- Method was tailored to the questions at hand
- Questions had to be scoped down to available resources
- Method not tested across strong cross-expert conflicts
- Application of method requires extraordinary expertise
- Difficult to execute in turnkey fixed price contract

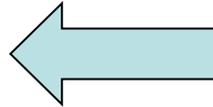


SUPPLEMENT CONCERNING RIL-1001

Verification: Does the system satisfy its requirements?



Are the requirements correct?



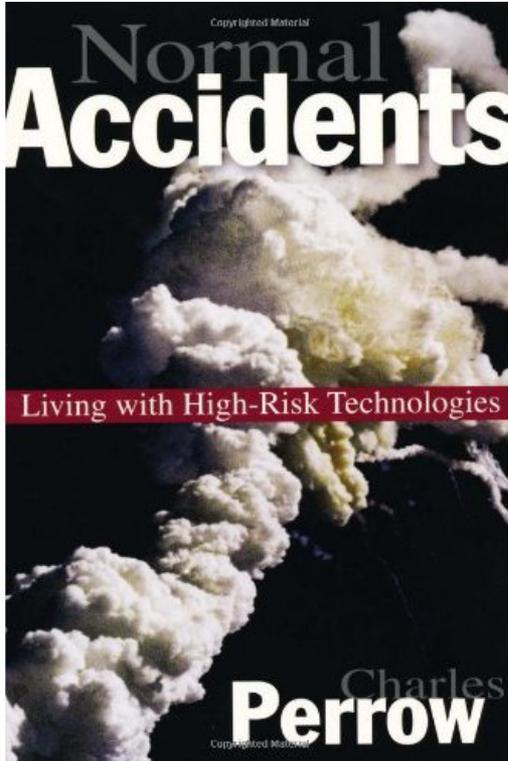


U.S. NRC

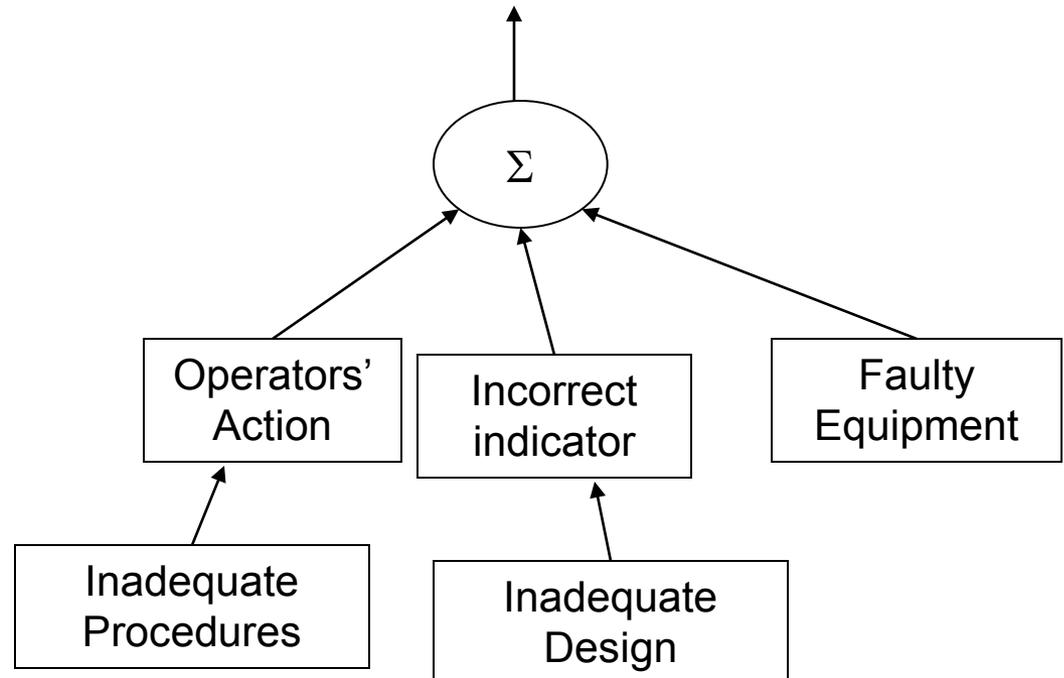
United States Nuclear Regulatory Commission

Protecting People and the Environment

Combined effects of seemingly insignificant deviations



High consequence failure of a complex system



RIL-1001 Table 4 (tools)

ID#	Limitation or challenge	Remark
1	Tool support and validity of results from tool-automated processes is dependent upon appropriate models and methods for requirements engineering, architecture design, coding or code generation, and deployment and the correct fit of the respective work products.	See Appendices A.1-A.6 Serious limitation: Shortage of skilled people.
2	Verification of complex tools such as compilers.	
3	Confidence in certitude of verification.	
4	Adapting traditional software processes to model-based development.	
5	Understanding the effects of automation on the ability of humans to fully comprehend the state of a system or tool.	
6	Determining appropriate mix of human and automation interaction to efficiently leverage respective strengths and compensate for individual weaknesses.	
7	Automation can miss important aspects that have implicitly been performed by humans.	
8	Ability to put enough practical detail in a model to be able to drive the development process realistically enough not to have to tweak results.	



RIL-1001 Table 6 (change impact)

ID	Recommendation	Remarks
1	Items under configuration control and change control should include the safety demonstration and all items on which the safety demonstration is dependent... incl. system architecture, processes, the tools, competencies and data on which the processes depend, supporting tools, operating conditions, and maintenance.	
2	Assure safety demo makes explicit what aspects, features, characteristics, items or other factors the safety argument depends upon....	
3	Include analysis against the original system not just the most recent version.	
4	Test space is large - seek preventative approaches.	See Appendixes A.1-A.6
5	Assure architecture prevents or limits the propagation and effects of change provably.	See "Appendix A.4 – esp. criteria # 5-7
6	Evaluate readability of documentation & code: comprehensibility and consistency	Poor readability leads to mistakes....
7	Check that rationale for design decisions, e.g., architectural, is documented for comprehension by unfamiliar third party.	
8	Maintain traceability documentation to assess impact of changes, e.g. dependencies	
9	Check information is maintained in one place - referenced rather than duplicated	
10	Calibrate the performance of an organization. Adjust review depth accordingly.	
11	Check change crew as qualified & familiar as original developers....	
12	(As defensive measure) Operate new & old for extended periods to validate....	



RIL-1001 Table 8: Evaluation of auto code generation tool set

ID	Factor	Criterion/Constraint/guideline
1	Independence of Verification & Development	Verification cases not dependent on the information that tools and other resources use for automated code generation.
2	Transformation process	The process is mechanized (reduced to a routine) correctly. The process activity is deterministic: I/O unambiguously defined; transformation algorithmically specified.
3	Input	Input language, has a published specification, unambiguously comprehensible to the community of its users - humans and other tools.
4	Output	
5	Composition rules	Unambiguous, published rules of composition in source and target languages.
6	Elements mappable	Unambiguous mapping from each source element to a corresponding target element or composition, such that the mapping is backward-trace-able.
7	Compositions mappable	Unambiguous mapping from a composition of source language elements to a composition of target language elements.
8	Transformation rules	Transformation rules distinctly identifiable, unambiguous, and verifiable.
9	Architecture	Tool architecture provides clear distinction and independence of: Input; Output; Transformation rules and associated data; Transforming mechanism; User interface; Environment in which the input artifact is produced; Environment in which the output artifact is used.
10	Complexity	Unnecessary complexity avoided utilizing sound architectural principles - Appendix A.4
11	Published limitations	The users of the tool are aware of its limitations and conditions of use.
12	User Competence	Users are competent in its correct use for the assigned process activity, considering known limitations.
13	Developer competence	Tool developers' competence is commensurate with the complexity of the assigned tasks.
14	Community of users	The individual persons and other tools, engaged in development or verification or other evaluation activities, or dependent on the tool are identified explicitly, are qualified for ability to use the tool correctly, and are included in the configuration-managed set for which the tool is qualified.
15	Configuration management	The tool and all items and factors on which the correctness of the tool is predicated are configuration-managed as a set, e.g., the restricted versions of the input and output languages, the community of users.





U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

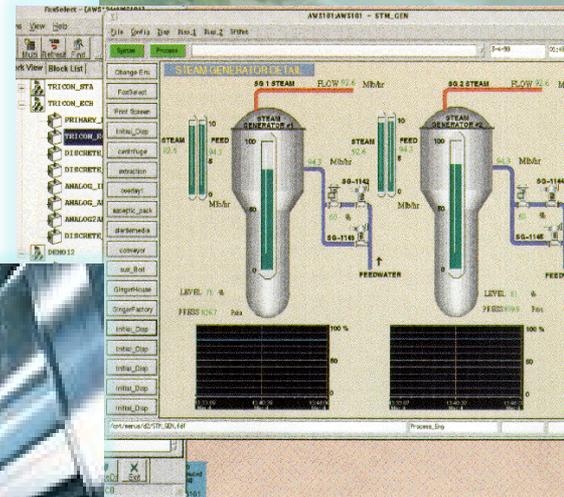
Learning From Digital Operating Experience

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
June 22, 2011

Karl Sturzebecher
Office of Nuclear Regulatory Research
Division of Engineering

Outline

- Operating Experience (OpE) Background
- Learning from Digital Systems Experience
- Collaborative Efforts
 - International
 - Domestic
 - Non-Nuclear
- Framing Process
- Path forward



OpE Background

- Supporting the SRM M070607, dated June 22, 2007, (ML07173024); “1. Develop an inventory and classification... 2. Evaluate the OpE with digital systems”
- Last ACRS Subcommittee on OpE was August 19-20, 2009, with EPRI, Mike Waterman, Debra Hermann, (ML092510087); “..start looking a level deeper and try to match up those failure mechanisms and draw the data from what ever source is appropriate... (p.22)”
- DI&C System Research Plan FY2010 – FY2014, February, 2010, (ML100581484), 3.4.5 Operating Experience Analysis

Learning from Digital Systems Experience

Learning From Digital System Experience

"Every event is a learning opportunity" – Sushil Birla



Learning Experience

- Mining existing data sources such as licensee event reports and Equipment Performance and Information Exchange System (EPRI) is difficult.
- Software and interconnection information is not available from existing data sources.
- Direct contact with the plants is needed to obtain information on system configuration, software, and interconnections.
- NRC and industry should work together to enhance digital inventory data structure and information.

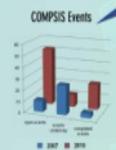
Next Steps
Work with the Institute of Nuclear Power Operations (INPO) and industry to develop enhanced methods for collecting and extracting digital information.

EPRI ELECTRIC POWER RESEARCH INSTITUTE
Improve digital instrumentation and control methods, tools, data, and technical information useful to the U.S. nuclear industry and the U.S. Nuclear Regulatory Commission (NRC).



Learning Experience

- Well-defined requirements can improve system safety and reliability.
- Main root causes are design defects, problems with configuration management, and hardware failures.



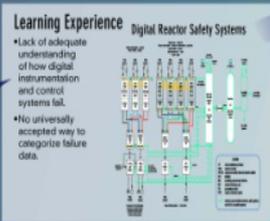
COMPSIS
Computer-based Systems Important to Safety
International participation in collecting information on fault experiences with computer-based safety systems at nuclear power plants.



Next Steps

- Continue adding research grade events.
- Add new lower-severity events to the database.
- Compare data structure with other databases, e.g., Working Group on Risk Assessment (WGRisk).

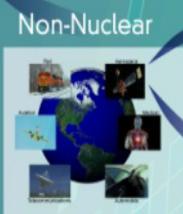
Other Collaborative Activities

Next Steps

- Support a consistent structure for categorizing failure data.
- Research methods for data mining and learning.
- Develop a framework for organizing information.

IRSN Institut de Radioprotection et de Sûreté Nucléaire
NASA National Aeronautics and Space Administration
Methods and Tools
Risk-informed methods and tools from other safety-critical applications domains outside the U.S. nuclear power industry.

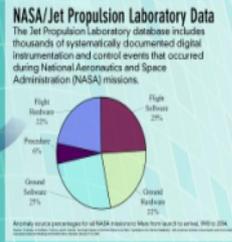


Learning Experience

- More careful and consistent documentation of minor incidents correlates with fewer major incidents.
- While incident frequency drops over time, it will increase whenever new conditions are encountered.

Next Steps

- Gain insight into diagnostics and prognostics.
- Investigate whether the root causes of minor and major events differ.
- Evaluate emerging technologies.
- Investigate NASA software rigor at different quality categories and compare to NPP software rigor.





Canadian Nuclear Safety Commission

- Starting a 2 year plan DI&C activities with NRR
- Feedback on DI&C Safety System Operation Experience



Institute of Nuclear Energy Research (Taiwan)

- Recently established OpE research collaborations under the TECRO-AIT Nuclear Cooperation Agreement



Institut de Radioprotection et de Sûreté Nucléaire (France)

- March 2011 - Started OpE technical exchange activities



Halden Reactor Project (OECD)

- Teleconferences with COMPSIS operating agent

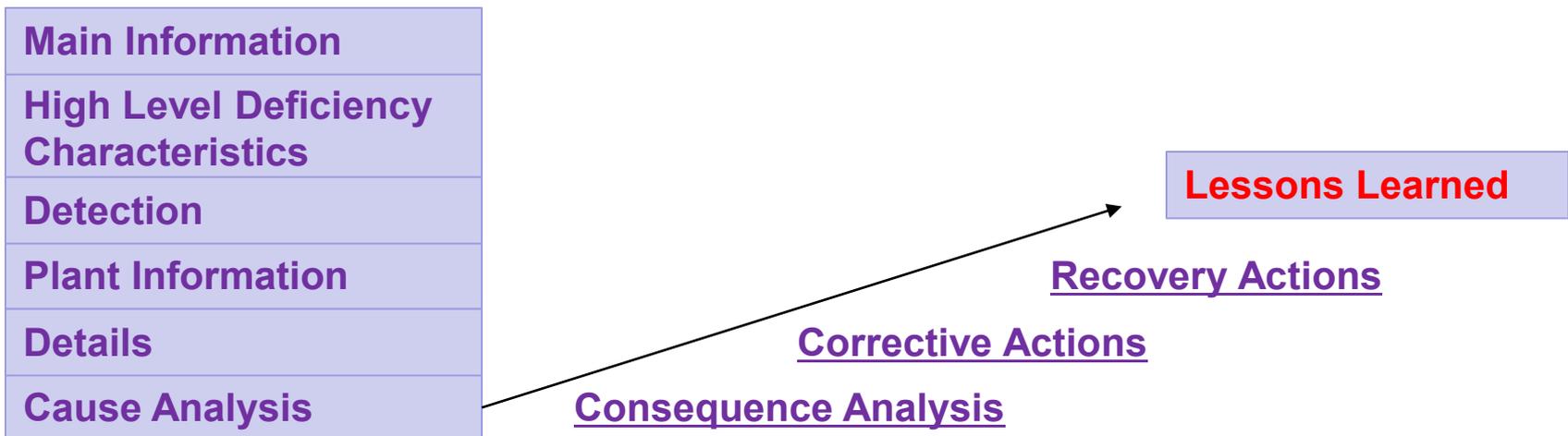
International Efforts

COMPSIS

Computer-based Systems Important to Safety (OECD/NEA)

- CSNI has given the go ahead for a 3rd phase of COMPSIS
- 2005 to 2007 study provided with 27 events with root causes: design defects, configuration management, and hardware failures...
- Continue adding research grade events; recently added 58/80 new events

FIVE REQUIRED FIELDS



International Efforts



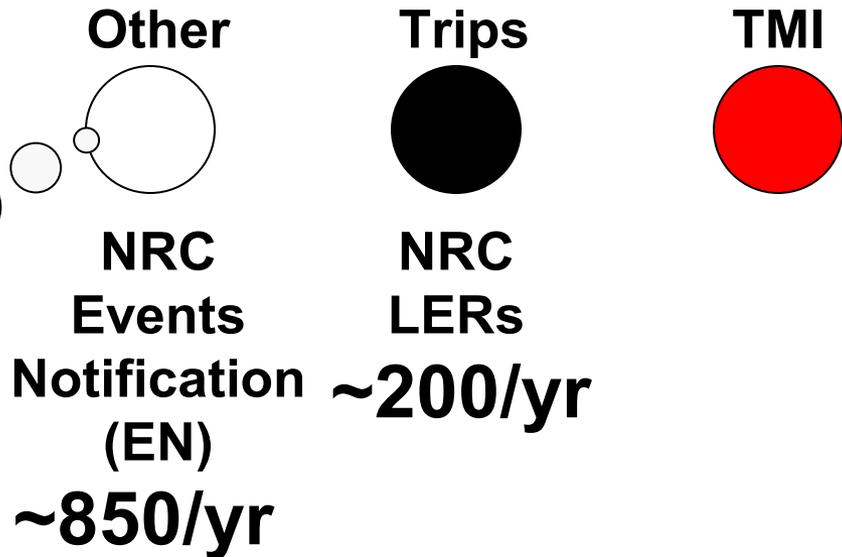
Électricité de France

- Series of discussions with eDF through the EPRI-NRC MOU
- Explore the possibility sharing of OpE



Motorola MC6800 Microprocessor

Event Model



More events !
 Increasing knowledge!
 Each event adds to the learning experience !

Domestic Efforts



Institute of Nuclear Power Operations

Equipment Performance and Information Exchange (EPIX)

- Discussions on improvements to EPIX to identify digital equipment



Electric Power Research Institute

Established MoU – June 2009

- Sharing information on DI&C research objectives and programs
- Develop of tools and data to support digital I&C systems
- Continue technical information-exchange

Domestic Efforts

Inventory and Classification

- Develop understanding of digital systems used or likely to be used in Nuclear Power plants
- Work to date
 - Oak Ridge National Lab draft letter reports on
 - Classification structure
 - Initial inventory
- Upcoming work - develop inventory database

Following NRR's work on the OpE summaries

Non Nuclear Efforts

NASA/JPL Collaboration

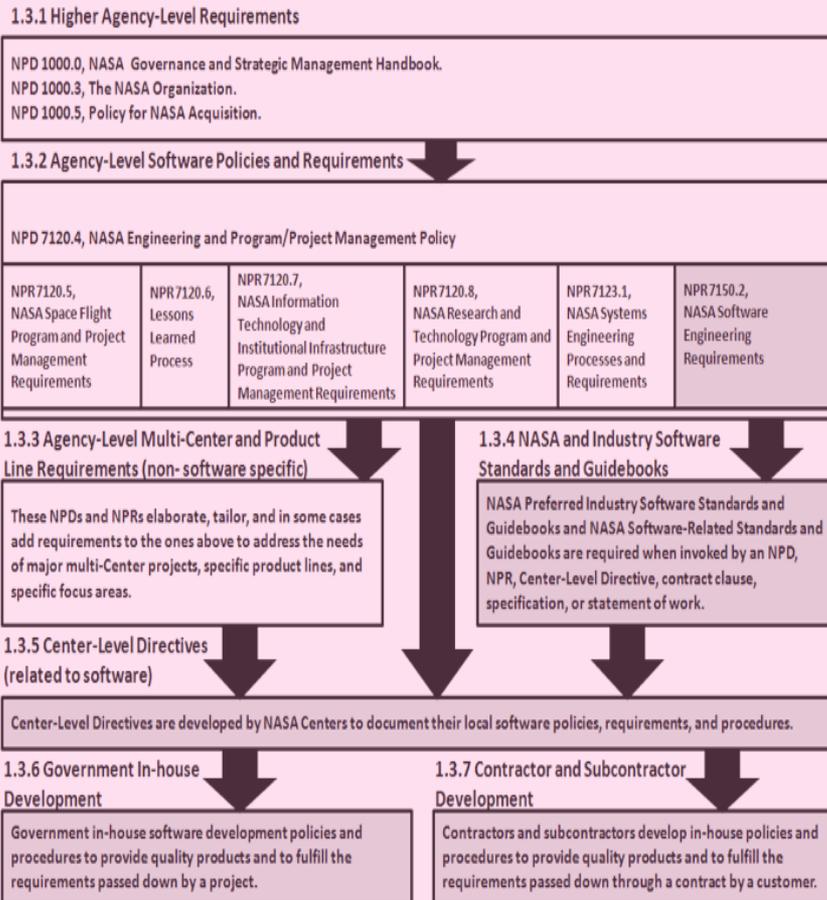
- NASA/JPL MOU with the NRC
- How did their learning influence the process?
- Similarities from shared underlying standards and NASA's role in assurance of contracted software
 - Continuing discussions

Digital I&C-ISG-06: Licensing Process

**NASA Procedural
Requirements 7150.2A:
NASA Software
Engineering
Requirements**

Non Nuclear Efforts

NASA procedural standards map from 7150.2A (P. 7 of 70)



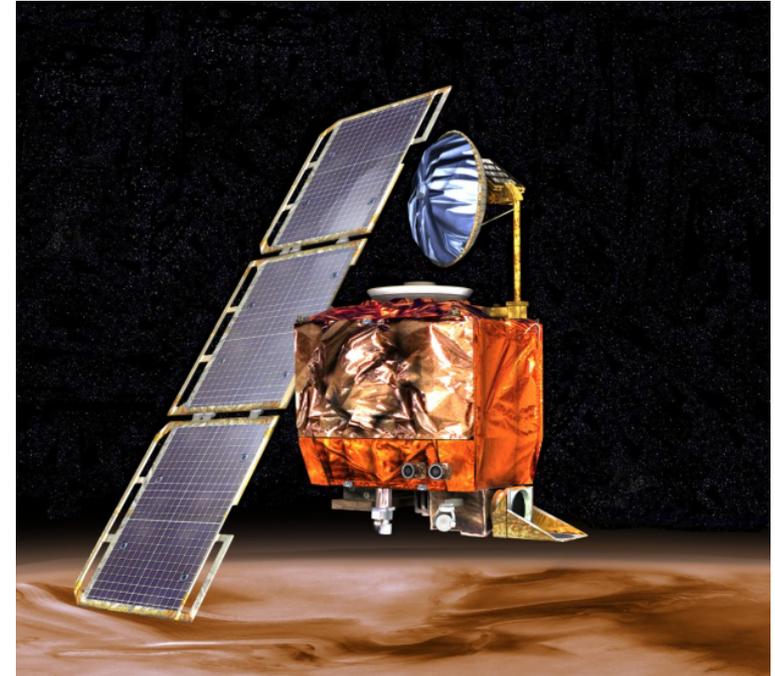
- a. Safety-critical software is initialized, at first start and at restarts, to a known safe state.
- b. Safety-critical software safely transitions between all predefined known states.
- c. Termination performed by software of safety critical functions is performed to a known safe state.
- d. Operator overrides of safety-critical software functions require at least two independent actions by an operator.
- e. Safety-critical software rejects commands received out of sequence, when execution of those commands out of sequence can cause a hazard.
- f. Safety-critical software detects inadvertent memory modification and recovers to a known safe state.
- g. Safety-critical software performs integrity checks on inputs and outputs to/from the software system.
- h. Safety-critical software performs prerequisite checks prior to the execution of safety-critical software commands.
- i. No single software event or action is allowed to initiate an identified hazard. **(9 of 25)**

NASA example software items from 7150.2A (P. 14 of 70)

Non Nuclear Efforts

10 Rules and NASA/JPL Events

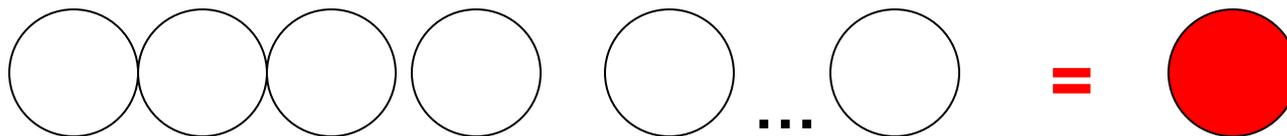
- Dr. Gerald Holzmann's "Power of Ten"
- JPL database: 14,000 mission events for review
- Lessons Learned data listing
- Mission ending events often heavily documented



Mars Climate Orbiter

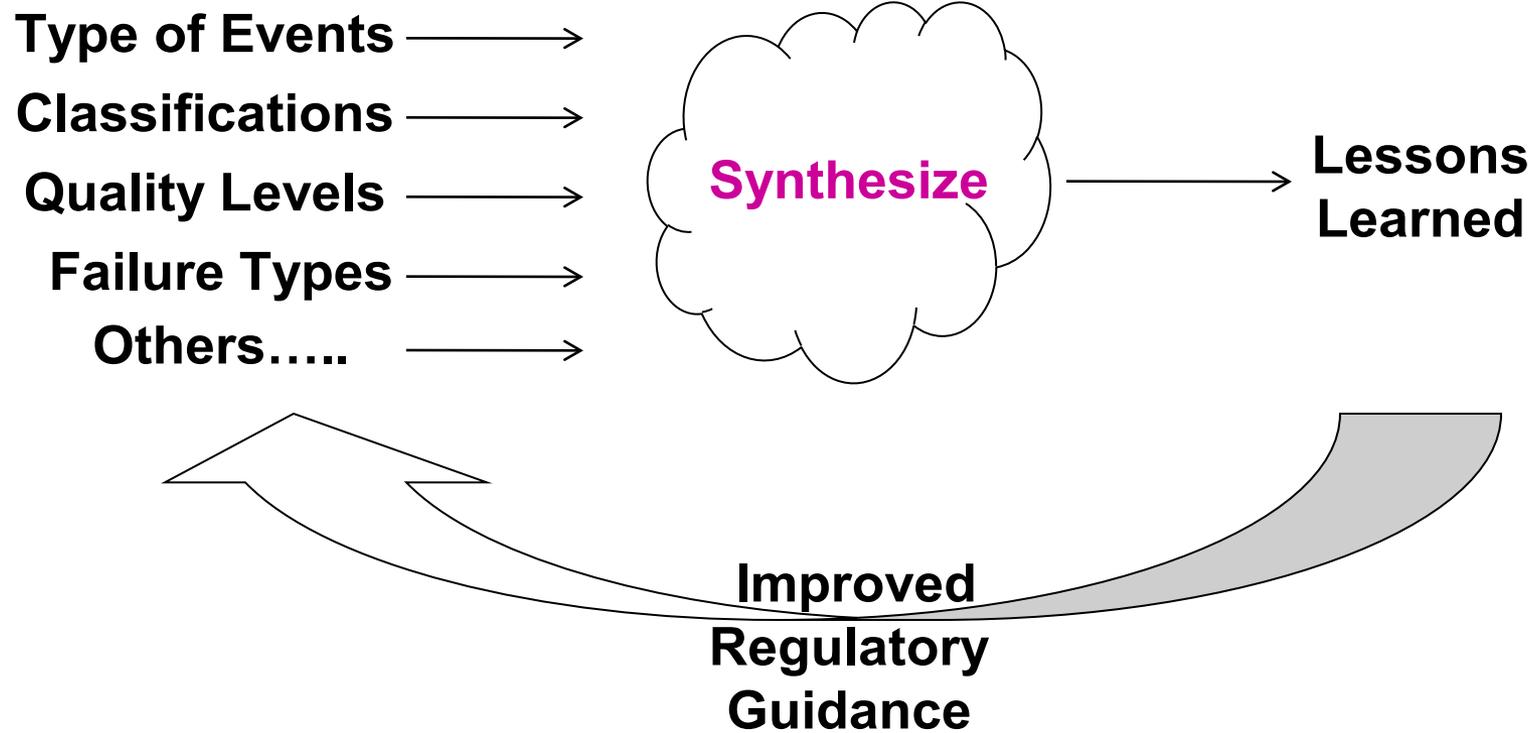
Courtesy of <http://www.jpl.nasa.gov/pictures/solar/mcoartist.html>

- Mars Climate Orbiter Discussion



ftp://ftp.hq.nasa.gov/pub/pao/reports/1999/MCO_report.pdf

Framing Process



Framing Process

Event Attributes: Name of Site,
 Date, System, Event title, Severity,
 Descriptions, Cause, Failure, Quality ...

COMPSIS
 LERs →
 ~53,000 Total

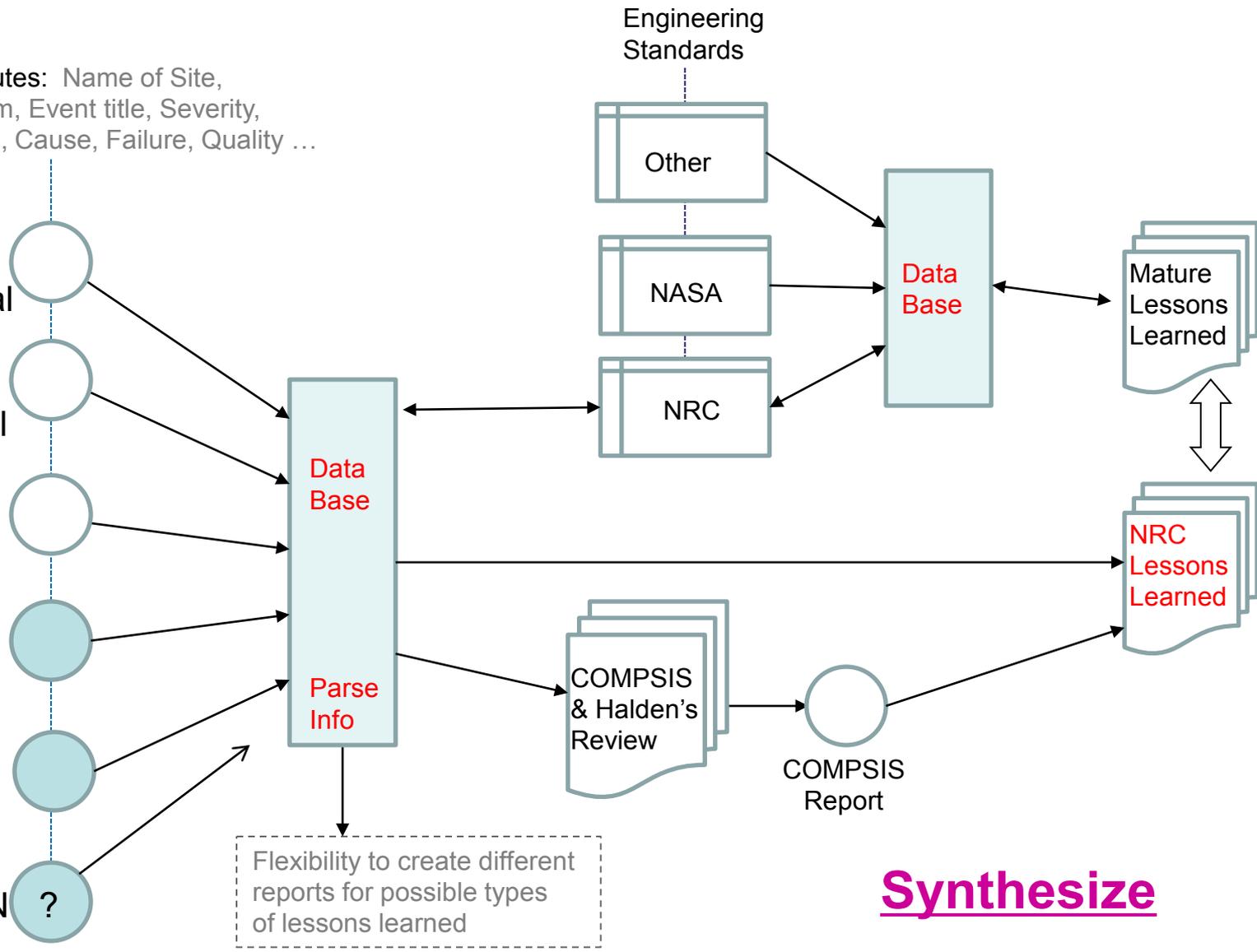
COMPSIS
 ENs →
 ~7,775 Total

Industry
 EPIX →

Inventory
 Study →

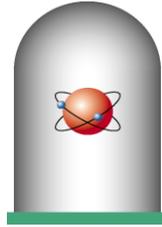
ADAMS →

Others...
 INER, IRSN ?



Flexibility to create different reports for possible types of lessons learned

Synthesize



Path Forward

- Add more events and find sequences
- Continue to expand on the Mind Map
- Transfer techniques from each area of interest
- Build a flexible digital OpE data base
- Develop OpE reports for other NRC branches
- Review lessons learned

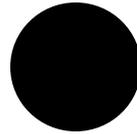
Acronyms

- **ACRS – Advisory Committee on Reactor Safeguards**
- **ADAMS - Agencywide Documents Access and Management System**
- **CNSC – Canadian Nuclear Safety Commission**
- **DI&C – Digital Instrumentation and Control**
- **eDF - Électricité de France**
- **EPIX - Equipment Performance and Information Exchange**
- **EPRI - Electric Power Research Institute**
- **INER – Institute of Nuclear Energy Research**
- **INPO – Institute of Nuclear Power**
- **IRSN – Institut de Radioprotection et de Sûreté Nucléaire**
- **ISG – Interim Staff Guidance**
- **LER – Licensee Event Report**
- **MOU – Memorandum Of Understanding**
- **NASA/JPL - National Aeronautics and Space Administration /Jet Propulsion Lab**
- **NEA – Nuclear Energy Agency**
- **NRR – Office of Nuclear Reactor Regulation**
- **NRC – U.S. Nuclear Regulatory Commission**
- **NPP – Nuclear Power Plant**
- **OpE – Operational Experience**
- **OECD – Organisation for Economic Co-operation and Development**
- **RCIC – Reactor Core Isolation Cooling System**
- **RES – Office of Nuclear Regulatory Research**
- **SRM – Staff Requirement Memoranda**
- **TMI – Three Mile Island**

Backup Slide

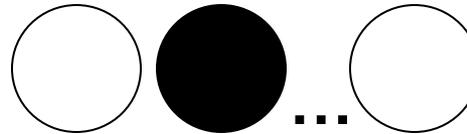
Nuclear OpE Examples

Single Event LERs

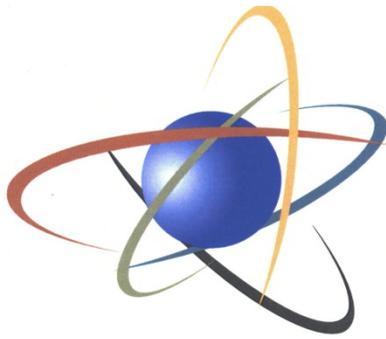


- Power supply related events (LER 3152007001)
- Software design to resolve power supply issues (LER 2372007002)

LER Event Sequences



- Digital Feedwater event with analog RCIC
(LER 4402007001 & 4402007004)
- Push button lacks de-bouncing software feature
(LER 3971996004 & 3971997004)
- Other series for Turbine, Feedwater, Digital Rod Position controls and Core Protection Calculator...



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Redundancy and Independence among Safety Channels

A Whitepaper Prepared by the Office of Nuclear Regulatory Research

**Presentation to the
Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
June 22, 2011**

Paul Rebstock

**Division of Engineering
Office of Nuclear Regulatory Research
(301-251-7488, Paul.Rebstock@nrc.gov)**

- **Proposed Designs & Justifications**
- **Aspects of Independence**
- **Joint Request**

Code of Federal Regulations

- **10CFR50.55a(h) (IEEE 603-1991, as amended)**
- **GDC (10CFR50 Appendix A)**
 - GDC 21, Protection system reliability and testability
 - GDC 22, Protection System Independence
 - GDC 24, Separation of Protection and Control Functions
 - GDC 29, Protection against anticipated operational occurrences
- **10CFR52.47(a)(3)(i)**
invokes the GDC without exception for plants licensed under Part 52

- **Digital I&C Interim Staff Guidance #4**
- **Standard Review Plan – Chapter 7**
- **Regulatory Guides**
(titles are paraphrased)
 - 1.152 computers in safety systems
 - 1.75 independence criteria for electrical systems
 - 1.47 Bypass/InOp status indication
 - 1.53 Single-failure criterion

- **International Perspective**

- MDEP Common Position EPR-01
- Joint Regulatory Position Statement
(United Kingdom, Finland, France)

- **ACRS**

- “Closure of Design Acceptance Criteria for New Reactors,” letter dated 9-19-2010

- **National Research Council**

- Software for Dependable Systems: *Sufficient Evidence?*

- **Not satisfied to say**

“It’s the Rule”

- **To be redundant, entities must be independent**

Simple logic:

If “A” needs “B” then “A” cannot act if “B” fails.

- ***Beyond Good Design***

- » *Thorough V&V does not obviate the need for redundancy.*
- » *Thorough analysis cannot obviate the need for independence.*

- ***The need for simplicity***

- **Must not compromise the safety function**
 - Receiving system must not *need* the information to perform its safety function
 - Communication process must not be able to interfere with the safety function
- **Automatic trip on loss of incoming information is not sufficient**
 - Receiving system cannot detect bad data independently

Each redundant channel must be capable of performing its safety function...

- **Without the participation of any component in the channel(s) to which it is redundant.**

AND

- **Without need for:**

- information from
- connection to
- proper operation of

... **any equipment or device outside its own safety division**

- **This conclusion is a reaffirmation of existing regulations**
 - Not a new interpretation
 - Not a new regulatory position
- **No new rule seems necessary**
- **Updated guidance may be warranted**

- **Any provision that is claimed to improve system performance, but which also increases the possibility of system failure, should be viewed with a great deal of skepticism.**
 - *One must distinguish between improvement in safety performance and improvement in economic performance.*
- **It seems unlikely that the installation of a digital safety system could fall under 50.59**
 - *It could be difficult to prove the absence of new failure modes and consequences.*

● **Hardware complexity**

- Compared with typical “analog” modules...
 - Higher parts count
 - Programmable components, use of firmware
 - Programming & state-based operation complicate testability
 - Far higher module complexity

...do some of the concerns related to software also apply to this type of hardware?

● **Diversity considerations**

- “Diverse” functions executed on the same processor might not be sufficiently diverse.



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Knowledge Management: Strategies and Practices in Digital I&C

Milton Concepcion

Digital Instrumentation and Controls Branch

Division of Engineering

Office of Nuclear Regulatory Research

- Section 3.4 of Digital Systems Research Plan 2010-2014, Knowledge Management
 - Survey of Emerging Technologies (RES 3.4.1)
 - Collaborative and Cooperative Research (RES 3.4.2)
 - Standards Development, Regulatory Guidance, and Regulatory Review Guidance (RES 3.4.3)
 - Organization of Regulatory Guidance (RES 3.4.4)
 - *Operating Experience Analysis (RES 3.4.5)*

Survey of Emerging Technologies

- Objective: Explore emerging (i.e., R&D stage), early adoption, and established Digital Instrumentation & Controls (DI&C) that may have applicability for safety-related systems in nuclear power plants.
- Periodic NUREG-series reports (3 complete)
 - 2003, NUREG/CR 6812 (ML031920412)
 - 2006, NUREG/CR 6888 (ML060870216)
 - 2009, NUREG/CR 6992 (ML092950511)

Collaborative & Cooperative Research

- Objective: Establish active collaborative and cooperative liaisons with domestic, international experts in DI&C and leverage research activities and products from other agencies.
 - Keep up with the rapidly changing DI&C technologies.
 - Better understand the potential for systemic failures in DI&C systems.

External Collaboration & Cooperation

Universities

- SEI, Carnegie Mellon
- Mass. Institute of Technology
- McMaster University
- Ohio State University
- University of Maryland
- University of Virginia
- Vanderbilt University

Federal/NITRD

- NASA/JPL
- NSA
- NSF
- FDA
- FAA/RTCA
- DOD
- NIST
- DHS

International Partners

- Halden Research Program
- AEC/INER
- IRSN
- KAERI
- Safety Critical Software Task Force (SCS-TF)
- Software Certification Consortium (SCC)

National Labs

- Brookhaven (BNL)
- Idaho (INL)
- Oak Ridge (ORNL)
- Pacific Northwest (PNNL)
- Sandia (SNL)

Industry Partners

- EPRI
- INPO

DICB
Collaboration
Efforts

Intergovernmental Organizations

- OECD/NEA/MDEP DI&C-WG
- OECD/NEA/CSNI COMPSIS
- IAEA

Standards Development Participation

- Objective: Enhance consistency of existing DI&C regulatory guidance by leveraging cooperation among standards developing organizations (SDOs) responsible for the coordination, promulgation, and maintenance of consensus standards.
 - Minimize NRC-specific standards
 - Incorporate existing regulatory guidance
- Federal and agency specific guidance
 - OMB Circular A-119, and NRC Management Directive 6.5
- Collaborators Include:
 - NRC Offices: NRO, NRR, NMSS
 - SDOs: IEEE, IEC, ISA, ASME, etc.

Organization of I&C Regulatory Guidance

- Objective: Review the existing framework of regulations and guidance relevant to I&C, organize the guidance, and generate a comprehensive report that will serve as the basis for the development of an electronic-based support system.
- Specific regulations and guidance include: SRP Chapter 7, RGs, SECY Papers, Generic Letters, Information Notices, RIS, ISG, Industry Standards, NUREGs.
- Collaborators include:
 - Oak Ridge National Laboratory
 - Office of Information Services (OIS)

Acronyms

- AEC/INER - Taiwan Atomic Energy Council / Institute of Nuclear Energy Research
- DI&C – Digital Instrumentation and Controls
- EPRI – Electric Power Research Institute
- HRP – Halden Research Project
- IAEA – International Atomic Energy Agency
- IEC – International Electrotechnical Commission
- IRSN – Institut de Radioprotection et de Sûreté Nucléaire
- ISA – International Society of Automation
- ISG – Interim Staff Guidance
- KAERI – Korean Atomic Energy Research Institute
- MDEP – Multinational Design Evaluation Programme
- OECD – Organisation for Economic Co-operation and Development
- OIS – NRC Office of Information Systems
- OMB – Office of Management and Budget
- RG – Regulatory Guide
- RIS – Regulatory Issue Summary
- SRP – Standard Review Plan

Summary of Digital Instrumentation and Control Research Products from 2008-2011

Informational Handout for June 22, 2011 ACRS

Safety Aspects of Digital Systems

DI&C Failure Mode research (regulatory use – improve understanding of DI&C system failure modes to support improved safety assurance)

An Investigation of Digital I&C System Failure Modes, ORNL/TM-2010-32, March 2010
ML102210520

Digital I&C Systems Inventory and Classification study – two draft ORNL letter reports currently under review

Research Information Letter, RIL -1001. Software Related Uncertainties in the Assurance of Digital Safety Systems, Expert Clinic Findings, Part 1

NUREG/IA – 0254, Suitability of Fault Modes and Effects Analysis for Regulatory Assurance of Complex Logic in Digital Instrumentation and Control Systems, TBD 2011

Digital PRA Research (regulatory use – develop PRA methods for digital systems)
NUREG/CR – 6985, A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems, February 2009

NUREG/CR – 6962, Traditional Probabilistic Risk Assessment Methods for Digital Systems, October 2008

NUREG/CR – 6997, Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods, September 2009

Security Aspects of Digital Systems

Cyber Security (regulatory use – guidance and knowledge management in support of 10 CFR 73.54)

RG 5.71, Cyber Security Programs for Nuclear Facilities, January 2010

Digital Platform Cyber Vulnerability Assessments –

- Westinghouse Common Q, June 2009 (ML092160792)
- Plant Data Network, June 2009 (ML092160781)
- Invensys Tricon, September 2009 (ML092590732)
- AREVA Telerperm TXS, May 2011 (ML111310003)
- Port Tap, July 2009 (ML092530291)

NUREG/CR – XXXX, Wireless Network Security for Nuclear Facilities (internal review)

NUREG/CR – XXXX, Secure Network Design for Nuclear Power Plants (internal review)

Security Aspects of Digital Systems (continued)

EMP/HRF Threats (regulatory use –regulatory impact assessment)

EMP/HRF Impact Study - Assessing Vulnerabilities of Present Day Digital Systems to Electromagnetic Threats at Nuclear Power Plants, Sandia Report, December 2009 (ML111670005)

A Comparison of HEMP MHD and Geomagnetic Induced Currents and a Preliminary Assessment of Digital System Vulnerability at Nuclear Power Plants, Sandia Report, December 2010 (ML111670006)

Advanced Nuclear Power Concepts

ORNL Letter Reports (regulatory use – support HTGR research plan and regulatory review of NGNP license submittal)

LTR/NRC/RES/2010-002, TASK 1, Instrumentation in VHTRS for Process Heat Applications (NRC Project No. N6668)

LTR/NRC/RES/2011-002, Task 2. Impact of Operating Conditions on Instrumentation During Normal Operation and Postulated Accidents

LTR/NRC/RES/2011-003 TASK 3. Models for Control and Protection System Designs in VHTRS

Knowledge Management

Regulatory Guide updates (regulatory use – update and maintain NRC regulatory guidance)

RG 1.47, Rev 1, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, February 2010

RG 1.62, Rev 1, Manual Initiation of Protective Actions, June 2010

RG 1.151, Rev 1, Instrument Sensing Lines, July 2010

Draft Regulatory Guides- Seven in the update Process (under internal review)

DG- 1141, RG- 1.105 Rev 4, Setpoints for Safety Related Instrumentation

DG-1267, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

DG-1206, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

DG-1207, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

DG-1208, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

DG-1209, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

DG-1210, Developing Software Life Cycles for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

Other Knowledge Management research (regulatory use – anticipatory research)

NUREG/CR – 6992, Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update, October 2009

Recently completed 2005 - 2009 DI&C Research projects

NUREG/CR – 6991, Design Practices for Communications and Workstations in Highly Integrated Control Rooms, September 2009 (technical basis for ISG-4)

NUREG/CR – 7006, Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems Plant, February 2010 (technical basis to support license reviews and develop a RG)

NUREG/CR – 7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, February 2010 (technical basis for ISG-2 and BTP 7-19)

NUREG/CR – XXXX, Large Scale Validation of a Methodology for Assessing Software Quality (pending publication), TBD 2011 (exploratory research on use of software metrics for assurance purposes)

NUREG/CR – 6895, Technical Review of On-Line Monitoring Techniques for Performance Assessment, Volume 2: Theoretical Issues, May 2008 (technical basis to support license review of applications for using on-line monitoring for tech spec surveillance)

NUREG/CR – 6895, Technical Review of On-Line Monitoring Techniques for Performance Assessment, Volume 3: Limiting Case Studies, August 2008 (technical basis to support license review of applications for using on-line monitoring for tech spec surveillance)