

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Tuesday, May 21, 2013

Work Order No.: NRC-4237

Pages 1-316

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

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

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

TUESDAY

MAY 21, 2013

+ + + + +

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,
Jr., Chairman, presiding.

Reported by Toby Walter

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

1 COMMITTEE MEMBERS:

2 CHARLES H. BROWN, JR. Subcommittee Chairman

3 DENNIS C. BLEY, Member

4 JOHN W. STETKAR, Member

5 MYRON HECHT, Consultant

6 NRC STAFF PRESENT:

7 CHRISTINA ANTONESCU, Designated Federal

8 Official

9 JOHN LAI, Acting Designated Federal

10 Official

11 ALSO PRESENT:

12 MIKE CASE, RES

13 KARL STURZEBECKER, NRR

14 STEVEN ARNDT, NRR

15 NORBERT CARTE, NRR

16 WILLIAM ROGGENBORDT, NRO

17 DAN SANTOS, NRO

18 RICH STATTEL, NRR

19 JOHN THORP, NRR

20 TUNG TRUONG, NRO

21
22
23
24
25

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

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

TABLE OF CONTENTS

| <u>ITEM</u> | <u>PAGE</u> |
|----------------------------|-------------|
| Opening Remarks | 4 |
| Introduction | 7 |
| Overview of RG 1.173 | 12 |
| Overview of RG 1.172 | 104 |
| Overview of RG 1.171 | 135 |
| Overview of RG 1.170 | 159 |
| Overview of RG 1.169 | 205 |
| Overview of RG 1.168 | 256 |
| Question & Answer | 279 |
| Closing Remarks | 309 |
| Adjourn | |

P R O C E E D I N G S

8:30 a.m.

CHAIRMAN BROWN: The meeting will now come to order.

This is a meeting of the Digital Instrumentation and Control Systems Subcommittee. The date is obviously May 21st. That's in my reading notes. So, I have to say that, I guess.

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

I am Charles Brown, Chairman of the Subcommittee. ACRS Members in attendance are Dennis Bly and John Stetkar. Myron Hecht is also participating as a consultant for the Subcommittee.

Christina Antonescu is the Designated Federal Official. For our staff in her absence, for the short period of time here, John Lai will fill in while she arrives.

During this meeting, the staff will discuss six Regulatory Guides on computer software, which endorse the latest IEEE software standards.

One thing I'd like to say thank you for before this, about a week and a half or two weeks ago, whatever it was, I did request that Karl revise the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 meeting minutes to expand them somewhat, to give us a
2 little bit more, to kind of allocate time, and to
3 identify some subjects of what we would be talking about,
4 in a little bit more expansive manner, and he did that.

5 I understand you had some assistance from
6 a couple of your compatriots. I think it was Dave Rahn
7 and Norbert Carte, that helped you with that.

8 So, I really do appreciate their extra
9 effort at the late -- you know, last minute, to provide
10 a significantly expanded set of slides for the meetings,
11 I think which will be helpful. I took a quick look at
12 them last night, and I thought that would be very useful
13 to the meeting today.

14 So, I wanted to thank you all for your extra
15 effort there.

16 The Subcommittee will gather information,
17 analyze relevant issues and facts, and formulate the
18 proposed positions and actions, as appropriate for
19 deliberation by the full Committee.

20 The rules for participation in today's
21 meeting have been announced as part of the notice of this
22 meeting, previously published in the Federal Register
23 on May 10th, 2013.

24 We have received no written comments or
25 requests for time to make oral statements from members

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 of the public, regarding today's meeting.

2 Also, we have on the bridge phone, listening
3 to the discussions, Skip Butler, Peter Yandow, Patricia
4 Campbell, Jerald Head, all from GE Power and Water, and
5 Anthony Masters, Jodi Rappe, NuScale Power, and a couple
6 of staff from the Construction and Inspection Branch
7 from Region II Atlanta.

8 First thing I'd like to do is, if there is
9 anybody else on the line, would you please identify
10 yourselves at this time?

11 MEMBER STETKAR: We need to open it.

12 CHAIRMAN BROWN: I guess that's a good
13 idea. We need to open the lines. So, we'll check to
14 see that we've got everybody. Thank you, John. Good
15 morning, Christina.

16 Subsequent to this, for precluding
17 interruption of the meeting, the phone line will be
18 placed in the 'listen-in' mode during the discussions
19 and presentations, and Committee discussions.

20 A transcript of the meeting is being kept
21 and will be made available as stated in the Federal
22 Register Notice.

23 Therefore, we request that participants in
24 this meeting use the microphones located throughout the
25 meeting room, when addressing 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 volume,
3 so that they may be readily heard.

4 We can now proceed with the meeting, after
5 I check now, to see if we do have actual people that can
6 talk on the phone right now and tell us they're there.
7 Can anybody say something?

8 MR. BONNEY: Yes, this is Matthew Bonny
9 with GE Hitachi Nuclear.

10 CHAIRMAN BROWN: Okay, anybody else?

11 MS. RUDY: Sarah Rudy, GE Hitachi.

12 CHAIRMAN BROWN: Keep talking. Anyone
13 else?

14 MR. BUTLER: Skip Butler with GE Hitachi
15 Nuclear.

16 CHAIRMAN BROWN: Okay, and anybody else
17 want to pipe up?

18 I guess that's it. Thank you very much.

19 John, could you get them to mute the -- okay,
20 thank you.

21 All right, I will now call on Mr. Mike Case,
22 Director of the Division of Engineering in the Office
23 of Research, to provide some opening remarks.

24 MR. CASE: Okay, thanks. Thanks,
25 everybody, for coming. This is a good effort.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I actually have two interests in these set
2 of Reg Guides.

3 Karl used to work for me. So, the reason
4 that Karl is doing these Reg Guides is, he started in
5 the Office of Research and he started on this project,
6 and he moved over to NRR, and so, now, he actually works
7 for NRR, but NRR was nice enough to let him continue with
8 this project, because he had a lot of time and sweat
9 equity in the project, and we want to get it done right.

10 My second interest comes because I also have
11 the Reg Guide update program, and so, I have a staff that
12 does that.

13 And so, I think that -- I haven't done this
14 in a while, so, I just wanted to give you a sense of where
15 we are in the Reg Guide update program.

16 There is about 454 Reg Guides in the NRC's
17 overall suite of Reg Guides. These are six of them.

18 We've updated about two-thirds of them.
19 So, we've been making good progress on that, and quite
20 frankly, ACRS has been an unindicted co-conspirator in
21 making that progress. So, we really appreciate, you
22 know, their support to that.

23 These are what I would probably term normal
24 updates, in that, you know, if you look at what was in
25 these guides before, they're pretty old. They're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 vintage 80's and 90's, and so, it's always important to
2 me that we get some of these things up to modern
3 standards. So, I think that is a great outcome of this
4 particular endeavor.

5 But what I think we need at this point is
6 a good sports analogy. So, when I look at my desires
7 for this particular endeavor, these six Reg Guides, it
8 reminds me of a golf tournament.

9 So, quite frankly, what I'm shooting for on
10 this hole is par, in that Karl had a lot of good strokes
11 along the way with these six Reg Guides.

12 So, let's see, he's updated them to current
13 standards, for the most part. He's made them
14 complementary among themselves, and he made them
15 complementary with our other guides.

16 So, that is another good stroke of Karl, as
17 he moved along, and then the third one, he got the major
18 offices to agree to all of this, which is -- in the I&C
19 world, that's a pretty unusual task.

20 And so, he got NRR involved. He got NRO
21 involved. He got NSIR involved. He got Research
22 involved, and he got them all to agree to these six Reg
23 Guides, which is a terrific accomplishment.

24 So, I think I'm just shooting for par on this
25 hole. I want Karl to get on the green and I want him

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 to be able to tap it in after this particular meeting.

2 Now, what is the ACRS's role? You know, I
3 didn't want to insult you, but I think you guys are the
4 caddies, but successful caddies in the PGA tour earn a
5 lot more money than I do.

6 CHAIRMAN BROWN: You just lost it.

7 MEMBER STETKAR: Think of us more as the
8 hole.

9 MR. CASE: You know, we actually want your
10 advice and guidance. You know, we want to make sure Karl
11 keeps his elbow straight. You know, we want to make sure
12 that he keeps his eye on the ball.

13 But probably what we don't want him to do
14 is, we don't want you to encourage him to try and drive
15 it over the water hazard, nor do you want to try and say,
16 "Karl, let's see if we can make a hole in one with these."
17 I'm just shooting for par.

18 I think it's important that we get these Reg
19 Guides compatible with today's modern standards. They
20 may not be perfect when they're done, but one of the
21 features of the Reg Guide program, that we haven't had
22 in the past, is that we're not going to leave these things
23 for another 25 years, before we look at them again.

24 We have a five-year program that we started,
25 and we're doing pretty good with getting people to pick

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 these things up, again after five years, and make more
2 improvements.

3 So, with that, and with the Chairman's
4 permission --

5 CHAIRMAN BROWN: But based on John's
6 comment, I think you should hope for a hole in one,
7 doesn't pay for par.

8 MEMBER BLEY: Actually, you should have
9 asked if any of us play golf.

10 CHAIRMAN BROWN: I used to play golf, until
11 I took this job.

12 MR. CASE: So, now, we can turn it over to
13 the Tiger Woods of these particular six Reg Guides.

14 CHAIRMAN BROWN: All right, Karl, fire
15 away.

16 MR. STURZEBECKER: Okay, you know, I'm Karl
17 Sturzebecher.

18 John Thorp, my Branch Chief, and just per
19 the eloquent statement by Mike Case, over here is Dr.
20 Steven Arndt, and I have a couple of members of my Reg
21 Guide team in the back, that they may come up here and
22 there, depending on which guide I'm on.

23 So, with that, I'm going to start with the
24 first slide.

25 This is the agenda I put together. Like you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 said, I re-modified the print -- or the presentation
2 here, and I'm going to go through the background, and
3 it covers what the guidance does, the gang of six, as
4 they're called, or some of the team members call them.

5 I'm going to point out some common topics
6 that came to our attention when we were doing the guides,
7 that kind of cross between each of them, cover who was
8 on the team and some of the learning experiences that
9 we received from other people, and show you a matrix of
10 the actual guides.

11 When I get into the actual -- when we
12 actually work through a Reg Guide, I have a set pattern
13 that I wanted to follow.

14 So, I have this section here, you've
15 probably seen it now, on how I'm trying to explain the
16 materials, so, the mechanics of the presentation, and
17 I'll show -- go through that color key, and I gave you
18 a separate handout for that, so, you can pull it aside
19 from the main presentation.

20 Let's see, I'm going to start with Reg Guide
21 1.173, and go down, and the reasoning for that is 1.173
22 is the umbrella, the overarching guide that the other
23 guides and standards support.

24 At the end, I'm going to have a conclusion
25 and go through some of the differences between the guides

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 and where they're going, and kind of an overall
2 philosophy, I think, of what we're seeing going on, and
3 how we -- what we've adapted to them.

4 So, without further adieu, background.
5 So, these guides, what are they for? Well, they're for
6 making -- developing a safety system software product.

7 The original Reg Guides were released in
8 1997. They were brought out at that time, because there
9 seemed to be a growing number of digital subversions
10 going on.

11 When we reviewed some of the OpE items back
12 in those times, we saw a set of types that -- we've talked
13 about before in the presentation two years ago, about
14 that.

15 So, there is a certain set of LER's that we
16 see during that time period, and the OpE team is looking
17 at what is going on now.

18 So, the way these guides move forward, I
19 hope we're going to be refining that and helping the --
20 following what the industry has done with the standards
21 and what we're following with that, to see less and less
22 LER's, and better overall guidance.

23 MEMBER STETKAR: Before you go to the next
24 slide, I had actually, a -- since we're going to get into
25 details here.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 I had a common topic that I wanted to ask
2 you, or the team about, and it may affect my
3 understanding of several of the Reg Guides, and how
4 they're applied.

5 There is a common footnote in every
6 Regulatory Guide that says, "The term safety systems is
7 synonymous with safety related systems."

8 "The scope of the GDC includes structure
9 systems and compliments important to safety. However,
10 the scope of the Regulatory Guide is limited to safety
11 systems, which are a sub-set of systems important to
12 safety." I understand that.

13 However, in many new plant designs, we have
14 safety related equipment, and we have equipment that is
15 identified as being important to safety, and those are
16 typically SSC's that are populated in either regulatory
17 treatment of non-safety systems RTNSS lists for the
18 passive plant designs, or reliability assurance
19 programs, RAP, for the active plant designs.

20 Those are non-safety related SSC's, but
21 they're important to safety. That's why they're in
22 those lists.

23 Those non-safety related SSC's are
24 typically actuated and controlled by non-safety related
25 digital hardware and software.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 If that is the case, if these Reg Guides only
2 apply to the safety related digital systems and their
3 associated software, what guidance do we have for
4 reviews of that important to safety, by definition,
5 non-safety related software?

6 The reason I bring it up now is, you're going
7 to -- integrity levels, for example.

8 MR. STURZEBECKER: We'll go right to that
9 one.

10 MEMBER STETKAR: Is one way to address
11 that. I mean, you know?

12 MR. STURZEBECKER: Yes, integrity.

13 MEMBER STETKAR: And that does filter
14 through a few of the Reg Guides, not all of them, but
15 a few of them.

16 MR. STURZEBECKER: Right.

17 MEMBER STETKAR: Now, something that
18 struck me, that -- does it mean that in practice,
19 although greater regulatory attention is paid toward --
20 especially RTNSS, because of their designation, but
21 also, the RAP pumps and pipes and valves, if I can call
22 them that.

23 MR. STURZEBECKER: Right.

24 MEMBER STETKAR: Why don't we pay attention
25 to their actuation and control software, perhaps not at

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the same level of scrutiny as the safety related stuff,
2 but more than just something that lives in the plant?

3 MR. STURZEBECKER: I am aware of some
4 companies that do put a feedwater system in, and they'll
5 do it at a 1E level. They are --

6 MEMBER STETKAR: Some of this is a lot more
7 pervasive than just a -- just a stand-alone feedwater
8 control system, though.

9 It's an integrated secondary side of the
10 plant, turbine feedwater, steam. It's much more
11 pervasive in some cases, than just a -- you know, just
12 a single function-oriented set of controls.

13 MR. STURZEBECKER: That may be something we
14 need to look at, consider. Steve, do you have any
15 comments on that?

16 DR. ARNDT: Well, it really gets to the
17 broader concept, and it's not just new reactors, it's
18 current reactors, as well, that in our structure, I&C
19 and a lot of systems, is a 'yes' or 'no' kind of
20 regulatory structure. It's not like what is done in
21 Europe, for example, under the IEC standards, that has
22 multiple levels of regulatory review.

23 First of all, the Reg Guides are products
24 for the industry, as Karl was mentioning. These are
25 methods that we would find acceptable for safety system

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 design, development, etcetera.

2 So, your real issue, the way you phrased it,
3 is really an SRP issue, for our internal review.

4 But they're all integrated together, but
5 right now, our regulatory structure, not just these
6 software guides, but also the entire regulatory
7 structure, is designed around the safety and the
8 non-safety and certain special cases for important to
9 safety systems, such as ATWS and the actuation and other
10 things that have additional requirements.

11 CHAIRMAN BROWN: Let me -- can I make one
12 -- go ahead.

13 MEMBER STETKAR: Let me give you an
14 example.

15 Some plants don't classify -- new plants
16 don't classify their diesel generators as safety related
17 equipment, and yet, they're started and controlled and
18 -- by non-safety related software that senses voltage
19 and loading and all of that kind of stuff.

20 They always show up on the important to
21 safety lists, either as RTNSS or in the active plants,
22 they're typically safety related.

23 That is my concern. I mean, and it's
24 broader than just the control of the diesel itself.
25 It's the whole integrated electro-power system

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 controls.

2 The IEEE standards have provisions for that
3 hierarchical treatment of different levels of software,
4 depending on their safety significance or mission
5 critical significance, or whatever you want to call it.

6 It's just that these particular Reg Guides
7 don't recognize anything other than "safety related".
8 They don't invoke those parts of the existing standards,
9 that the industry may or may not use.

10 But if the regulator says you don't need to
11 use it, industry may not use it.

12 DR. ARNDT: Yes, I think what you're
13 getting at is a broader issue of the diesel generators,
14 for example.

15 The NRC basically has two decision points.
16 One, are we going to accept those systems as non-safety
17 systems?

18 But once we make that decision, then it
19 drops the system into a particular regulatory framework.

20 In the case of the I&C systems, it's either
21 safety or non-safety. We don't have that intermediate
22 --

23 MEMBER BLEY: Well, I guess, John's point,
24 at least when I read up on this --

25 DR. ARNDT: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MEMBER BLEY: -- you have something that
2 isn't safety in a new plant --

3 DR. ARNDT: That's right.

4 MEMBER BLEY: -- but it's RTNSS. It's
5 important to safety, and you're going to have to have
6 some kind of special treatment.

7 DR. ARNDT: Correct.

8 MEMBER BLEY: What about the I&C associated
9 with that?

10 Should we apply the safety grade I&C
11 requirements or --

12 DR. ARNDT: Well, I think --

13 MEMBER BLEY: -- or not, and if it's not,
14 I don't get it, at all.

15 DR. ARNDT: Well, some apply.

16 MEMBER BLEY: How?

17 MR. SANTOS: Some apply still, like some of
18 -- Dan Santos from NRO.

19 Some requirements still apply, like some of
20 the independence type related requirement, where you
21 don't want adverse interaction coming from the
22 non-safety to the safety.

23 At the level of software development, like
24 these Reg Guides may cover, we might not go through that
25 level of detail.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 But at a higher level, what is the -- is the
2 analysis bounding these issues associated with this
3 system? Yes, we have to look at that.

4 MEMBER STETKAR: But that is -- the only
5 requirement is that nothing -- theoretically, nothing
6 that goes on out there in that "non-safety related" part
7 of the world should prevent any safety related function.

8 It doesn't say that it needs to work okay,
9 out there, even though it's important to safety.

10 In other words, if something happens, if the
11 software life cycle, the design implementation
12 requirements don't recognize that the software needs to
13 account for some electrical configuration, and start the
14 diesels or transfer buses, or whatever it's designed to
15 do, there is no way of the regulator following up on the
16 design of the software, according to those functional
17 requirements.

18 As long as it not doing that, doesn't affect
19 any of the safety related systems.

20 DR. ARNDT: Yes, I think --

21 MEMBER STETKAR: Follow me?

22 DR. ARNDT: Yes, no, I know exactly what
23 you're saying, and the point is, the licensee will make
24 a decision, as part of their application, as to what
25 falls into what bins.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 That will drive what analysis we do or do
2 not do.

3 So, for example, diesel generator
4 reliability or functionality, for example, if they've
5 chosen it to be a non-safety system and we've agreed that
6 that's okay, they still fall under DRAP and other
7 reliability programs, because they're important to
8 safety.

9 But the actual software associated with
10 that particular system would not be reviewed against
11 requirements in the SRP or 603 or looked at here.

12 What I'm trying to --

13 MEMBER STETKAR: So, what do I have -- the
14 hardware can be sitting out there, perfectly reliable,
15 and it's monitored by the maintenance rule --

16 DR. ARNDT: Right.

17 MEMBER STETKAR: -- and it's got all of
18 these restrictions applied to it, and yet, it never gets
19 a chance to start because the hardware -- the software
20 --

21 DR. ARNDT: No, but --

22 MEMBER STETKAR: -- has not been reviewed
23 or developed appropriately.

24 DR. ARNDT: The reliability -- the software
25 and the programming and everything else would also fall

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 under the maintenance rule under the -- all the other
2 stuff that the hardware falls under --

3 MEMBER BLEY: But it wouldn't have had this
4 process stuff.

5 DR. ARNDT: It would not have necessarily
6 had a process review.

7 MEMBER BLEY: What we claim, as part of our
8 confidence in the software.

9 DR. ARNDT: Of the safety related software.
10 I know I'm playing word games with you --

11 MEMBER BLEY: But it's not the word game
12 that bothers me. It's the --

13 DR. ARNDT: I know.

14 MEMBER BLEY: Okay.

15 DR. ARNDT: But the point is, we've got a
16 regulatory structure and we've set it up, so that the
17 analysis that we do to ensure safety falls within that
18 structure.

19 I understand your question and your
20 concern, could we not do a better job, if we use some
21 of this structure that already exists in the standards,
22 to look at or impose additional requirements on the
23 important to safety equipment?

24 MEMBER STETKAR: That is really the genesis
25 of my question.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. ARNDT: Right.

2 MEMBER STETKAR: In the places where the
3 standards do explicitly give you this -- this I'll call
4 it hierarchical treatment --

5 DR. ARNDT: Right.

6 MEMBER STETKAR: -- why does the regulatory
7 -- do the regulatory guides not recognize the reality
8 of things, like RTNSS and RAP --

9 DR. ARNDT: Okay, I'll give you --

10 MEMBER STETKAR: -- non-safety, important
11 to safety --

12 DR. ARNDT: -- two answers to that
13 question. One, that you're not going to like and the
14 other one, you may or may not like.

15 The first answer is, our regulatory
16 structure is not set up to be able to do that. We would
17 have to change --

18 MEMBER BLEY: But it can for hardware.

19 MEMBER STETKAR: It is. Why -- it's set up
20 for the diesel, itself, the piece of hardware.

21 DR. ARNDT: We look at those kinds of issues
22 associated with the reliability program, and we can
23 apply that kind of information, under the maintenance
24 rule or the DRAP or whatever, and the licensee is free
25 to use this standard or any other standard, because we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 don't have a particular set of guidance upon it, in those
2 programs.

3 MEMBER STETKAR: But Steve, even in those
4 programs, although it does -- although that piece of
5 equipment doesn't need to meet Appendix B quality
6 assurance, for example, during the procurement process,
7 they do need to meet some sort of enhanced quality
8 assurance, don't they?

9 DR. ARNDT: No.

10 MEMBER STETKAR: It's not just commercial
11 off the shelf.

12 So, even in the design and procurement of
13 that piece of non-safety related important equipment,
14 there are -- the regulatory framework does have enhanced
15 quality --

16 DR. ARNDT: Absolutely.

17 MEMBER STETKAR: -- requirements, in
18 addition to the reliability, you know, the
19 post-installation reliability.

20 DR. ARNDT: Absolutely, and the simple
21 answer is, we haven't provided guidance in the I&C
22 particularly software area, as to how they should
23 demonstrate that.

24 So, the answer is, for the safety related,
25 non-safety related, there isn't structure there to hang

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 on, in terms of maintenance rule or DRAP or the other
2 things.

3 There is regulatory structure to hang it on,
4 and we just simply haven't provided that additional
5 guidance.

6 MEMBER STETKAR: But okay --

7 DR. ARNDT: One option would be in the
8 future, to go down the path that you're suggesting.

9 CHAIRMAN BROWN: Steve, I mean, if I go out
10 and buy a diesel, diesel generator --

11 DR. ARNDT: Yes.

12 CHAIRMAN BROWN: -- and it's a non-safety
13 related -- it's designated non-safety related, and it's
14 got other stuff that you -- you know, we've gone through
15 this discussion, that says hey, it's got other
16 requirements or other things that actually get
17 associated with it.

18 But the governor and the voltage regulator
19 and those types of things that start it and run it are
20 part of that overall system.

21 Why doesn't -- why don't those ancillary
22 systems that are required to make the diesel generator
23 work, why don't they fall under that, or in the case of
24 the feedwater system, if you've got pumps and stuff
25 feeding that, that have to be controlled, why don't --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 why aren't they considered in the umbrella, relative to
2 that, in terms of systems?

3 You're right, these Reg Guides specifically
4 state that for safety systems, you must use -- I'm sorry,
5 you do not say 'must'. You usually worded the word
6 'must' out of all of these Reg Guides, okay.

7 It was in the earlier sets from 10 and 15
8 years ago.

9 Now, it says 'should assign integrity level
10 four', which means you've got to -- you've got to do the
11 whole gamut of everything, to show that they're
12 satisfactory, very explicit, which I don't disagree with
13 the explicitness, except I wish you would have put the
14 'must' in.

15 But I still don't understand why these other
16 non-safety related sub-systems, that are part of a
17 larger overall diesel generator -- but they don't
18 operate unless the governor and the voltage regulators
19 and the starting devices work properly.

20 So, when you tell me I don't have anything
21 that applies to that, I don't know why they fall outside
22 of that umbrella in the QA process, the other more
23 umbrella QA process that you're talking about, as
24 opposed to just a software process.

25 MEMBER BLEY: Before you answer that, if I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 could.

2 We've had some long discussions about
3 hardware in the new plants and how this will be -- what
4 kind of special treatment that will have.

5 But if it's hardware, you know, most of that
6 special treatment will either be inspection or
7 observation or test, reliability programs, that sort of
8 thing, which are -- you can do, after the fact and see
9 how things work.

10 This software development, you're doing
11 ahead of time, and if we're not looking at that ahead
12 of time, I don't know that there are parallel kinds of
13 observations and tests for software, that we'd be able
14 to use as special treatment.

15 So, can you talk to that a little, including
16 Charlie's comment?

17 DR. ARNDT: Well, I'm not going to get too
18 far into this, because this is the -- this is something
19 that I don't want to talk about in gory details off the
20 cuff.

21 But as I've tried to articulate, obviously
22 not sufficiently to explain to Mr. Brown at least, there
23 are requirements, and even though those requirements for
24 non-safety/important to safety systems are not as
25 explicit, we don't have a Reg Guide for how to deal with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 this particular issue.

2 The licensees, or applicants in the case of
3 some of the new reactors, can use this industrial
4 guidance or the Reg Guide itself. We just don't have
5 any particular guidance on it. That is a gap. We just
6 haven't looked at it.

7 As Mr. Brown mentioned, we did make an
8 explicit discussion about software integrity levels and
9 related issues for safety systems, and chose level four
10 only. There was a big discussion about that, when this
11 -- these guides were originally done.

12 Some of our colleagues in the European
13 countries, that use IEC, which also have integrity
14 levels, although they're defined slightly differently
15 than our's, have an intermediate safety classification,
16 the ABC concept. We just don't -- we just haven't chosen
17 to do that at this time.

18 We have an intermediate level, with special
19 treatment requirements, but they're not as well defined.

20 I'm not saying I disagree with you. I'm
21 just saying we haven't, at this point, made that step.

22 CHAIRMAN BROWN: Can I -- we need to kind
23 of move on here a little bit.

24 I think this is -- we're not going to resolve
25 this in this particular discussion. It may be subject

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 for some observations in the letter we write, just to
2 get us thinking about that.

3 But I would -- if that is -- can we move on,
4 John?

5 MEMBER STETKAR: Oh, yes.

6 CHAIRMAN BROWN: Okay, Dennis?

7 MEMBER BLEY: Yes.

8 CHAIRMAN BROWN: All right, we haven't
9 gotten to the member list yet, on the team, so, I'd like
10 to go through the boiler plate.

11 MEMBER STETKAR: I couldn't see where else
12 to --

13 CHAIRMAN BROWN: No, that's fine. I mean,
14 it's a good -- it's a question that I think was on
15 everybody's mind, because we've dealt with this before.

16 No, we're not going to talk about this
17 anymore, Dan. Go ahead, I'm sorry.

18 MR. SANTOS: I just want to offer to the
19 Committee, as they think about this issue in the broader
20 context and for the -- for whatever deliberations.

21 We did hear on the DSRS, which is a pilot
22 initiative for the EMPOWER, in that we are writing a new
23 section on basically, quality Section 7.2, that
24 basically takes a look at this issue, and tries in a pilot
25 manner, just for the EMPOWER, take a crack at those

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 systems that are important to safety, that are not safety
2 related.

3 So, we could talk separate from this, in the
4 context of that pilot, that could help shape the future.
5 So, that's all.

6 CHAIRMAN BROWN: Okay.

7 MEMBER BLEY: I'm sorry, Charlie.

8 CHAIRMAN BROWN: No, go ahead.

9 MEMBER BLEY: Where we've had some of these
10 issues, I don't remember our discussions. Did the --
11 what did the applicants do?

12 MR. SANTOS: Similar to the existing
13 reactors, no different than the framework Steve was --

14 MEMBER BLEY: Well, for these things like
15 the diesels, did they apply these --

16 MR. SANTOS: No.

17 MEMBER BLEY: -- these controls to their
18 software development?

19 MR. SANTOS: In some cases, where the
20 applicant made that decision, yes, but that's --

21 MEMBER BLEY: But not all?

22 MR. SANTOS: Not all.

23 MEMBER BLEY: Both things were there?

24 MR. SANTOS: That's right.

25 MEMBER BLEY: Okay, that's all.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Okay, Karl?

2 MR. STURZEBECKER: Okay, all right. So --

3 CHAIRMAN BROWN: We can read this. Do you
4 want to go to the next slide --

5 MR. STURZEBECKER: Yes.

6 CHAIRMAN BROWN: -- and introduce your team
7 members, or do you want us to read this, too?

8 MR. STURZEBECKER: You can just read
9 through them. Some of them --

10 CHAIRMAN BROWN: I don't want to shortcut
11 anybody, but --

12 MR. STURZEBECKER: But that is the team
13 members.

14 We broke into sub-teams and divided up the
15 guides that way, and then we have a process for -- a
16 stakeholder review process. We keep like a
17 configuration management, with all comments, and for
18 each section.

19 So, everyone can see what is going on, and
20 that is how we came to a consensus on this.

21 The learning experience from different
22 organizations like Martha Wetherholt from NASA, they use
23 IEEE for their engineering standards.

24 We talked to like Jennifer Bayuk at MITRE,
25 for some of the security items that we're going to talk

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 about today.

2 Dan Derrico, who is a railroad software
3 engineer, and what they have to deal with, for just unit
4 test and testing. He's a test engineer for the programs
5 they run there.

6 So, it's some very good input that we've
7 been taking, as we went through the guides.

8 So, here is the matrix, and this is how I
9 keep the organization straight of what is going on.

10 You can see, we've got the previous, we have
11 interim and the updated, and there are some future
12 guidance we have here.

13 The interim, where sometimes, just the --
14 like the previous, or they really set the format for the
15 next version, but we've gone through every particular
16 guide -- or standard here, just to see where the trends
17 were and where things were going.

18 Okay, so, I'm going to stop here for a
19 second.

20 This next section is to lay out how I'm going
21 to demonstrate the color coding and some of the blocks,
22 diagrams that I have here, just to keep track of the
23 different items that have either moved or they're brand
24 new.

25 What you have in red, if you see the section

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 in red, can be a -- some kind of activity or a clause.

2 Yellow shows what I've deleted and I'm going
3 to have highlighted written on that side, what that is,
4 and on the left, you see the IEEE standard. That is just
5 -- I think that is -- the first one -- the next one we're
6 going to go on to, 1.173.

7 But this is just an example here, and I have
8 the Regulatory Guide, Part A, B, C, D and the references.

9 So, overall the Regulatory Guide endorses
10 the standard and this is particular -- how we're going
11 to -- how it's laid out for these type -- these Reg
12 Guides, the -- either the -- they endorse without saying
13 an exception, or they'll have some sort of variation,
14 where we show an exception or an addition to what the
15 standard said.

16 On the far right there, you see the software
17 project life cycle process.

18 CHAIRMAN BROWN: Now, Part C, you mean
19 where you establish your regulatory positions or
20 whatever, part of the Reg Guide?

21 MR. STURZEBECKER: Part C, yes.

22 CHAIRMAN BROWN: Okay.

23 MR. STURZEBECKER: I'm not going to cover
24 A and B today.

25 CHAIRMAN BROWN: But it's -- it was -- that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 is a good idea.

2 MR. STURZEBECKER: Yes, it --

3 CHAIRMAN BROWN: It's really sort of
4 boilerplate.

5 MR. STURZEBECKER: It's all boilerplate.
6 It should be --

7 MEMBER STETKAR: Except for that one
8 footnote.

9 CHAIRMAN BROWN: Except for the -- exactly.

10 MR. STURZEBECKER: Right.

11 CHAIRMAN BROWN: I knew you'd read the
12 footnote. No, I'm just kidding.

13 MR. STURZEBECKER: Yes.

14 CHAIRMAN BROWN: Okay, go ahead.

15 MR. STURZEBECKER: Okay, so, Reg Guide
16 1.173, this is the centerpiece of the guides.

17 So, it follows as 1074-2006 directly. It
18 provides a set of directions for building a life -- a
19 software project life cycle process, and this is pretty
20 much -- well, it's part of the new section in 1074, the
21 steps I'm going to go through here are in Clause 3 and
22 4, and it would be -- it would be the direction that the
23 project or the architect would do, to hold this project
24 together.

25 The first step here we have is the -- they're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 going to have to establish the requirements and look to
2 Reg Guide 1.72 and associated 830.

3 MEMBER STETKAR: Karl?

4 MR. STURZEBECKER: Yes.

5 MEMBER STETKAR: I'm going to have to
6 interrupt you because I need to ask you about Section
7 B on this.

8 MR. STURZEBECKER: Section B?

9 MEMBER STETKAR: Because you're not going
10 to get into it.

11 There -- and it's only in this Reg Guide.
12 So, I wanted to bring it up here, and I'll apologize
13 beforehand, because you'll recognize why I apologize.

14 In Section B under the 'description' of the
15 change, in 1.173 in particular, there is a statement that
16 says, "Regulatory Guide 1.152 provides specific
17 guidance concerning the establishment of SDOE secure
18 development and operational environment."

19 "It should be noted that any material
20 submitted in support of cyber-security will not be
21 reviewed as part of the SDOE review."

22 This is the only Reg Guide that makes that
23 statement, that specifically -- we have a long history
24 of the ACRS kind of disagreeing with that process.

25 MR. STURZEBECKER: I understand.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: I just wanted to bring
2 that to your attention, and it's the only one of -- it's
3 the only one of the set.

4 All of the others refer to Reg Guide 1.152
5 and the secure development and operational environment,
6 as being controlled under the Reg Guide --

7 MR. STURZEBECKER: Yes.

8 MEMBER STETKAR: -- and we've had
9 discussions about that Reg Guide separately.

10 But this one is the only one that still
11 specifically says, "We're not going to review
12 cyber-security as part of that process."

13 MR. STURZEBECKER: And it --

14 MEMBER STETKAR: You may want to rethink
15 that.

16 MR. STURZEBECKER: And the team decided
17 that that was the place to put that statement.

18 I think -- and also, 1.173 is the only guide
19 that has it, has in it in Part C, where it does reference
20 cyber-security 5.71.

21 MEMBER STETKAR: It does, and I was going
22 to ask you about that, when we get to --

23 MR. STURZEBECKER: Well, we thought it was
24 --

25 MEMBER STETKAR: -- Section C, because in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Section C, it's kind of --

2 MR. STURZEBECKER: Okay, we have --

3 MEMBER STETKAR: -- different because it
4 says, "It's important to treat cyber-security as part
5 of the development process."

6 MR. STURZEBECKER: It is important. It is
7 important because, you know, I was part of the --

8 CHAIRMAN BROWN: We're going to do it
9 later.

10 MEMBER STETKAR: Okay, we'll do it -- we'll
11 talk about C later then, because Charlie has --

12 CHAIRMAN BROWN: No, no, I just had similar
13 observation, but I guess I would -- since John brought
14 it up, I'll ask to try to get a separation or a thought
15 process on the cyber part real quick, before you move
16 on.

17 SDOE as opposed to -- is an environment. I
18 mean, I'm still trying to wrap my hands around SDOE,
19 which is kind of this amorphous mush-ball, where
20 everybody is suppose to put up a cone around everything,
21 so that nothing un-torrid or nasty happens.

22 But it doesn't really tell you how to do it
23 very well.

24 But there is two pieces to the software.
25 One is the environment under which you develop your

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 software, how it's controlled, how it's managed, who
2 gets access, the types of code you use, etcetera,
3 etcetera. There is a whole mish-mash of stuff.

4 The other aspect of this, which is not
5 addressed, I didn't see anything explicit, and if you
6 do -- did explicitly put that in somewhere, I'd like you
7 to tell me.

8 MR. STURZEBECKER: Okay.

9 CHAIRMAN BROWN: Is that if some of these
10 folks, in trying to come -- take your kind of, we're not
11 going to look at it, but if you happen to do something,
12 well, we're still not going to look at it, because you
13 do talk about cyber -- the security of this stuff,
14 security, integrity or whatever, is if you have embedded
15 protections or code, which helps determine whether
16 somebody is trying to do something nice.

17 In other words, kind of a small firewall
18 within the code, which says, "Hold it, you can't go do
19 this or you can't go do that," that -- you don't -- you
20 know --

21 MR. STURZEBECKER: No.

22 CHAIRMAN BROWN: In other words, code --
23 this is my personal opinion, so, don't take this.

24 Code ought to do what it's suppose to do,
25 and not, in the specific code for performing a control

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 function or a protection function or a monitoring
2 function or an alarm function or anything like that, none
3 of that application code should have algorithms or
4 anything which would divert the attention from the main
5 line application code, from accomplishing a job.

6 Nothing is said about doing that, and how
7 -- whether it's relevant or whether it's covered
8 somewhere else, but I just --

9 MR. STURZEBECKER: I can explain what we
10 were thinking on this.

11 There is actually three levels, three
12 different areas.

13 When I went through the standard, I
14 categorized in three different types of security.
15 There is the SDOE look at things. There is the 5.71,
16 and then there is what you're mentioning, is the code,
17 the actual code and can you put an IDS type system in
18 there, or something that monitors it.

19 After discussions with MITRE and Jennifer
20 Bayuk, it's at least five, maybe 10 years down the line,
21 that that kind of code can even exist in the software
22 that we're doing here, from what MITRE is saying.

23 I mean, Apple and Microsoft are slowly
24 moving this way to create -- you know, the common
25 weakness enumeration is what they call it, or you know

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 what code sequences you don't want to use.

2 But then I would say if you step back, I
3 would say, even if you did not use that particular
4 sequence of code, the top 25 on the SANS list or not --
5 don't use this line of code in C or whatever, it's going
6 to only have an effectiveness date. It's only effective
7 at that point.

8 So, when they build this, it's effective at
9 that point. How often are they going to do updates and
10 do release management on that software?

11 It's not like the software that goes on with
12 the industry -- with Wall Street, where they're changing
13 it constantly. They don't have firewalls. That is
14 game changing technology.

15 We're in a trusted space area, where we try
16 to keep the jelly donut, the jelly is the software and
17 it's protected by the outside. Even 5.71 has an SDOE
18 type approach, in a way.

19 I mean, do you understand what I was -- I
20 mean, I was trying to explain --

21 CHAIRMAN BROWN: Well, yes, that's at a
22 different level than what I'm talking about.

23 MR. STURZEBECKER: Okay.

24 CHAIRMAN BROWN: I mean, your code, your
25 operating system, your application code are all buried

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 in a read-only -- in a read-only prong of some sort.

2 MR. STURZEBECKER: Okay.

3 CHAIRMAN BROWN: Electrically erasable,
4 whatever kind of prong it is, okay, and we need to change
5 that, if you can change it without just replacing the
6 chip.

7 You should be able to go in and change it.
8 There shouldn't be code embedded within the code that
9 says, "Hold it, if you don't have three passwords and
10 you cross your fingers twice," --

11 MR. STURZEBECKER: Absolutely.

12 CHAIRMAN BROWN: -- and everything else,
13 you can't get into it.

14 But once somebody clamps on with a device
15 that can go across the prong and have access to the --
16 the double E ports, or open it up, so that you can get
17 -- there shouldn't be codes within the code that says,
18 "Oh, hold it, you haven't, you know, whistled three times
19 and walked through it."

20 That is access -- that is a control of access
21 from the external part. You shouldn't complicate the
22 code with trying to protect itself, other than by the
23 physical access or control of access we have.

24 You know, somebody getting into the
25 cabinet, they ought to be able to change the code. I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 mean, I, you know, may not like that, but I mean, that
2 is because this other kind of code can -- does nothing
3 but disrupt to the main process.

4 So, we're talking a little bit of different
5 things, relative to this other type of stuff.

6 MR. STURZEBECKER: Right.

7 CHAIRMAN BROWN: I just --

8 MR. STURZEBECKER: But it --

9 CHAIRMAN BROWN: All I'm trying to do here
10 -- you can go on, I'm just trying to get to the point,
11 that there is two separate issues of this -- that there
12 is -- the issues here, in terms of what we're looking
13 at --

14 MR. STURZEBECKER: Okay.

15 CHAIRMAN BROWN: -- and at least, some of
16 what we're thinking about.

17 MR. STURZEBECKER: Well, the framework
18 that I explained was how we approached this and we --
19 we address it from 5.71's perspective in saying, "Okay,
20 you need to think about this, because you're eventually
21 going to need it."

22 CHAIRMAN BROWN: Okay, let me get to the
23 point, John's point. Where does it say that?

24 "Will not be reviewed. Cyber -- all
25 efforts of cyber will not be reviewed."

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I think we disagreed with that back when we
2 did 1.152. It should be reviewed -- you should be
3 looking for where people have done things that would
4 complicate or impact the potential safety operation of
5 a code. We had this in old -- as an oral discussion
6 in the previous meeting.

7 I don't remember anything specifically,
8 other than there was one sentence, if I remember, in
9 1.152, that says, "You'll look at it for some safety
10 related impact," but that was -- somebody is going to
11 miss that line simply, because there is no other emphasis
12 anywhere.

13 So, that -- I just -- this is so explicit,
14 it says, "You're not going to look at anything," I just
15 don't think that is a good idea to be that explicit,
16 because you do have to look at it from the impact of
17 somebody doing something that may impact the actual
18 application, and that is my only point.

19 DR. ARNDT: Yes, Charlie, I think you're
20 correct. We'll look at that particular phrasing.

21 The reference you're referring to in 1.152
22 is a statement that basically says, "To the extent the
23 staff will review features is limited to ensuring that
24 these features do not adversely affect or degrade the
25 system's reliability or its capability of performing

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 safety functions."

2 CHAIRMAN BROWN: Doesn't say that here.

3 DR. ARNDT: I understand that. That is
4 what it says in 1.152.

5 CHAIRMAN BROWN: Okay.

6 DR. ARNDT: And we'll look at exactly how
7 we map that, but the --

8 CHAIRMAN BROWN: Well, I just don't like
9 the reference to it. It's just easily lost, because
10 this is the project management, as it --

11 DR. ARNDT: Understand. We'll take this
12 --

13 CHAIRMAN BROWN: And you reference 1.152
14 in the -- I know that it's in this one, I presume it is
15 in this one.

16 MEMBER STETKAR: It's in all of --

17 CHAIRMAN BROWN: I thought it was in all of
18 them, yes, but that's just the -- I mean, when you've
19 got to search for -- to get that point, that's all.

20 MR. THORP: Yes, I think there is room for
21 us to examine this -- this is John Thorp, with respect
22 to ensuring consistency with the 1.152 statements, that
23 indicate that we absolutely do need to look at this, with
24 respect to its impact on safety. So, I think that is
25 something that we can examine.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: Okay.

2 MR. THORP: And address.

3 CHAIRMAN BROWN: Thank you.

4 MR. STURZEBECKER: I'll make a note of
5 that.

6 MEMBER STETKAR: I think it's also
7 important, and I know Charlie wanted to defer this
8 discussion, but kind of in the context --

9 CHAIRMAN BROWN: Well, I'm finished now.

10 MEMBER STETKAR: -- of what we're just
11 dealing -- there is -- there are statements later in the
12 regulatory positions, that emphasize the need to include
13 explicitly, include cyber-security as part of the
14 development process.

15 So, the implication there -- I mean, it is
16 -- there is quite a discussion. It says, "NRC takes
17 exception to the IEEE Standard 1074-2006's directions
18 for appropriate security assurance level in Section
19 A.1.1.5," and it goes on.

20 I agree with that, because those statements
21 in the IEEE standard could be misinterpreted.

22 But the regulatory position goes onto say,
23 "The planning activity is necessary and the applicant
24 or licensee should refer to the following primary
25 security objectives."

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 "One, secure software development
2 environment, and two, cyber-security."

3 I mean, you know, in this Regulatory Guide,
4 in the regulatory positions, you, not IEEE, you raise
5 cyber-security to that level of kind of review
6 attention.

7 MR. STURZEBECKER: Of some -- yes, and --

8 MEMBER STETKAR: To some extent, anyway.

9 MR. STURZEBECKER: Well, the rule says one
10 thing and then what we're trying to say is, okay, we
11 understand that the rule divides it up, but we still
12 think it's important.

13 MEMBER STETKAR: Yes, yes.

14 DR. ARNDT: And it's in the context of the
15 statement in 1.152.

16 When you're doing software development, you
17 have to understand all the requirements. You have to
18 understand all the specifications. You have to have a
19 process.

20 But the safety review will look at it, with
21 respect to the safety aspect. Those requirements have
22 to be there, but we're looking at it in that particular
23 context.

24 MEMBER STETKAR: Okay.

25 CHAIRMAN BROWN: Let's see if we can keep

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 moving here.

2 MEMBER STETKAR: Okay.

3 CHAIRMAN BROWN: 1.173 is suppose to be
4 done in a few minutes.

5 MR. STURZEBECHER: All right, well, so, I
6 was at the first step of establishing the requirements.

7 The project architect would look at Reg
8 Guide 1.172 and the associated 830 Standard.

9 The next step would be to collect a model,
10 and it depends on the industry you're in, because that
11 is the way the -- you know, the standard is written for
12 an overarching type community here.

13 It does say -- they did take, from the
14 original 1074, and moved that section out, down into an
15 Annex D.

16 So, it's kind of de-emphasized that a little
17 bit, and we'll get into that a little bit further, when
18 I start talking about the standard itself.

19 Then we go into developing the software
20 project life cycle, which I've got the classic life cycle
21 sitting there, that is from 1.152.

22 After you establish this, you begin to
23 tailor and manage your different activities that you
24 have in the Annex A of 1074, and you put this into the
25 framework of this process. You build your project from

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 there.

2 At the end, you validate and make sure this
3 plan is ready and it meets the scope of the stakeholders.

4 It's just -- okay, so, the general overview
5 of changes.

6 So, what changed from the last version?

7 Well, the Reg Guide itself, there were only
8 four minor changes. The biggest significance is in the
9 standard itself.

10 The life cycle model, still the same when
11 you look at the Standard 1074.

12 The standard -- or the standard changes
13 terminology.

14 Some of the -- when you go through and you
15 step through it, you'll see that it moved from group --
16 or from processes to activities. So, now, it lists a
17 group of activities inside that standard, because there
18 was too much confusion.

19 If you're trying to build a process, but
20 then you're calling all these sub-things processes, it
21 just -- you could see the confusion there.

22 There is -- there was a de-emphasis on the
23 project management from the original one, to the new one.
24 It added planning, but it used its own -- it re-shuffled
25 the different planning activities from the life cycles,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 from the original one to a new section.

2 So, and it also kind of dropped this project
3 management down a little bit, but you're thinking of
4 planning, and it also -- and the standard, when we get
5 to that point.

6 It removed the quality assurance section
7 clause and the V&V clause. So, those two major clauses
8 that were, I wouldn't say necessarily removed, but they
9 were moved into other activities that are in the life
10 cycle of this new standard.

11 I think what was interesting about this is
12 the -- by doing this, the standard is sort of taking more
13 of a lightening bug approach versus the strike of
14 lightening, and that is kind of the way I see the
15 philosophy going on here.

16 So, when you're developing and you're going
17 through your process of creating your software, your
18 plan, you can do peer-to-peer reviews. You can -- you
19 don't have to bring in the full V&V at that particular
20 level.

21 So, it's kind of a better -- much more
22 improved, refined process of the standard.

23 So, next slide. So, like I was saying, the
24 Reg Guide changed in four basic areas.

25 The first one is a comment from the public,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 where we have reference for pre-existing software, we've
2 referenced EPRI topical report, the guidelines on the
3 evaluation, acceptance of commercial grades, digital
4 equipment for nuclear safety applicants.

5 The public comment was that we needed to
6 show that we endorsed this. So, that was added.

7 We've added a new -- the new term 'security
8 analysis', and we've just discussed that.

9 So, it's in the Reg Guide, and the other
10 thing that the team wanted to add was the system
11 transitions, and the reason why here was because it --
12 there was this general consensus that the new digital
13 systems that are being considered, you know, if they're
14 revising them, you know, if they're outside the 50.59
15 process, then there really needs to be a license
16 amendment request required, and I think the team members
17 wanted to put a little emphasis on that. So, that's why
18 we added that particular new position.

19 Then last was the Annex, and that is more
20 of a boilerplate.

21 So, what changed in the standard itself?
22 It's major re-shuffling of activities and -- that -- into
23 the Annex of the standard.

24 There is the new clauses one through four,
25 and we kind of stepped through one through -- or three

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 through four, on just establishing your process.

2 The model, like I said, was moved to Annex
3 D.

4 Process now is replaced with that -- with
5 activities, and I mentioned before, there is a different
6 emphasis on quality management and one of the sections
7 was called an intrical processes -- processes, and it
8 was -- that is where the V&V section was removed, in that
9 part of the standard, and that one has a new name, which
10 it's -- it supports section activities groups.

11 So, in general, we're focusing on more of
12 the planning activities, with a -- building this
13 process.

14 We've got a new security objective in there.
15 There is a new section that -- the standard added the
16 planned release management and a close-out activity.
17 Those are all in the project management.

18 So, when you look at the mapping of that
19 standard, it starts with the PM section, the
20 pre-development section and implementation, and a
21 post-development, and each section had a couple new
22 activities added to it, and you can see them listed
23 there, if you have any questions.

24 CHAIRMAN BROWN: I have one question,
25 relative to the quality management part, because you've

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 mentioned it twice now, in that -- and I went back and
2 looked again at the Reg Guide. I didn't go back as far
3 as 1074.

4 But you said there was a different emphasis
5 and it de-emphasized V&V, and you said that either two
6 or three times now.

7 MR. STURZEBECKER: Right.

8 CHAIRMAN BROWN: Am I missing something,
9 that V&V --

10 MR. STURZEBECKER: Well, it's not --

11 CHAIRMAN BROWN: -- now, has less
12 importance than it used to, as part of the overall
13 project management? I mean, the project management is
14 not suppose to be interested in this?

15 MR. STURZEBECKER: I think you have to look
16 at the standards as a family, in the sense that here is
17 1074, and those 1012's there. It's been going hardcore,
18 saying -- rewriting this whole section in there about
19 V&V, and they realize, well, the folks in 1012 are --

20 CHAIRMAN BROWN: So, you're just a
21 reference -- I don't disagree with --

22 MR. STURZEBECKER: Yes.

23 CHAIRMAN BROWN: -- that repetition, but
24 the -- I guess I was having a little bit of a hard spot
25 with saying it de-emphasizes V&V, and I would have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 phrased that somewhat differently --

2 MR. STURZEBECKER: Well --

3 CHAIRMAN BROWN: -- in that the quality
4 management is there, it's just that it -- it's the --
5 its details are covered somewhere else, but it's still
6 part of the overall project plan.

7 MR. STURZEBECKER: But the 1995 version is
8 pretty heavy. I mean, it has it in there, just like --

9 CHAIRMAN BROWN: Well, I don't -- I didn't
10 have a copy of that.

11 MR. STURZEBECKER: Yes.

12 CHAIRMAN BROWN: So, I had no idea what was
13 in there.

14 MR. STURZEBECKER: Yes, it is pretty heavy,
15 and I mean, even the quality -- I mean, I can pull it
16 out if you --

17 CHAIRMAN BROWN: No, no, no.

18 MR. STURZEBECKER: That is the -- the whole
19 section is four pages --

20 CHAIRMAN BROWN: All you're saying is the
21 -- it was simply a de-emphasis relative.

22 It wasn't in terms of the quality management
23 needed. It was a manage of -- matter of the detail
24 included in the overall project plan, when there is a
25 more detailed explanation and details to that, in one

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 of the other standards, it's invoked by one of the other
2 Reg Guides? Is that --

3 MR. STURZEBECKER: Well, that is --

4 CHAIRMAN BROWN: Is that -- did I phrase
5 that properly?

6 MR. STURZEBECKER: Yes, what it -- I think
7 maybe the answer would be to say that what it's doing
8 is, it's say, okay, there is a V&V process, as the --
9 the team is working on this product, and coming up with
10 a plan, and they go through the life cycle.

11 Then they get to the maintenance section and
12 they've gone through the full cycle and they look at it,
13 there are -- there is new activities where they look at
14 process improvement, and it's a peer-to-peer type, or
15 you can go to the full level of the V&V if you want. It
16 does say -- I think it says that, and this is similar
17 to what NASA has done with their's also, their standard.

18 So, or their engineering document. So,
19 they're following this verbatim. It is sort of a softer
20 approach, is what I'm trying to say.

21 You're still going to do V&V at one
22 particular point. It's just that there are --

23 CHAIRMAN BROWN: Okay, I just --

24 MR. STURZEBECKER: Yes.

25 CHAIRMAN BROWN: That's fine. You can go

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 on. I just --

2 MR. STURZEBECKER: That's why I'm saying
3 it's de-emphasized, but --

4 CHAIRMAN BROWN: All right, all right, I
5 got --

6 MR. STURZEBECKER: Maybe I used the wrong
7 word.

8 CHAIRMAN BROWN: I've got the point. You
9 can keep rolling, all right.

10 MR. STURZEBECKER: I'm sorry, I got that.

11 It's just a -- a change in the philosophy,
12 and I think they're more -- they're trying to refine this
13 to be more process oriented, is what I'm trying to say.

14 CHAIRMAN BROWN: Okay, I got that.

15 MR. STURZEBECKER: So, here is the figure,
16 and like we were saying, here is -- there was a whole
17 section V&V processes. It's pretty much deleted.

18 You'll find that though, in this part here,
19 in if you watch my pointer here, in identifying software
20 improvements needed. So, this is where it mentions that
21 aspect.

22 So, you're still -- it's still there, but
23 it's -- this is really focused on building a process,
24 and then the quality software -- software quality
25 management process, which references QA, and again, that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 was -- okay, let me think.

2 Am I pointing to the wrong one? Yes, I was,
3 sorry.

4 The V&V moved to A.5, that Annex there. The
5 quality management software, that is now represented in
6 this whole process of improvement, and it's mentioned
7 there for improving the quality of your software.

8 This is going to be a theme that you'll see
9 in the 829, for Reg Guide 1.170, when we talk about
10 developing your documentation.

11 Again, you come up with anomalies or a bug
12 in the software, and it gives a new section in there on
13 how you handle the discrepancies in the software.

14 So, they're kind of parallel in action
15 between this standard and that standard, and they move
16 together. So, it's really well done, I think.

17 Is there any particular comments on this?

18 CONSULTANT HECHT: I am not sure, Karl,
19 whether I should bring this up now or later, but we've
20 spoken about security. You've spoken about commercial
21 software, you've spoken about the EPRI commercial
22 dedication report.

23 The problem, when we deal with the whole
24 issue of cyber-security, is that it's constantly
25 evolving threat and constantly evolving software, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 a lot of that is handled in the commercial, or I'll call
2 it externally developed software.

3 Do you feel that that is addressed in this
4 Reg Guide, and where is it exactly addressed?

5 CHAIRMAN BROWN: In the commercial
6 dedication or --

7 CONSULTANT HECHT: Well, yes, commercial
8 dedication --

9 CHAIRMAN BROWN: I thought they were kind
10 of downplayed commercial dedication all the way through
11 here, if I'm not mistaken.

12 CONSULTANT HECHT: Well, whether you call
13 it commercial dedication or you call it something else,
14 the point is, is that systems are today, an integration
15 of a platform, which is developed -- which is supplied
16 by the PLC vendor or the control systems vendor.

17 Then the system developer, which adds its
18 own application software, and then all that is, of
19 course, integrated into the plan.

20 But the point is, is that the security
21 adaptations are going to be done probably by the
22 equipment vendor, somebody like Rockwell or Siemens or
23 something -- or equivalent organization. They're not
24 going to be done by the licensee. They're probably not
25 going to be done by the licensee's I&C vendor, unless

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 that I&C vendor is the same as -- is the Siemens or the
2 Rockwell.

3 CHAIRMAN BROWN: So, you're talking about
4 the operating system for the platform?

5 CONSULTANT HECHT: Well, the platform.
6 It's not only the operating system. It's the network
7 stack. It could be the whole access control system. It
8 could be the maintenance --

9 CHAIRMAN BROWN: Well, you're talking --
10 yes, you're just talking about operating system, the
11 housekeeping stuff, all the other stuff that goes along
12 with --

13 CONSULTANT HECHT: Right.

14 CHAIRMAN BROWN: -- making stuff move,
15 while the application code --

16 CONSULTANT HECHT: Right.

17 CHAIRMAN BROWN: -- operates.

18 CONSULTANT HECHT: And that is basically
19 where a lot of the security is going to be implemented
20 and a lot of the changes are going to be implemented.

21 At the same time, we have this overall
22 development process.

23 So, we have parts that are moving, parts
24 that are fixed, parts that the NRC has visibility into,
25 and parts of it doesn't, and how is that addressed in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the Reg Guide, or do you --

2 MR. STURZEBECKER: Well, in this
3 particular Reg Guide, when we look at what is going on
4 in the standard, I have to look at it specifically.

5 MR. THORP: I don't know if this helps, but
6 when -- one of the paragraphs that I've been looking at,
7 as I listen to the members here, under 'description of
8 change', the third paragraph in the 1.173, speaks to the
9 cyber-security controls and requirements, and it
10 relates it to the 10 CFR 73.54 and protection of digital
11 computer communication systems and networks, as part of
12 the programming.

13 So, that paragraph speaks to that in
14 general. I don't know, it certainly doesn't go into the
15 details related to the vendor implemented security fixes
16 and things like that. Let me show it to you.

17 MR. STURZEBECKER: Yes.

18 CHAIRMAN BROWN: Well, let me just -- I
19 guess I hadn't -- I'm not sure I thought about this.

20 73.54 is nothing but a plan. It really is
21 --

22 MR. STURZEBECKER: Yes.

23 CHAIRMAN BROWN: -- I think it really does
24 nothing, other than say, you got to have a plan, which
25 is done after this stuff is designed. That is one of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the difficulties with it.

2 I guess what Myron is saying is, at least
3 -- and I hadn't really thought about it from that
4 standpoint, from the platform standpoint, that the
5 licensee develops the application code, or whoever he
6 hires to do this, do his design.

7 The designer pulls a platform out, whether
8 it's a Common Q or whether it's a Triconex or whether
9 it's a -- who is the other one? I don't know, there is
10 three or four platforms.

11 MR. THORP: ALS.

12 CHAIRMAN BROWN: Okay, what is one of the
13 other ones we're dealing with? What is the APW? Our
14 platform? I've forgotten what that one is.

15 MR. THORP: OIQ?

16 CHAIRMAN BROWN: I just looked at it.

17 MEMBER BLEY: It's MilTech.

18 CHAIRMAN BROWN: MilTech, right, okay.
19 Those are -- you know, somebody develops that and then
20 the designer comes and puts his code into it, and I think
21 Myron's point is that there is a whole swath of code
22 that's already in there, when he gets it, that manages
23 the entire platform.

24 There will be secure -- based on his
25 knowledge and his application of that platform and other

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 applications, and I'll get -- let you to talk here in
2 a minute, that will have stuff that you guys never see,
3 I mean, and the licensee never sees, unless he wants to
4 go see it, and I'm not even sure he'll get -- it's
5 probably proprietary, more than likely.

6 So, that is -- I mean, so, there is a
7 separation between that, in my mind. I think that is
8 what you're a little -- a little bit about what you're
9 talking about, and there is a bunch of security stuff
10 possibly buried in there.

11 CONSULTANT HECHT: Well, we know it will be
12 changed and I guess the point is, is that as part of the
13 project life cycle management, and how are we addressing
14 that?

15 CHAIRMAN BROWN: Yes, okay, let me -- and
16 I'm -- now, that just sparked another thought, and maybe
17 you can address this.

18 Right now, you have your PC and you're
19 operating at home, and you've got an operating system
20 and you've got some type of security stuff, code that's
21 stuck in there, and it's always downloading all these
22 updates all the time.

23 When you install this stuff in a plant, it's
24 fixed with what you want to put -- you know, what you've
25 brought in.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 The guy who is designing that platform, if
2 you look at what he does three years from now, he may
3 have updates to that. You probably don't care.

4 CONSULTANT HECHT: Five-point-seven-one
5 requires that you --

6 CHAIRMAN BROWN: You keep -- you look at
7 that, exactly.

8 So, that is a -- that has always been a
9 concern to me, how you get -- did you want to say
10 something?

11 MR. STATTEL: Yes, I would like to say a few
12 words on this.

13 My name is Rich Stattel, and I perform
14 technical reviews on these very systems, and this is an
15 issue we deal with on a regular basis.

16 I'd like to point out that these Reg Guides
17 and -- which we get to these Reg Guides, basically
18 through our Standard Review Plans.

19 Our Standard Review Plan is what we refer
20 to, whenever we get an application for a license
21 amendment or a new system being installed in a plant.

22 It's equally applicable for operating
23 systems, for application development.

24 So, in my experience, we see these when we
25 get topical reports or platforms, like you mentioned,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Common Q platforms or TXS platform, and in those arenas,
2 you know, we're looking at the vendors on how they
3 applied the life cycles, or if they have dedicated
4 software that they have embedded within their platforms,
5 we evaluate those processes as well.

6 So, basically, these standards and the Reg
7 Guides are equally applicable to the development of the
8 platforms, as they are to the development of the
9 application itself.

10 So, it's all within scope, and we deal with
11 that on many aspects, when we review a systems design.

12 CONSULTANT HECHT: Okay, so,
13 you've said how the NRC handles it. But this is a Reg
14 Guide that talks about software life cycle management.

15 MR. STATTEL: Right.

16 CONSULTANT HECHT: And so, this is a Reg
17 Guide for how the applicant or how the licensee is
18 suppose to be doing it, and the point is, is that this
19 is what I would call a waterfall type of approach here.

20 MR. STATTEL: It is -- that is one option.
21 This isn't prescriptive guidance. It's not telling --
22 telling an applicant --

23 CONSULTANT HECHT: It's the prescriptive

24 --

25 MR. STATTEL: -- this is how -- no, it's not

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 prescriptive.

2 CONSULTANT HECHT: Yes, it --

3 MR. STATTEL: It allows various life
4 cycles, and we see many.

5 CONSULTANT HECHT: Sure, but I guess the
6 question is, if you're -- if the NRC is providing
7 guidance, there is suppose to be an economic value to
8 the guidance, in terms of reducing the uncertainty.

9 So, here is an area, I think of uncertainty,
10 and how is it going to be addressed in --

11 MR. STURZEBECKER: But that is the classic
12 argument I've heard at MITRE, where, you know, they would
13 come in -- or manufacturers would come in and say, you
14 know, "We have a time table to make."

15 You know, it's not necessarily to follow
16 what is exactly correct for the best security. I mean,
17 that is what -- the impression I got from some of those
18 conferences I've attended with the SWA Software
19 Assurance Group.

20 What we do have is Regulatory Position 3 for
21 software analysis. We do lay out, under 'activity
22 description' --

23 CONSULTANT HECHT: Can you give me a page
24 reference?

25 MR. STURZEBECKER: It's page eight,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Regulatory Position 3, Software Safety Analysis.

2 CONSULTANT HECHT: Okay.

3 MR. STURZEBECKER: And it's B, under
4 'activity description', six, seven -- or six and seven,
5 "To develop threat models for safety software products,
6 system architect -- system software architects are
7 exploring the main -- the main and potential SW -- DOE,"
8 that is the vulnerabilities and their impact.

9 CONSULTANT HECHT: Okay, so, you've got --

10 MR. STURZEBECKER: Yes.

11 CONSULTANT HECHT: -- it once.

12 MR. STURZEBECKER: What is that?

13 CONSULTANT HECHT: You've done it once.

14 MR. STURZEBECKER: Right there, yes.

15 CONSULTANT HECHT: But the problem is, it's
16 going to be changing.

17 MEMBER STETKAR: The Reg Guide says any
18 time you make a change, if it's -- you have to invoke
19 this Reg Guide.

20 MR. STURZEBECKER: Right, you have to
21 follow the whole process and the --

22 MEMBER STETKAR: Well, that is if they make
23 the change, if they're going to make the change.

24 MR. STURZEBECKER: Okay.

25 CHAIRMAN BROWN: Well, that is the -- I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 wanted to try to separate the variables here for a
2 minute. I wanted to ask Rich a question.

3 MR. STATTEL: Sure.

4 CHAIRMAN BROWN: Relative to the comment.

5 I mean, once -- since you've seen this,
6 you're talking about you've seen this on an ongoing
7 basis.

8 So, a plant is designed. It's got a
9 platform, call it a Common Q, AP1000, whoever is got
10 whatever, and it's operating.

11 You have what you have. The systems, all
12 the support stuff, not the -- I'm not talking about the
13 application code, now.

14 But the guy who owns the platform says, "I
15 have some security upgrades to my platform software."

16 MR. STATTEL: Right, and they would invoke
17 their change process, which is part of --

18 CHAIRMAN BROWN: Who does that? The
19 licensee does -- has to do that, if they decide -- what
20 if they decide -- if they don't decide to incorporate
21 the platform manufacturer's security upgrade --

22 MR. STATTEL: Yes.

23 CHAIRMAN BROWN: -- then they don't have to
24 do anything. I mean, they have to evaluate it, but they
25 don't have to --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STATTEL: Well, one of the things we
2 evaluate -- because we do a lot of process review. We
3 evaluate the process they use for updating their
4 software.

5 CHAIRMAN BROWN: No, no, I understand that,
6 but I mean if -- this is a licensee. I mean, they're
7 now -- and now, the platform Common Q guy comes in and
8 says, "Hey, I -- it's been five years. We've got seven
9 safety upgrades that we have made to this platform in
10 subsequent applications."

11 MR. STATTEL: Right.

12 CHAIRMAN BROWN: Whatever the applications
13 are, for whatever they do with them, and you really ought
14 to install these.

15 Now, does the licensee -- he doesn't have
16 to do that, does he? He can make the decision not to
17 or he can decide --

18 MR. STATTEL: Well --

19 CHAIRMAN BROWN: -- he can evaluate them
20 and see if they're applicable to his design, in which
21 case, then if he wanted to change it, then you all would
22 have to see it as -- is that in the license amendment,
23 to change --

24 MR. STATTEL: That is quite possible. It
25 basically comes -- the decision of whether or not to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 incorporate security improvements to a system, that
2 really rolls into their security plan and the
3 implementation of that. It's a programmatic issue.

4 CHAIRMAN BROWN: Okay.

5 MR. STATTEL: So, they would identify
6 vulnerabilities and this may be a means of addressing
7 a vulnerability that has been identified, and they
8 re-assess those on a periodic basis. That is my
9 understanding of most of the plans that the utilities
10 are incorporating right now.

11 When a decision is made to incorporate that,
12 to you know, address -- import or install a security
13 feature, then of course, that invokes their standard
14 update process.

15 Now, for most of the safety related systems,
16 the applicants are not doing the application development
17 or the upgrade process themselves, and they basically
18 contract that out to the vendors, to actually perform
19 those updates.

20 It could very well invoke, because our
21 safety evaluations and our safety conclusions are tied
22 to specific versions and topical reports that are
23 basically, you know, we document exactly, you know, the
24 point in time that we perform that evaluation.

25 So, if any of those safety conclusions

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 become challenged or need to be re-assessed, then it
2 could very well require a license amendment to come to
3 us.

4 MR. SANTOS: This is not --

5 MR. STATTEL: In truth, we don't see a lot
6 of those. We don't see a lot of those amendments.

7 Those platforms are actually fairly stable
8 right now, from the plants that we've -- that have the
9 installed systems.

10 So, but we have seen updates. We have seen
11 updates to platforms. We have reviewed updates to those
12 platforms, and when -- you know, like for instance, for
13 Triconex, we just reviewed their Version 10, and when
14 we review those updates, they become reference-able.

15 So, if a plant that is running a Triconex
16 Version 9 wants to upgrade and incorporate measures that
17 were put into Version 10, then we have reviewed that.
18 We've performed the safety evaluation, and that is
19 reference-able by the licensee.

20 MR. SANTOS: Yes, that is --

21 CHAIRMAN BROWN: But you really don't know
22 whether -- I mean, if you've got two different vendors
23 with somewhat different plant designs, how do you assess
24 the impact of that on the application code and its
25 processing?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 You've looked at the --

2 MR. STATTEL: We have looked at the --

3 CHAIRMAN BROWN: -- platform aspect but --

4 MR. STATTEL: We do review both. We do
5 review both.

6 CHAIRMAN BROWN: But you have to do that for
7 --

8 MR. STATTEL: Is someone comes in and they
9 say, "Well, here is our application," we look through
10 that and we see, well, what is the platform that you're
11 using to implement that application? Have we reviewed
12 that? Do we have a safety evaluation that we've
13 performed in the past, or do we need to evaluate that
14 separately?

15 So, it really is one of the things that makes
16 our safety evaluation actually, a very difficult
17 process, because we're not only reviewing, you know, one
18 life cycle that the -- that is being used for development
19 of the application.

20 There may be two, three, four different life
21 cycles being done by different vendors, for example,
22 that we have to basically, assess them, using this
23 guidance.

24 So, the guidance is equally applicable to
25 the development of the platform, as it is to the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 development of the application.

2 CHAIRMAN BROWN: And any changes to it
3 during its operation.

4 MR. STATTEL: Absolutely, absolutely.
5 So, you know --

6 CHAIRMAN BROWN: And that is within the
7 licensing basis of the -- that the licensee has to deal
8 with, relative to --

9 MR. STATTEL: Right.

10 CHAIRMAN BROWN: -- the SER that they've
11 had, that's there --

12 MR. STATTEL: And it is -- it is a, you know,
13 changing world, right.

14 So, it's very common for us to get an
15 application that references a platform that we've
16 previously reviewed, maybe a year or two years ago, but
17 there are changes, right, that have been made since we
18 evaluated that.

19 So, we basically perform a special
20 evaluation of those deltas, and if those deltas include
21 incorporation of security measures into that platform,
22 yes, we would evaluate that against this criteria, yes.

23 MR. SANTOS: I just want to add to -- this
24 is Dan Santos, NRR, to everything that Rich said, to go
25 to your original question.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 The Regulation 10 CFR 73.58 called 'Safety
2 Security Interface Requirements for Nuclear Power
3 Reactor' applies to existing and new reactors.

4 It says, "The licensee shall assess and
5 manage the potential for adverse effects on safety and
6 security, including the site emergency plan, before
7 implementing changes to plan configurations, facility
8 conditions or security."

9 Now, as part of that assessment, that --
10 some of the conclusions may trigger 50.59, which then
11 will come for the NRC evaluation.

12 But each licensee is required to do that
13 assessment. So, when a vendor comes in and say, "Hey,
14 I want this new security feature," that will trigger that
15 process.

16 CONSULTANT HECHT: Okay, so, I guess the
17 short answer is, is that a security change, not
18 withstanding the fact that that may be coming much faster
19 than a functional change or other changes, are handled
20 in exactly the same way as any other change? That is
21 basically what you're saying here?

22 MR. STATTEL: They are, but I'd also like
23 to point out that the vast majority of security features
24 that are incorporated at the plant, are to protect the
25 safety application, and they're not embedded within the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 safety application.

2 So, there are --

3 CONSULTANT HECHT: Well, that is the --

4 MR. STATTEL: -- very few security features
5 that are actually built into the safety application --

6 CHAIRMAN BROWN: Well, let's address that
7 before -- I mean, before we worry about that, I mean,
8 I still think we're talking about the other -- not the
9 application code necessarily, but the --

10 MR. STATTEL: Well, not --

11 CHAIRMAN BROWN: I mean, that counts, but
12 --

13 MR. STATTEL: But even the --

14 CHAIRMAN BROWN: I understand.

15 MR. STATTEL: Even the vendor's code --

16 CONSULTANT HECHT: Because I think the
17 whole thing that you say, you put stuff at the boundary
18 and you protect the soft jelly center, with the hard
19 shell, when we get into systems that are integrating
20 TC/PIP into the entire system, then we're in a different
21 world than when we were using Allen-Bradley Highways or
22 all of the other Field Bus standards that used to be
23 there, and we used to feel that we had protection. We
24 no longer do.

25 CHAIRMAN BROWN: Okay, I think we're done

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 with that, for right now.

2 MR. STURZEBECKER: So, I'm going to finish
3 up with the last slide, unless you want to get -- well,
4 we'll touch on this one here. Let me make sure I have
5 this.

6 So, this demonstrates some of the touch
7 points that the Reg Guide on the right, that I went
8 through, the particular items, has made variations or
9 exceptions to, and we'll start with the letters that are
10 A, B, C, D, I'll refer back to slide 13. So, if there
11 is any questions?

12 So, between the two of them, you can see,
13 this is what we've accepted, or considered, yes,
14 correct.

15 The next set of slides are the specific
16 changes, and I'm not sure you want to -- they're kind
17 of a repeat of what we've already done. It's just more
18 description of -- from title changes to the --
19 everything.

20 MEMBER STETKAR: I have a couple of
21 questions, Karl. Sorry, Charlie.

22 CHAIRMAN BROWN: No, you've got five
23 minutes.

24 MEMBER STETKAR: C.3 speaks about software
25 safety analysis, and I got confused, when I read through

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 this.

2 Are the analyses that are described there,
3 analyses of the safety functions that the software
4 performs, or are they analyses of the safety of the
5 software development process, because I can -- I thought
6 it says -- it says, "Planned and documented software
7 safety analysis activity should be conducted for each
8 phase of the software development life cycle," okay.

9 Then it has listed 'input, activity
10 description and output', and I started to read this
11 saying, "Well, this says that I'm suppose to perform some
12 sort of analysis of the safety functions that the
13 software is designed to perform.,"

14 But then there are things like in the input,
15 establish baseline SDOE objectives, and in the activity
16 description, it says there are developed threat models
17 for the safety software products, safety system software
18 architectures are explored or known, and potential SDOE
19 vulnerabilities enter impact.

20 The reason I'm interested in this, is if
21 we're talking about the function of the software to
22 perform a particular safety goal for the plant, if you're
23 talking about threats and vulnerabilities, that is kind
24 of an interesting thing.

25 If you're talking about threats and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 vulnerabilities to the process that somebody has invoked
2 for a secure development environment, making sure that,
3 you know, nobody can walk through that door who isn't
4 authorized to actually work on this software, that is
5 much different.

6 That is what I would call -- and it talks
7 about a safety officer and a software safety plan.

8 If it's the latter function, it almost is
9 a software development security analysis, rather than
10 a software safety analysis.

11 So, I was curious, what is the distinction
12 here, because I'm not sure now, in my mind, what -- what
13 the applicant is expected to do, as part of this software
14 safety analysis.

15 MR. STURZEBECKER: We did add the
16 sub-clause under secure analysis, under 1(d), and these
17 were put in under the analysis, and it possibly could
18 have just left them underneath the secure analysis
19 section instead.

20 MEMBER STETKAR: But is this -- I mean, the
21 intent is the actual systematic evaluation of the
22 development environment, not -- regardless of what the
23 software is suppose to do, is that the correct
24 interpretation?

25 MR. STURZEBECKER: For those particular

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 sub-tasks there, yes.

2 MEMBER STETKAR: Okay.

3 MR. STURZEBECKER: Because even when
4 you're doing -- you're looking at particular software,
5 or if it's a pre-existing software, you're -- you need
6 to look at the history. You need to look at certain
7 aspects of what it's done in the past, its performance.

8 You know, what product would you buy one
9 versus the other on the market?

10 CHAIRMAN BROWN: John, I guess the way I
11 read this, you know, I think I have a vague understanding
12 of what you said.

13 But when I went down and looked at -- under
14 the activity description, I -- same question.

15 Are we just saying, "Hey, they've got a
16 process that keeps all the bits and bytes going to the
17 right place," and if they find -- they actually go from
18 point A to point B and whatever, but do they really shut
19 down the plant if it wants to? Does it --

20 MR. STURZEBECKER: Well, but the --

21 CHAIRMAN BROWN: But yet, if you read the
22 activity description part it says, "Your analyses should
23 ensure that systems safety requirements have been
24 correctly addressed, no hazards have been introduced,
25 and that software elements that affect safety," in other

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 words, if they look at them, "Are identified," etcetera,
2 etcetera.

3 So, it is -- the way I read this, is that
4 it covered not just, you know, software glitches that
5 could get you into trouble, but did it really perform
6 the plant function that it was suppose to accomplish?

7 Now, maybe I was being overly generous in
8 my interpretation --

9 MR. STURZEBECKER: Okay, that is -- that's
10 what it says --

11 CHAIRMAN BROWN: That is what it says to me.
12 That is why I didn't -- I didn't --

13 MEMBER STETKAR: If that is the case,
14 you're asking somebody -- remember, not -- a threat and
15 hazard analysis doesn't just address, does it do what
16 it's suppose to do?

17 It addresses, does it not do what it's not
18 suppose to do, when it's not suppose to do it, under a
19 variety of really clever threats and hazards, and I'll
20 challenge you that I don't think anybody can do that.

21 So, if you're really intending people to do
22 that type of systematic hazard and threat analysis to
23 all of the functions that this software is suppose to
24 perform in the plant, to support plant safety, and make
25 sure that it doesn't do things that it's not suppose to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 do, it's a real challenge, and it's not clear, that
2 people know how to do that.

3 If you're only saying, "Does my software
4 development process provide assurance that
5 inappropriate activities are not performed for the
6 development of this software," regardless of what it's
7 suppose to do or not suppose to do in the plant, it could
8 be software to, you know, control a jellybean
9 manufacturing facility. That is a different -- much
10 different connotation, because I have a lot better, I
11 think concept, of what I need to do in that second
12 environment than I do in the first.

13 So, that is why I wanted to at least better
14 understand, because I got confused, and what I'm hearing
15 today is that the intent is the former, that I'm suppose
16 to evaluate threats and hazards to the mission of the
17 software itself.

18 MR. STATTEL: I won't try to interpret what
19 exactly the guidance had intended.

20 However, however, what I will say, I'll
21 point out what I see in practice, with applicants and
22 these development processes.

23 We look at V&V summary reports as one of the
24 most important documents we look at during the -- during
25 our evaluation, and in those summary reports, we look

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 -- we specifically look for identification of
2 vulnerabilities or threats to the system, and the -- in
3 each phase of the development process.

4 So, we look for a preliminary hazards
5 analysis.

6 So, you know, what were the hazards
7 identified up front? How -- you know, what measures
8 were put in place to address those hazards and security
9 vulnerabilities, and then in each phase of the process,
10 we look -- there is a separate report usually.

11 We look in that report, what new
12 vulnerabilities were introduced in the process of
13 developing the design, implementing the design of the
14 software or installing it into the hardware, you know,
15 whatever the process is.

16 Then for each one of those, what measures
17 did the vendor or did the developer take, to address
18 those vulnerabilities that were introduced during the
19 life cycle phase? That is what we typically see, and
20 that is what we look for in the applications when we
21 perform our evaluations.

22 So, typically it will be a list and it's
23 usually a short list, right.

24 So, if someone is going through a design
25 phase, and so, they -- they are basically taking the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 requirements and implementing them in a design, they'll
2 identify, you know, a couple of -- you know, where are
3 the potentials for introduction of errors into that
4 design?

5 Where are the vulnerabilities of the
6 system, and then we expect them to follow that through,
7 you know, with their corrective action program, or
8 whatever programs they have in place, in order to
9 identify what measures they've taken to address those
10 vulnerabilities.

11 It may be, you know, downstream V&V
12 activities, for example.

13 CONSULTANT HECHT: Rich, you started off by
14 saying that you -- one of the most important documents
15 you look at is the verification summary report.

16 Now, does this mean that this verification
17 summary report is actually much more than simply saying
18 the requirement to have verified, that you also include
19 the activities of the preliminary hazard assessment
20 then, that preliminary hazard assessment also includes
21 security?

22 MR. STATTEL: Typically, V&V summary
23 report will be created at the end of each phase of
24 development, right.

25 At the end of that phase, that summary

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 report will identify, it will speak to every activity
2 that was performed during that phase of the development
3 process, right.

4 So, it is a lot more than just saying, yes,
5 all the requirements have been met, and you know, we're
6 ready to proceed to the next phase.

7 It's actually listing -- identifying the
8 vulnerabilities, the errors that were detected.

9 There will usually be a section on metrics,
10 like you know, things -- problems that we had during that
11 development phase, problems that still exist and will
12 need to be addressed in the subsequent phase.

13 There is usually a risk analysis involved
14 with that V&V summary report, and a decision made to
15 proceed to the next phase, even with errors or issues
16 that need to be carried forward.

17 So, usually the V&V plan will identify what
18 the contents of that V&V report are and -- it's basically
19 -- the V&V reports tell you all of the activities, how
20 they went, and what is being done to address the issues
21 that came up during those activities.

22 CONSULTANT HECHT: And is that going to be
23 -- are we going to discuss those V&V -- the contents of
24 those reports, when we get to, I think it's 1.168?

25 MR. STATTEL: Six-eight and 1.170, and they

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 are called for, also in 1012, IEEE 1012.

2 CONSULTANT HECHT: Well, I guess that is
3 referred to, I think by 1.168, right?

4 MR. STATTEL: Right.

5 CONSULTANT HECHT: Yes.

6 MR. STATTEL: Part of that, yes.

7 CHAIRMAN BROWN: Okay.

8 MEMBER STETKAR: It's not okay. One more
9 thing.

10 Under C.4, where you talk about the
11 installation act -- system transitions or whatever you
12 call them, I just wanted to understand -- I want to make
13 sure I understand the staff's intent here.

14 There is a statement that says, "As a
15 minimum, all functions performed in part by a given
16 software executable should be declared inoperable, if
17 the software executable, its configuration or its
18 operating platform is to be altered."

19 "Inter-connections of all types, with other
20 software, hardware, human elements should also be
21 examined."

22 "All interfacing, interconnected systems
23 must also be taken out of service and declared
24 inoperable."

25 Okay, now, again, in new plants, many of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 new plants have a four-train safety system design, and
2 their technical specifications allow one train to be
3 inoperable, out of service, whatever you want to call
4 it, indefinitely, because their safety analyses say they
5 can mitigate any design basis accident with two of the
6 remaining three trains, so therefore, they can handle
7 a single failure.

8 So, in principle, during plant power
9 operation, I can take train A of everything, out of
10 service, with no un-torrid violations of technical
11 specifications.

12 In principle, I could update the software
13 for train A, at the same time.

14 Does this requirement and this connotation
15 of inter-connections of all types with other software,
16 hardware or human elements, and all interfacing
17 inter-connected systems must also be taken out of
18 service, prohibit me from updating my software during
19 plant power operation or during other -- any other plant
20 operating mode, that requires my safety systems to be
21 operable? That is just a question.

22 CHAIRMAN BROWN: Let me put it -- let me
23 give it -- let me try to take his question, if you don't
24 mind, and provide a specific example.

25 You take train A out of service, call it a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 protection train. Protection train A sends a voting
2 signal to trains B, C and D. Those are interfacing and
3 inter-connected signals.

4 MR. STATTEL: That's right.

5 CHAIRMAN BROWN: If I wrote -- if I read
6 this -- and I didn't think about this either. As usual,
7 that's John going on this.

8 MR. STATTEL: It's not your fault.

9 CHAIRMAN BROWN: That would say that I
10 would have to take train B, C and D out of service --
11 declare them inoperable because I am modifying the
12 software in train A, and it does connect to those voting
13 systems in the other trains.

14 It's very clear, all
15 interfacing/inter-connecting systems must also be taken
16 out of service and declared inoperable.

17 MEMBER STETKAR: It says,
18 "Inter-connections of all types with other software,
19 hardware," --

20 CHAIRMAN BROWN: Or human element.

21 MEMBER STETKAR: -- "or human elements."

22 CHAIRMAN BROWN: But that is the sentence
23 before what I just read.

24 So, those are pretty all-encompassing and
25 could be kind of -- I know that is not the intent.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MEMBER STETKAR: My question was, is it the
2 intent? I mean, you can read things --

3 MR. STATTEL: We obviously have systems
4 that basically allow changing configuration in one
5 division without declaring the other divisions
6 inoperable.

7 Really, the idea of that, it's really -- we
8 don't want -- we don't want licensees or plants to be
9 changing configurations on a system when -- while
10 they're relying on that system to perform the safety
11 function.

12 So, basically, we have them carve out that
13 part of the system, in order to allow the
14 configurability, right, because really, there is
15 regulatory requirements for them to be able to configure
16 those systems online.

17 So, they have to have a means of doing that.

18 Now, this is guidance, right. It also
19 comes into play, where we have systems that have channel
20 bypass capability within a division.

21 So, in other words -- and a lot of the analog
22 plants have this.

23 They have -- they're able to take presurizer
24 pressure to test, make it inoperable and they can
25 reconfigure that without affecting containment pressure

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 or the other 12 parameters that are in that same
2 division. They remain operable.

3 When we go to digital based systems, that
4 becomes a little bit more difficult to justify, because
5 you don't have that physical separation between the
6 individual channels.

7 Typically, they're all being processed by
8 a similar processor.

9 So, what we require, in the case of Ocone, we
10 require them to basically declare that entire
11 division inoperable while they are performing those
12 configuration changes, right.

13 So, if they want to do a similar thing,
14 right, if they have a failed transmitter on pressurizer
15 pressure, and they want the rest of the channels, they
16 want -- they're still -- they can still function, the
17 rest of the channels, they have the ability to take the
18 entire division out of service, go in and bypass
19 pressurizer pressure, and then subsequently, declaring
20 the remaining channels operable again.

21 So, that is how we apply that --

22 CHAIRMAN BROWN: You mean, the remaining
23 functions within that --

24 MR. STATTEL: Right.

25 CHAIRMAN BROWN: -- that division?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STATTEL: Right.

2 CHAIRMAN BROWN: Not channels, but the
3 remaining --

4 MR. STATTEL: Well, it is --

5 CHAIRMAN BROWN: -- functions?

6 MR. STATTEL: Right, it's kind of a
7 pressure --

8 CHAIRMAN BROWN: Well, the pressure,
9 temperature or flow, you might have multiple parameters
10 --

11 MR. STATTEL: That's correct.

12 CHAIRMAN BROWN: -- or you can take a
13 parameter out of service, effectively.

14 MR. STATTEL: Right.

15 CHAIRMAN BROWN: But yet, the overall
16 division can remain in service, once you've restored it,
17 after you've disconnected the one thing that --

18 MR. STATTEL: That is correct.

19 CHAIRMAN BROWN: -- is not functioning, and
20 utilize the other functions.

21 MR. STATTEL: Right.

22 CHAIRMAN BROWN: And there is --

23 MR. STATTEL: Now, in the case of Oconee,
24 and I don't want to get into specifics, however, I think
25 it's important to note, they didn't have provisions in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 there, when they specified their system, they didn't
2 include provisions for bypassing individual functions,
3 right.

4 But in other applications, we're seeing
5 where they're specifying that up front in the design.

6 So, basically, they're retaining the
7 ability to bypass individual functions within a channel,
8 and it's specified in the design.

9 So, they're building that into their
10 design, as they go. So, they're retaining those channel
11 -- or function bypass capabilities that they had in their
12 -- in their analog systems, for example.

13 We evaluate those very carefully because
14 basically, they're establishing kind of a virtual
15 separation between the functions that are -- remain
16 operable and the ones that they're able to go in and
17 configure.

18 CHAIRMAN BROWN: Well, I didn't -- my
19 example was --

20 MR. STATTEL: So, we do a very careful of
21 whether they are --

22 CHAIRMAN BROWN: I understand that, but I
23 mean, John's point is valid, when it says --

24 MR. STATTEL: Well, I think that is more of
25 a literal interpretation.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Well, let me give you an
2 example.

3 MR. STATTEL: It is guidance, though. We
4 basically -- it causes us to consider --

5 CHAIRMAN BROWN: Well, this was the one
6 thing --

7 MR. STATTEL: -- when we're configuring --

8 CHAIRMAN BROWN: Hold it. This is the one
9 place, as opposed to putting the weasel word 'should'
10 in, you've got the word 'must'.

11 MR. STATTEL: Right.

12 CHAIRMAN BROWN: And if your processor that
13 is doing your calculations for reactor trip is feeding
14 system -- you know, all of the other divisions, and you
15 need to change that -- so, are you ready for five -- to
16 perform a software upgrade on it, you read this, and --

17 MEMBER BLEY: And five years from now, when
18 you guys are doing something else and somebody new is
19 reading this guidance, it seems pretty clear.

20 MEMBER STETKAR: You can -- I can come down
21 on either side of this, and let me give you an example.

22 Charlie has it exactly right. I have four
23 trains, and I have software that lives in each of those
24 four trains. Nominally, it's identical software, it
25 does the same functions.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I want to update my software. Suddenly,
2 something has happened and I got smart, and I used to
3 have a function that says, "If A and B occur simultaneous
4 -- in coincidence, then do 'x'," and I discovered
5 something that says, "Oh, I need to modify that, that
6 says now, if A and either B or C occur, then do 'x'."

7 So, I change my software coding, and I do
8 that. I take train A out of service. I re-code train
9 A. I put it back in service and now, I have different
10 software logic residing in each of my trains.

11 MR. STATTEL: Right, and --

12 MEMBER STETKAR: For some period of time,
13 because I can't do this simultaneously, I do it in real
14 calendar time, and because I'm taking the whole darn
15 train out of service, I'm going to do it according to
16 my rules and according to the staff's rules, and
17 according to the technical specifications, and as long
18 as I can do that, I'll do it over a long period of time.

19 MR. STATTEL: That is very --

20 MEMBER STETKAR: Now --

21 MR. STATTEL: That is a very interesting
22 example, because we did get into these discussions with
23 a couple of applicants, and in the end, basically,
24 software upgrades being performed on safety systems,
25 particularly protection systems online, become very

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 complicated for the very reasons you're talking about.

2 When we started with Ocone, we started
3 walking through those very scenarios, "Well, what if I
4 want to upgrade the software on division A," and so, I
5 take it out of service, I update it, and now, I want to
6 go to division B.

7 Now, I'm in kind of a weird configuration
8 here, because I've got one channel, you know.
9 Obviously, I'm going to go through all of these --

10 CHAIRMAN BROWN: He's changed the -- who
11 has changed the --

12 MR. STATTEL: It's a logical function.

13 CHAIRMAN BROWN: -- as opposed to some
14 other --

15 MR. STATTEL: In conclusion --

16 MEMBER STETKAR: Our's could do that.

17 MR. STATTEL: Our conclusion, however, was
18 basically that they would not be able to upgrade or
19 change software configurations, while the plant is
20 online, and that was the final result, because they were
21 not able to answer those questions, of how to address
22 all of the --

23 MEMBER STETKAR: Well, they -- now, in the
24 15 minutes, we've come back to, it's the staff's intent
25 that I cannot make software changes online.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STATTEL: Now, set point changes are
2 different --

3 MEMBER STETKAR: I didn't talk -- I didn't
4 say set point changes, did I?

5 MR. STATTEL: Right, okay.

6 MEMBER STETKAR: I said at a minimum, all
7 functions performed in part, by a given software
8 executable --

9 MR. STATTEL: That's right.

10 MEMBER STETKAR: So, we're talking about
11 software here. We're not talking about a pressure
12 transmitter. We're not talking about other things.
13 We're talking about software here.

14 If it's the staff's intent, according to
15 this regulatory guidance, that you shall not, because
16 this says 'must be declared inoperable', you shall not
17 change safety system software during -- and I don't want
18 to call it, during plant power operation, because there
19 are many safety functions now, that are required, while
20 a plant is in shut down modes.

21 MR. STATTEL: That's right.

22 MEMBER STETKAR: So, if it's the intent
23 that you shall not change any safety system software
24 during any plant operating mode for which that software
25 function is required, that seems to be different with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the intent of many of the technical specifications that
2 don't explicitly say anything about changing software.

3 The technical specifications, as I read
4 them, would allow me to do exactly what I said. I could
5 change that logic to read, as long as I have evaluated
6 that new logic, if A and either B or C perform 'x'.

7 MR. SANTOS: And are you --

8 MEMBER STETKAR: And I could do it
9 sequentially over a period of time, and I'm not violating
10 any technical specifications.

11 MR. SANTOS: Okay, this is Dan Santos. But
12 in addition to the tech spec, you also need to make sure
13 you're not violating none of the other regulations at
14 any time.

15 And if your logic change will drive you to
16 potential violation of independence requirements of an
17 adverse impact to the overall safety function, then that
18 will drive you to the decision not to do it online,
19 because you will be violating another regulatory
20 requirement.

21 MR. STATTEL: Well, and also, the problem
22 comes in when -- so, when you go into Alpha, you make
23 your software change, and when you -- where you run into
24 problems is, now, I want to declare Alpha operable and
25 I have Bravo, Charlie and Delta that are operating with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 different software versions. Have you analyzed that
2 condition?

3 MR. SANTOS: Right.

4 MR. STATTEL: You know, and then when you
5 do Bravo, now, you have two with one software, two with
6 the other software, and they would have to do that, in
7 order to declare those -- in order to get Alpha back in
8 service, in order to declare those functions operable,
9 in order to continue operations, right.

10 Now, the other thing I'll point out is the
11 regulation applies not only to protection systems and
12 protection functions, but it applies to, for instance,
13 PAMS systems, right, where you can have the channel --
14 like, you have a channel inoperable, load new software
15 in, put that channel operable, and then go -- then go
16 to the other channel, right.

17 It's actually possible to perform software
18 upgrades on systems that are not protection functions.

19 But what we have found in our experience,
20 and even -- we're having these same discussions with
21 Diablo Canyon right now.

22 Our experience is that for protection
23 systems that are performing two of four protection
24 functions, it's not possible to load software into those
25 divisions with the plant online, in order to continue

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 to meet regulatory requirements, because essentially,
2 you end up with all four other channels inoperable.
3 It's just not feasible.

4 MEMBER STETKAR: Okay, I'll -- I hear you
5 saying that.

6 I'll take a piece of hardware though, this
7 piece of hardware, and I have four of these pieces of
8 hardware, and I decide to put -- let's call this piece
9 of hardware a diesel generator.

10 I'll decide to put a new cooler in this
11 diesel generator, an upgraded cooler. It cools better,
12 and I've got my other three diesel generators that have
13 the old coolers, that didn't cool quite as good, but they
14 work perfectly fine.

15 They're accepted. They were licensed.
16 They cooled good enough. This one just cools a little
17 better.

18 You allow me to do that, and yet now, I have
19 a plant that has four different diesel generators --

20 MR. STATTEL: The difference is, that
21 cooler isn't crossing over to the other diesel
22 generators and --

23 MR. THORP: That's right, and the other
24 piece of it is --

25 MEMBER STETKAR: I'm not talking to your

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 systems.

2 MR. THORP: Post-modification, you're able
3 to test that cooler, prior to declaring that system
4 operable again.

5 MR. STATTEL: Right.

6 MR. THORP: And so, you assure yourself,
7 before you even declare it operable, that that cooler
8 is tight, sealed, functional, carries out the functions
9 that it's suppose to and now, it's operable again, now,
10 you take the next channel out.

11 So, it's a difficult sort of -- it's not all
12 apples to apples comparison there, in terms of the
13 software.

14 MEMBER BLEY: I kind of think they meant
15 what they said, although it took them a while to get
16 there.

17 You left out one of the little phrases
18 before all the stuff that you've been quoting, John,
19 which was, determination of effective functions can
20 depend on extremely subtle considerations with software
21 and --

22 MEMBER STETKAR: That's true.

23 MEMBER BLEY: -- and that seems to be the
24 -- what your example has, all of the sudden it just --

25 MR. STATTEL: Right, and actually --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: It's just too complicated to
2 say all the --

3 MR. STATTEL: -- we'll rule it out. When
4 we were evaluating Ocone, we didn't want to rule out
5 the possibility of upgrading a software, you know, to
6 a different version.

7 But when we started walking through the
8 scenario and having them explain to us, how you would
9 maintain operability through -- to these various
10 iterations, it got very complicated, especially when you
11 get into upgrading the software on the voter.

12 Now, obviously, the voter is receiving
13 input from all four channels.

14 So, it got complicated to the point where
15 they just kind of threw up their hands and they said,
16 "Yes, we're not going to upgrade software while the plant
17 is online." It's never going to happen.

18 MEMBER BLEY: Now, back to where we
19 started.

20 MR. STATTEL: And they put that --

21 MEMBER BLEY: This is the --

22 MR. STATTEL: They have that restriction in
23 place, and that is actually also articulated in the
24 safety evaluation that we wrote.

25 MEMBER BLEY: Even though these words are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 in the guidance, if they decide there is a good way to
2 do it, they can come in and --

3 MR. STATTEL: I don't know what it would be.

4 Actually, in Diablo Canyon, for example,
5 they've been operating with a digital system since 1993,
6 and we've had those discussions with them, and
7 basically, they're saying, "Yes, we would never upgrade
8 software without the plant being offline."

9 CHAIRMAN BROWN: Well, it's not only just
10 the voting unit.

11 I mean, the calculation unit, once you put
12 it back in service, you have to verify that it is actually
13 sending its signals to the other three divisions. That
14 requires some other divisions to be in some type of a
15 test mode, where you can confirm that that new software
16 in the division you've already modified is now
17 performing, before you've even performed it on the other
18 channels.

19 MR. STATTEL: It's almost like you have to
20 do a whole series of operability determinations as you
21 roll in the new software versions, and it's actually very
22 prohibitive.

23 CHAIRMAN BROWN: All right, we're going to
24 have to move on here.

25 MEMBER BLEY: Are you ever going to have a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 break?

2 CHAIRMAN BROWN: Yes, that's what -- no,
3 we're going to -- we're going to not have a quorum here.

4 So, even though we're not finished with
5 1.173, I am going to declare a 15 minute break, and we'll
6 come back, and try to finish this.

7 Karl, I would ask you, as we move through
8 these next pages, there is really kind of just -- I don't
9 --

10 MR. STURZEBECKER: It's a repeat.

11 CHAIRMAN BROWN: We ought to try to go
12 through those quickly, because they're kind of saying
13 what was changed, but we don't --

14 MR. STURZEBECKER: Well, it's specific.

15 We went through the highlights ahead of
16 time. This is specifics. So, if you want to touch base
17 on this, we can skip through the next four slides, go
18 right to the conclusions.

19 CHAIRMAN BROWN: We'll talk about that when
20 we get back.

21 Right now, we'll take a recess for 15
22 minutes and be back at 10:45 a.m.

23 (Whereupon, the above-entitled matter went
24 off the record at approximately 10:30 a.m. and resumed
25 at approximately 10:50 a.m.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: Okay, the meeting will
2 come back into order. Karl, proceed.

3 MR. STURZEBECKER: Okay, so, the next
4 several slides here are the specific changes. It's kind
5 of a recap of what we've done.

6 This adds title changes and more specifics
7 that I've had to go through.

8 If anyone has any questions on any of them,
9 we can go through that, or I can just kind of move to
10 the end. Particular area.

11 CHAIRMAN BROWN: I don't have any. I'd
12 actually -- I actually read those. So, unless you --
13 are you all okay to go to the next slide? I'm ready,
14 John, unless you got some other questions.

15 We've already discussed a couple of these,
16 anyway.

17 MR. STURZEBECKER: We can go to the next
18 slide, if you want.

19 CHAIRMAN BROWN: Okay, next.

20 MR. STURZEBECKER: All right, so,
21 finishing 1.173, we'll move to Reg Guide 1.172, and that
22 is the software requirements specifications.

23 So, this guide focuses on helping the
24 architect create those functions accurately and without
25 constraints by incorrect words or misinterpreted words.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 That's one of the big things that came out in the changes,
2 that we noticed.

3 It also brings in the whole idea of
4 traceability and the baseline for future development,
5 and we touched upon that, when we were looking at that
6 part, and it reports the -- obviously, the software
7 project life cycle process.

8 There were many changes to the Reg Guide,
9 and it follows the standard, and the next slide.

10 So, the Reg Guide itself -- the Reg Guide
11 itself incorporates a new topic -- well, it's a new topic
12 to the Reg Guide, if I recall, and it's been in the
13 standard for a while, I think.

14 The team wanted to bring more emphasis on
15 the whole unambiguity, sorry, easy for me to say. So,
16 that section was added.

17 There was a public comment when we first
18 wrote it. They did not like the description, so, we
19 rewrote it to make --

20 CHAIRMAN BROWN: The description of
21 unambiguity?

22 MR. STURZEBECKER: As in the standard -- or
23 the Reg Guide.

24 CHAIRMAN BROWN: Okay.

25 MR. STURZEBECKER: So, the way that it was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 written was confusing. It -- we had to -- I think it
2 was the second sentence that was --

3 CHAIRMAN BROWN: You mean, where it says,
4 "Software requirements are generally derived," is that
5 the second sentence you're talking?

6 MR. STURZEBECKER: Yes, "Software are
7 generally derived with associated products, such as
8 safety system requirements, a combination of the SRS and
9 as such, associated documents should be unambiguous."

10 I can't -- I'd have to look and pull out what
11 that sentence was originally, but there was a complaint
12 about that. So, we rewrote that.

13 We also added security analysis --

14 CHAIRMAN BROWN: All these -- excuse me.
15 You changed the second sentence?

16 MR. STURZEBECKER: I think it was the
17 second sentence.

18 CHAIRMAN BROWN: Okay, I didn't see what it
19 read before.

20 MR. STURZEBECKER: We had -- there was
21 version that went out --

22 CHAIRMAN BROWN: I mean, I've forgotten
23 what it read. I'm just trying to make sure I understand,
24 just the one point.

25 MR. STURZEBECKER: Okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: But the IEEE standard says
2 one thing, but you added --

3 MR. STURZEBECKER: Right.

4 CHAIRMAN BROWN: -- you kind of clarified
5 that, you know, other derived products and documents
6 also have to be unambiguous, if you're going to utilize
7 -- I mean, that is the flavor I got out of this.

8 MR. STURZEBECKER: Right, because --

9 CHAIRMAN BROWN: I mean, I went and looked
10 at all the unambiguity stuff, and was suitably ambiguous
11 in my understanding.

12 So, we don't have to go with -- I had one
13 question on this, relative to software requirement
14 specifications.

15 MR. STURZEBECKER: Okay.

16 CHAIRMAN BROWN: I understand -- I mean,
17 I've read what's in here, but in none of these documents,
18 and this is the closest I've come to this question, when
19 I -- in my prior incarnation, when I talk about software
20 requirements, it didn't just talk about the type of stuff
21 you talk about here, consistency and all these other type
22 things that you run through.

23 But it also had specific requirements, in
24 terms of how code was actually programmed. In other
25 words, we told people things they could and could not

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 do.

2 MR. STURZEBECKER: Right.

3 CHAIRMAN BROWN: For instance, we would
4 tell them that they couldn't use global variables,
5 because global variables introduce complexity into the
6 overall application code, and they can create problems.

7 If you're using -- and I don't know what the
8 programming language of the day is, but in the days when
9 I was doing it, it ranged from C to C++, and it had such
10 functions as friends, it had inheritants, it had
11 multiple inheritants, and all of these functional -- I
12 think it's object oriented code or something, I mean,
13 they had classes and all this other nifty stuff in there.

14 And I'm not a programmer, but I had my guys
15 who knew how to do that, show me all the difficulties
16 and how inheritants, friends and multiple inheritants
17 could create problems within your code, in terms of how
18 it's applied. So, we just prohibited it.

19 MR. STURZEBECKER: Right.

20 CHAIRMAN BROWN: So, I said -- it was easier
21 for me. We earned it. We told people what to do.

22 Here, I mean, in these fancy languages, the
23 really high level languages have oodles of flexibility
24 and they're trying to allow all types of things to be
25 done.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 And yet, there is actually no addressing of
2 languages or how people actually program or functions
3 that you do or don't want to do in any of these documents.

4 Is that --

5 MR. STURZEBECKER: Okay.

6 CHAIRMAN BROWN: Has there ever been any
7 thought given to that? I know Rich is -- always wants
8 to talk about this, but go ahead, Karl, you start.

9 MR. STURZEBECKER: I'll start off. I
10 think we really hit that in unit tests, the Reg Guide
11 on unit tests.

12 We're looking at it from a perspective that
13 they've got to go through and do the adequate testing,
14 and how they're going through it and preparing their
15 process and creating -- and making sure that the software
16 does what it's suppose to do.

17 There is a lot of resistance that we had to
18 -- with several public -- well, one public comment
19 definitely, that came back and said, "Well, if all this
20 function block programming, why is the NRC pointing to
21 unit tests," and you're using 20-year old or -- type
22 thinking, and the answer is, it's still done today.

23 Dan Derrico uses it for the railroad. In
24 fact, if requirements come in with the software or they
25 don't come in with the software, he rejects it right

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 away. There is -- and that is the safety systems on a
2 train.

3 So, when you're saying that we're not
4 specifying a particular set of rules, that is true, we're
5 not. But we're requiring them to at least do the due
6 diligence down to unit tests, component and then system,
7 and then having that kind of --

8 CHAIRMAN BROWN: But that's like the black
9 box approach. I mean, you're fundamentally saying,
10 "I've got," --

11 MR. STURZEBECKER: No.

12 CHAIRMAN BROWN: Well, I mean, that is
13 almost what it sounds like, and because you're talking
14 about inputs and outputs.

15 But you're not worried about how they're
16 mixing the ingredients inside, as long as the cake comes
17 out with the right consistency, and that assumes that
18 you can define every possible -- possible function or
19 input or output that -- or data bit and byte, or some
20 code that gets mixed around, that could actually create
21 problems.

22 MR. STURZEBECKER: I disagree because I
23 think it's white box testing, when you go to a unit test
24 type perspective.

25 CHAIRMAN BROWN: But I don't understand the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 term white box. I understand black box, but not --

2 MR. STURZEBECKER: These are going to force
3 people to go through this whole breakdown, and it's in
4 -- I can't remember where it is, that has the actual
5 definitions of what they call -- the standard calls white
6 box versus black box.

7 But the idea is, if you start 100 or less
8 than 100 lines of code, as the unit, you check that out,
9 before you bring in the next unit, and now before you
10 connect them up or go to a component level, the branch
11 testing goes from there, that there is really -- there
12 is this interactive testing at test points and -- on how
13 the software behaves, before it goes into a full system,
14 and then you can say, "Well, input process, output black
15 box."

16 CONSULTANT HECHT: Can I offer some --

17 MR. STURZEBECKER: Sure.

18 CONSULTANT HECHT: -- clarity -- some --
19 well, other --

20 CHAIRMAN BROWN: Clarity?

21 CONSULTANT HECHT: I didn't want to use
22 that term.

23 But the kind of requirements that you are
24 talking about, Charlie, I've seen in software
25 development specifications. I've seen them in coding

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 guidelines, and they are the 'how', and they are very
2 important.

3 But I think that those are separate from the
4 functional requirements, and can I also say --

5 CHAIRMAN BROWN: I agree with that.

6 MR. STURZEBECHER: Okay.

7 CONSULTANT HECHT: But I sensed, or my
8 reading of the software requirements here was that it
9 was functionally oriented and independent from the
10 coding guidelines and the coding restrictions, which
11 should also be reviewed.

12 The question about unit test and white box
13 versus black box testing, I would call white box testing
14 structural testing, and that is certainly not feasible
15 to do above the unit level.

16 I would also suggest, however, that you
17 could very well have global variables or multiple
18 inheritants, and still pass your structural test, and
19 still end up with problems during operation.

20 CHAIRMAN BROWN: That is true.

21 CONSULTANT HECHT: So, we need both -- we
22 need coding guidelines. We need good functional
23 requirements. We need to do functional testing. We
24 need to do structural testing, but those are all
25 separate.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 MEMBER BLEY: So, where are the coding
2 guidelines?

3 MEMBER STETKAR: Well, then you have to go
4 to --

5 MR. STATTEL: I'd like to be able to take
6 that. This is Rick Stattel again.

7 In practice, what we see -- you are correct,
8 in that our guidance does not specify the 'how'. It
9 doesn't specify --

10 CHAIRMAN BROWN: Using the word 'coding
11 guidelines'. Is that -- does that the correct --

12 MR. STATTEL: Right, however, what I have
13 seen invariably, each vendor will identify the
14 weaknesses or the coding standards that are not
15 preferred, for example, and they will produce documents,
16 and in the case of Westinghouse, they produced a code
17 restrictions document, which I reviewed, and basically,
18 that established exactly what you are saying.

19 It's basically -- it tells the programmers,
20 even though the software is capable of doing these types
21 of functions, using certain types of interrupts, for
22 example, they prohibit that in the development of safety
23 related code, and I've seen that in several vendors.

24 So, they come to that conclusion and we do
25 see that -- we do see those restrictions in place, in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 practice.

2 MEMBER BLEY: I guess I'm curious, though
3 from the staff's viewpoint.

4 Those are the things that allow us to meet
5 these higher level programmatic goals that we see in
6 these documents, and without those being specified, it's
7 not been clear to me, how we know we meet these higher
8 level goals, and I --

9 MR. STATTEL: Well, here is what I'll say
10 to that.

11 MEMBER BLEY: -- wonder what you guys have
12 done about that, and why you don't think it's necessary
13 to have something like coding guidelines.

14 MR. STATTEL: Okay, where is why I don't --
15 I feel that it's appropriate the way it is, is because
16 basically, we received a lot of applications using a lot
17 of different types of codes, and we are not the experts
18 in those codes.

19 So, it's really not appropriate for us to
20 be dictating to the developers, these methods are
21 acceptable, these are not acceptable. We don't know the
22 existing --

23 MEMBER BLEY: I think that's probably true,
24 but --

25 MR. STATTEL: -- methods, until after the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 fact --

2 MEMBER BLEY: -- there are some kind of
3 general principles, like the ones Charlie had mentioned,
4 that have been identified, starting in the 1960's and
5 forward, that have led to much better executable's than
6 we had before. Steven looks like he's ready to jump on
7 this.

8 DR. ARNDT: Well, and that's really the
9 point.

10 We articulate in our requirements and
11 guidance, what needs to be done, what we're going to
12 review, what criteria we have, and we go out of our way,
13 particularly in this area, to not do that 'how'.

14 One, as Rich mentions, we don't want to
15 restrain the licensees. We don't want to design the
16 systems for them. We want to look at what they did, and
17 the coding guidelines or prohibitions or whatever, to
18 determine that they have done what they said they were
19 going to do.

20 The other thing is, the systems and the
21 learning that's going on in the industry is continuous,
22 particularly in this area.

23 The second we put out a guidance that says,
24 "We don't want you to do 'x'," someone is going to come
25 up with something that is either different from that,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 or entirely making it non-applicable, like complex logic
2 devices and things like that.

3 So, if we stay at the 'what needs to be
4 done', and what is the acceptance criteria associated
5 with it, then we can evaluate, as Rich and the other
6 reviewers do, how they have accomplished it, without us
7 dictating what they need to accomplish and the 'how' kind
8 of way.

9 So, that is a philosophy we used, and it's
10 been fairly effective.

11 MEMBER BLEY: The reason I'm just sitting
12 here for a second, and as long as we have the level of
13 expertise that we have, to be able to make sure what they
14 provide meets the kind of goals we have in this guidance,
15 I think we're good.

16 I'm wondering if -- and you come up with
17 this, not just in software, but everywhere, how much we
18 need in the SRP world, to make sure folks in the future
19 are looking at the things that you just talked about.

20 DR. ARNDT: Well, and that is really one of
21 the keys, because the SRP doesn't stand alone.

22 It points to the regulatory guidance, but
23 it also points to best practices documents that our
24 Office of Research had put out, it also points to our
25 training program, which is a big ongoing challenge,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 operating experience and a lot of other areas that tries
2 to get at that specific issue that you're talking about.

3 MR. STATTEL: And what Steve said is
4 consistent with the documents that I review. They are
5 up to date. We do look for them.

6 Our review process gets us to the point
7 where we want to know what the restrictions are, with
8 regard to how you develop the code.

9 So, we always, in ever case, I'm not exactly
10 sure how we get to that point, but in every case, we get
11 to the point where we see what the capabilities of the
12 systems are, and we want to review -- we want to evaluate,
13 well, how are you going to restrict those capabilities
14 to the point where we have assurance that this code is
15 deterministic and it meets our regulatory requirements.

16 The consistency has to do with, these
17 documents are usually based on experience, where they've
18 had errors in codes, and often times, those documents
19 will describe the experience, "Here is why we don't want
20 to use these types of interrupts. Here is why," and
21 typically, what we see is, it ties back to some error
22 that was introduced into some code that's at a plant or
23 something like that.

24 Now, we don't have access to that, as the
25 experience is being had.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So, we want to have -- we want to allow the
2 vendors to have that flexibility, to be able to develop
3 these code restrictions or methods documents, let's call
4 them, so that they can continually improve their
5 process.

6 If we were to do it, it would just be too
7 far behind the eight-ball, I would think.

8 CHAIRMAN BROWN: Is there anything in this
9 process that requires line-by-line commenting of the
10 code, that these --

11 MR. STATTEL: Actually, it doesn't --

12 CHAIRMAN BROWN: Such as why that line is
13 --

14 MR. STATTEL: It is not that prescriptive.

15 However, there are requirements for
16 documentation of code, and for example, in cases where
17 the -- it's not the traditional code, where you have
18 comment lines that go right along with the lines of code.

19 Typically, we'll see a function block
20 diagram code, and our regulation -- or our Reg Guide will
21 tell us, "Make sure that they've documented, in a
22 narrative way, exactly how that code functions."

23 Well, there is no lines of code to look at.
24 There is no comment lines to look at.

25 So, what we ask for is, we look for, "Well,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 what is the equivalent of that," and typically in
2 software, that resides in a document that is typically
3 called a software design description, right.

4 It basically provides that narrative and it
5 explains, and different vendors do it different ways.

6 Some vendors have tools where they have
7 basically text boxes that go like, right next to the
8 function block, and it describes why it was there, what
9 its purpose is, how it fits with the overall function
10 of the system.

11 In other cases, it's just a narrative that
12 -- so, they provide a function block diagram and then
13 there is a narrative that goes with that, that basically
14 provides a description of how that function block works.

15 We do look for that. That is -- I believe
16 that is part of our configuration management evaluation
17 -- process evaluation. So, I believe that is addressed.

18 MEMBER BLEY: But comments, that external
19 comments go along with the code, I think would be part
20 of configuration management --

21 MR. STATTEL: It is.

22 MEMBER BLEY: -- but I think internal
23 comments would be probably within the coding standard,
24 wouldn't it?

25 MR. STATTEL: It could be, yes, and it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 varies from one -- it varies from vendor to vendor, but
2 the typical place I look for that is in the software
3 design description documents. Those are very detailed
4 documents, detailed design documents.

5 MR. STURZEBECKER: But you're suppose to be
6 following Reg Guide 1.170 --

7 CONSULTANT HECHT: Right, which is not a
8 requirements document.

9 MR. STATTEL: Now, we also might see -- you
10 know, going back to the topic at hand here.

11 We might see in a software requirements
12 specification, a requirement to provide those
13 descriptions or comments on the code, when it is
14 developed, because typically, the SRS is a pre-cursor
15 to the software design description.

16 CONSULTANT HECHT: Shouldn't that be -- is
17 there a software development plan, which is separate
18 from the SRS?

19 MR. STATTEL: Yes, yes, that's true, yes.

20 CONSULTANT HECHT: That may be more
21 appropriate. Well, okay.

22 CHAIRMAN BROWN: Okay, you're just --

23 MR. STURZEBECKER: But to answer your
24 question, we don't have specific --

25 CHAIRMAN BROWN: I've got that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Yes.

2 CHAIRMAN BROWN: I got that.

3 MR. STURZEBECKER: We have a NUREG --

4 CHAIRMAN BROWN: Very clear.

5 MR. STURZEBECKER: Yes, we have NUREG's
6 that do have those list of rules, which we've kind of
7 compared that to what other industries have done, like
8 NASA or JPL, Olsen's Power 10, I think I told you that.

9 CHAIRMAN BROWN: Oh, no, I understand your
10 difficulties, because you don't control what language,
11 what operate -- you know, how they're going to -- how
12 they're going to -- the platforms are going be set up
13 by any particular vendor, and I have the advantage of
14 telling the vendors, what language they would use, and
15 then we gave them rules they could or could not do. So,
16 it made it very, very easy.

17 MR. STURZEBECKER: Yes.

18 CHAIRMAN BROWN: No, not easy. That's the
19 wrong word. It made it controlled, and so, that we knew
20 what the product was -- I fixed my word there, Steve,
21 you don't have to shake your head too much.

22 MR. STATTEL: Well, in the process of
23 coming to our safety conclusions, we want the same level
24 of assurance, right.

25 CHAIRMAN BROWN: Well, no, but that's --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STATTEL: That is what drives us to look
2 for those documents and look to see that the vendor has
3 developed those documents and does have a method.

4 CHAIRMAN BROWN: But Rich, your point, and
5 I understand, this is a conclusion I've been drawing now,
6 for the last four years, is that this -- these are
7 processes that you have in place.

8 They end up with reports and/or
9 documentation that says, "We did this. We defined a set
10 of things we wanted to happen. We did the test. We got
11 the things we said we wanted to happen, but they're
12 process documents."

13 You don't have the resources to go and try
14 to nickel and dime every piece.

15 MR. STATTEL: Right.

16 CHAIRMAN BROWN: And you've probably heard
17 me say this before, this is why I get wrapped around the
18 axle, in terms of saying there has got to be something
19 in the architecture that protects you from the unknown
20 errors in the software, that tells the system to shut
21 down, and that is why you need an independent hardware
22 watchdog in each division, that actuate its trips and/or
23 safeguards alarms, that are independent of all the
24 software in that train, cannot utilize exception
25 handler's or other type stuff that -- or BASP's, whatever

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 they're called, and some other -- one of the other
2 projects, to end up initiating a trip.

3 That is all executed, assuming even though
4 the processor does not trigger the watchdog, it -- the
5 watchdog is now using, assuming that there is still some
6 functions available to create this trip, and that's a
7 problem, and that is why you tend to hear me say, "I need
8 an architecture configuration," that allows you to know
9 that, hey, we're going to do the best we can, as we
10 develop the software. We can't go look and control
11 every line of code.

12 But what we can do is build an architecture
13 that protects us from having that problem occur, and that
14 is -- and this will get -- that is why looking at these
15 six Reg Guides has been useful for trying to understand
16 your processes, and what you all do, and it's just --
17 you're just kind of cementing some of my other hardcore,
18 concrete thought processes, that I annoy everyone with.

19 CONSULTANT HECHT: But that should come
20 about through a system level requirement.

21 In other words --

22 CHAIRMAN BROWN: Yes, no, I --

23 CONSULTANT HECHT: -- there should be a
24 system level requirement that says you have that
25 diversity, you have that analog back.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. THORP: I'm hearing tons of D3. It's
2 just something that is --

3 CHAIRMAN BROWN: Well, the watchdog timer
4 is different than D3, okay. I mean, that is within the
5 architecture itself.

6 D3 is a separate non-software based
7 function, and if you look at the D3 systems, it normally
8 does not perform all the automatic functions that the
9 automatic system does.

10 So, and those -- you go through an analysis
11 that says, hey, we can depend on some guy taking 45
12 minutes to run out to the plant and turn a valve -- I'm
13 being -- I'm exaggerating slightly here.

14 But that is the point. They are not -- the
15 diverse systems that you put in are not complete
16 replications of what the -- and that is fine. I don't
17 have a problem with that, as long as we have an
18 architecture that protects us.

19 MR. STATTEL: Right, and the difficulty we
20 have is the variety of applications and designs that we
21 see.

22 CHAIRMAN BROWN: I understand that.

23 MR. STATTEL: But we're really trying to
24 come up with guidance and regulation that fits all of
25 them, and you know, you could -- I hear a lot of, "Oh,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 well, the requirement for providing commenting should
2 be at the system level or should be at the software
3 level."

4 It varies. I can point to three different
5 vendors and have those very requirements in three
6 different places, three different levels in the document
7 hierarchy.

8 So, we're trying to cover a lot of ground.

9 CHAIRMAN BROWN: Okay, I just wanted you to
10 understand my thought processes a little bit here, and
11 this is -- like I say, this has been useful to get a better
12 grasp on what we've been doing.

13 MR. STATTEL: It would be nice if we had the
14 luxury of just restricting this to two, you know,
15 specific vendors or one vendor, and that would --

16 CHAIRMAN BROWN: Well, I never did that.

17 MR. STATTEL: -- and you could be a lot more
18 restrictive than that, in that.

19 CHAIRMAN BROWN: Okay, all right, we can go
20 ahead and go ahead and roll.

21 MEMBER STETKAR: Can I ask something that
22 is somewhat related, but it's a little bit different
23 level.

24 There are -- there's discussion in here
25 about verify-ability and robustness, and the statement

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 about verify-ability, it's C2, basically says Subclause
2 4.3.6 of the IEEE standard, "Recommends the removal or
3 revision of unverifiable requirements," and according
4 to the IEEE standard, it says, "A requirement is
5 verifiable if and only if there exists some finite cost
6 effective process, with which a person or machine can
7 check that the software produce meets the requirement."

8 In the NRC statement it says, "The NRC
9 believes that all requirements should be verifiable and
10 should be modified or restated as necessary, to allow
11 for the verification of each one."

12 So, if I state a requirement, it should be
13 verifiable. If I can't verify it, does that mean I don't
14 state it as a requirement?

15 I'll put the converse in place. This is
16 important to me, because we're going to get -- I'm trying
17 to -- I'm very interested in what this says something
18 should do versus what this doesn't say something
19 shouldn't do.

20 Now, if I go down, let me finish the thought.

21 If I go down to robustness, there is a long
22 statement that says, "The licensee or applicant should
23 specify the software requirements for fault tolerance
24 and failure modes derived either from a consideration
25 of system level hazards analysis or from software

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 internals for each operating mode."

2 "The licensee or applicant should fully
3 specify software behavior in the presence of unexpected
4 and correct anomalous and improper in part -- input
5 hardware behavior or software behavior, and should
6 provide software requirements necessary to respond to
7 both hardware and software failures, including the
8 requirements for analysis of and recovery from computer
9 software -- system failures."

10 Now, for years, the ACRS has been after NRC
11 Research to define software failure modes. NRC
12 Research has not been able to do that for years.

13 I'm really interested in that, because if
14 we could define software failure modes, we might be able
15 to start modeling software and understand how one
16 evaluates the reliability of software and its
17 vulnerabilities to a lot of things that people haven't
18 yet thought about, until they happen, and then they think
19 about them.

20 But this statement in C6 says, "I, as a
21 licensee or applicant, have to do that." I have to
22 identify the software failure modes. I have to look --
23 and I have to specify requirements for software behavior
24 against all possible combinations of anomalous input
25 conditions, including behavior of the software itself.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 So, if I, as the licensee have to do that,
2 there must be some way of doing that, and I'm really
3 interested to see how people do that, because I haven't
4 seen anybody who can do that.

5 Now, if I am a licensee and I say, "Well,
6 I can't verify any of that because it's not a closed
7 solution," so, I can't state that as a requirement,
8 because I can't verify it. So, I can't do this.

9 How do you resolve this? In my mind, it's
10 -- you're asking somebody to do something that nobody
11 knows how to do, and you're asking them to specify it
12 as a requirement, which by definition, must be
13 verifiable, which means there has to be some way of
14 testing that behavior or lack of behavior.

15 (OTR comments)

16 MEMBER STETKAR: Okay, but does that mean
17 that every applicant and licensee who comes in takes
18 exception to this because they say, "I can't do what
19 you're asking me to do," and you say, "Yes, you can't
20 do what we're asking you to do, so you're okay."

21 MR. STATTEL: I'd like to speak to practice
22 a little bit. There is a reasonable assurance aspect
23 to this.

24 Typically, I mean, on the surface you would
25 say -- you could look at that and say, "Well, everything

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 should be verifiable, in some way," but we have found
2 very specific examples where code is not verifiable. In
3 other words, you can't test that code. There is no way
4 to do that.

5 A very simple example that I like to use is,
6 if binary variable equals one, then do 'a', else if it
7 equals zero, do 'b', else do 'c'.

8 Well, you're never going to get to the
9 'else', because it's either going to be a one or a zero.

10 However, my coding practices tell me that
11 I have to have 'else' statements every time I use an 'if'
12 statement, right. That way, I don't have any -- any
13 possibility of falling through.

14 So, I'm either going to have to break my code
15 -- my rule for coding practices, or I'm going to have
16 a line of code that is not verifiable, right.

17 What we typically see in practice, is a
18 vendor will do an assessment of test-ability, percentage
19 test-ability of the code, and we see this done on a
20 line-by-line basis on the code, and part of that process
21 is, they'll identify lines of codes or segments of codes
22 that you simply cannot test. It's not feasible to test,
23 and it's a small percentage, but it's -- but in a large
24 program, it becomes actually very significant.

25 So, to address those, they will typically

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 -- that is where they get into the line-by-line code
2 reviews, and they do alternate means of exercising that
3 code or verifying or validating that code.

4 So, now, do they actually achieve 100
5 percent testing, right? Actually, no, they can't.
6 It's not feasible to do that.

7 However, they've identified where the holes
8 are and they've taken compensatory measures to address
9 the lack of test-ability of those aspects of the system.

10 MEMBER STETKAR: I think I'm --

11 MR. STATTEL: So, in practice, that's what
12 we see.

13 MEMBER STETKAR: I think I'm actually
14 speaking at a somewhat higher level, than individualized
15 code or watchdog --

16 DR. ARNDT: Let me try to address that.

17 MEMBER STETKAR: -- times. I am speaking
18 about functions of the software system itself, such that
19 if the lights go off and someone sneezes in this room,
20 something that I have not necessarily thought of as
21 coincidence, the software suddenly doesn't eject me
22 through the roof.

23 DR. ARNDT: Right, and --

24 MEMBER STETKAR: Because that might be a
25 function of what the software is designed to do under

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 other conditions, and if I had thought about that, I
2 might specify that as requirement for my software.

3 DR. ARNDT: Right.

4 MEMBER STETKAR: It might not necessarily
5 be verifiable. You might not necessarily be able to
6 fully test all of the input conditions or have 100
7 percent coverage of all of the conceivable combinations
8 of things. But one could at least identify that and
9 specify that as a requirement.

10 However, the notion that any requirement
11 should be verifiable, could be read in the reverse and
12 say, "Well, I know I can't ever verify this, so, why would
13 I put that as a requirement?"

14 So, why would I ever think about that
15 combination of things?

16 DR. ARNDT: Right, and --

17 MEMBER STETKAR: Do you follow my thought
18 process?

19 DR. ARNDT: Yes, I do, and I think part of
20 this is, as was articulated earlier, you need to think
21 of this in terms of, this is guidance on what should be
22 done.

23 You should have verifiable requirements.
24 Your requirement should include the hazards that you've
25 identified. You should have a process to identify all

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the hazards, and work through that flow.

2 The point is, when we provide this guidance,
3 we're saying, "These are the things you should do."

4 When we evaluate that, we're using our best
5 engineering judgement, have they done a reasonable job?
6 Have they looked at all the operational occurrences?
7 Have they looked at all the operational failure modes?
8 Have they looked at all the things that could go wrong,
9 if x, y, z happened, and you articulated earlier,
10 hardware failure, software failure, combinations of
11 hardware and software failure.

12 The point is, you're never going to get to
13 an absolute prove-able situation, as you articulated
14 earlier, that you've covered all possible hazards,
15 because you're not going to know all the possible
16 hazards.

17 You're never going to get to a prove-able
18 reverse logic, like you articulated.

19 What we're trying to do is make sure they've
20 done good engineering judgement in the development of
21 this process, and by articulating the various things
22 they need to do in this guidance, we're trying to get
23 them -- lead them by the hand and say, "These are the
24 things, this is the process you have to get to, and the
25 things you need to consider," so that when we evaluate

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 it, it can be an acceptance criteria and an engineering
2 judgement level. Does that help?

3 MEMBER STETKAR: That does, thanks, yes.

4 MR. STATTEL: One of our key tools for
5 evaluating verify-ability or correctness is, we'll do
6 audits and we'll basically randomly choose
7 requirements, and we'll pull those down through the
8 implementation documents, and we get down to the actual
9 blocks of code and lines of code.

10 And if we have difficulty getting there,
11 right, then we basically challenge the developers, like,
12 well, if I'm having difficulty doing this, how is it that
13 your V&V team is coming to the conclusion that this
14 software was meeting those requirements?

15 It's not uncommon for us to have extensive
16 discussions on how they go about doing that.

17 CONSULTANT HECHT: Can I suggest that there
18 is a difference between reachability and the
19 verify-ability of these requirements here, and that they
20 are both valid, but distinct issues.

21 I think my -- myself, that this is a very
22 important point here. I'm glad it's there, because I
23 was looking for it, specifically.

24 These are what are called non-functional
25 requirements, and now, if I'm being paid as a control

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 system vendor to produce a feedwater control system or
2 whatever other control system that I am being told to
3 produce, I'm not necessarily getting paid to do this
4 stuff.

5 This is stuff which is there if things go
6 wrong, and it's very important to have this paragraph,
7 so that the NRC can go back, so the staff can go back
8 and tell the vendor or tell the licensee, "You haven't
9 fully addressed this.

10 Of course, we'll never know completeness.
11 We'll never know completeness about the safety of the
12 plant as a whole. A negative requirement saying that,
13 "You shall not release above a certain level at the plant
14 boundary," is in itself, un-provable.

15 CHAIRMAN BROWN: Okay, go on. The last
16 bullet is obvious, if there is no substantial changes.

17 MR. STURZEBECKER: Right. So, to shorten
18 this, I put the 830 Standard 1993. You can see a few
19 changes for the Annex, a new Annex B.

20 The existing items here, we've added our
21 variation or exception to, and we added that, yes,
22 unambiguity position statement there, and then the
23 secure analysis.

24 These were the specific changes. If there
25 is any comments on that, we can wrap up 72.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: Okay, 1.171 now.

2 MR. STURZEBECKER: Yes.

3 CHAIRMAN BROWN: Okay.

4 MR. STURZEBECKER: Unit testing, and this
5 is an important standard, or associated standard with
6 the guide.

7 It provides emphasis on unit testing for
8 software safety systems. You can usually go to the
9 smallest piece of software that can be tested
10 independently.

11 The general overview of changes in the
12 regulatory -- our Regulatory Position, we changed
13 Position 5 from other standards. We directed it
14 straight to 829, because it links -- touches base with
15 that standard, with the changes that's going on in 1.170,
16 which is coming up next.

17 So, what changed in the Reg Guide? I just
18 put down a few of the references that we've changed.
19 It's very minor items, just pointers to different parts
20 of the standard and the Reg Guide.

21 There is no substantial change to 1008, and
22 you can see I've got A for the references I was talking
23 about, and Regulatory Position 5.

24 So, we're asking that the licensee
25 recognize that, you know, unit testing is part of 829,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and we expect -- expectations that this guide is here
2 to stay.

3 Here is specific changes, title changes,
4 and that's that, for that one. Is there any questions?

5 CONSULTANT HECHT: Yes, I had some
6 questions here.

7 MR. STURZEBECHER: Okay.

8 CONSULTANT HECHT: Section 2 on page six,
9 you state that statement coverage isn't sufficient for
10 safety software, but you don't state what is sufficient.

11 MR. STURZEBECHER: Section 2, Regulatory
12 Position 2, and you're talking about -- what was the
13 section again?

14 CHAIRMAN BROWN: Which item is that again,
15 Myron?

16 CONSULTANT HECHT: It's on page six,
17 Section 2.

18 CHAIRMAN BROWN: Okay.

19 MR. STURZEBECHER: Section 2, testing,
20 okay, test program.

21 CHAIRMAN BROWN: Yes, which --

22 MR. STURZEBECHER: Yes, that was the
23 original.

24 CONSULTANT HECHT: That was the original
25 language --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Yes.

2 CONSULTANT HECHT: -- but I guess --

3 MR. STURZEBECKER: That was the original
4 language. Nothing has really changed from that. Was
5 there --

6 CONSULTANT HECHT: Well, I guess the
7 question is, after 30 years, can't we do more than that
8 statement?

9 CHAIRMAN BROWN: But which one are you
10 talking about, the A or the --

11 CONSULTANT HECHT: Just about statement
12 coverage --

13 MR. STURZEBECKER: Statement coverage?

14 CONSULTANT HECHT: -- not being
15 sufficient.

16 MR. STURZEBECKER: Well, you know, it
17 really hasn't changed the mechanics of it, from what I
18 understand.

19 But I -- I don't know of how much -- what
20 we would consider for 100 percent testing or make sure
21 the coverage is --

22 MR. SANTOS: You mean like suggestion like
23 FAA does for like MCDC?

24 CONSULTANT HECHT: Well, that would be one
25 approach which seems to have been feasible, and which

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 is fairly well defined and is unambiguous and provides
2 some clarity to a licensee.

3 And by the way, this gets back to the earlier
4 discussion we had about levels of -- levels of integrity,
5 because the DO178 and 278 standards have five levels.
6 Actually, DO278 has six.

7 So, I think both for the sake of the staff,
8 the poor staff guy who is confronted with a critical
9 safety kernel, perhaps involving the statement of what
10 this system does, in the event of a complex anomaly, and
11 for the licensee -- yes, for the licensee who is paying
12 the vendor, I guess, to do this, shouldn't an attempt
13 be done to do more than that?

14 MR. SANTOS: From my perspective, the key
15 word is commensurate with the level of complexity of the
16 particular code or application that is being looked at,
17 and I think that's why we keep the flexibility.

18 We are aware of those type of techniques,
19 but again, it's a matter that we don't specify
20 necessarily, the 'how'.

21 I don't expect that level of rigor for
22 various levels of complexity in the software.

23 CONSULTANT HECHT: But what -- shouldn't --
24 this is the -- this is going to be a real cost driver
25 here.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. SANTOS: Yes.

2 CONSULTANT HECHT: I mean, this might be an
3 issue of whether something is actually implemented.
4 This is not small.

5 MR. STURZEBECKER: Okay.

6 MR. SANTOS: I know. I mean, it's one of
7 those -- we can -- we're aware of, you know. I
8 understand your comment.

9 CONSULTANT HECHT: Are you going to -- is
10 there going to be any response to do anything about it?

11 MR. STURZEBECKER: I think we're going to
12 have to go back and look at this.

13 CHAIRMAN BROWN: I'm trying to look at
14 3.1.2, item two, that is -- 3.1.2 is planned tasks.

15 (OTR comments)

16 CHAIRMAN BROWN: No, it's under 1008.
17 That is what we're looking at, right?

18 MR. STURZEBECKER: Right 1008.

19 CHAIRMAN BROWN: And item two is specify
20 completeness requirements, and it says, "When testing
21 a unit during software, every software feature must be
22 covered by a test case or an approved exception."

23 I'm missing the coverage part of this,
24 statement coverage. How does that fall into this, for
25 this item?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 It says, "Section 3.1.2 item two specifies
2 statement covering, statement coverage, covering each
3 source language statement with a test case."

4 If you got a test case, why -- I am trying
5 to understand the comment a little bit here, Myron.

6 A test case does more than just -- what more
7 would you do?

8 CONSULTANT HECHT: Well, just because you
9 have complete statement coverage, doesn't mean that you
10 -- that you've covered all of the functions that the
11 software must do.

12 So, I'm just trying to think of an easy
13 example.

14 So, we have the section of code that says,
15 "Do 'x' if the threshold is at level one. Do 'y' if the
16 -- if the threshold is at level two."

17 Now, there is a question of, was the
18 condition level one or level two, was that correct?

19 MR. SANTOS: Correct, it might not cover.

20 CHAIRMAN BROWN: Okay, so, you're saying --

21 CONSULTANT HECHT: So, the decision of what
22 -- when to go into that -- into the branch, that led to
23 those statements?

24 CHAIRMAN BROWN: Well, that is questioning
25 the input though, right? I mean, the one and the two,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 I mean, I'm not a programmer. So, tell them.

2 MR. SANTOS: It's a good example we follow.
3 You might not get to the decision branch all the way
4 through.

5 CHAIRMAN BROWN: Say that again.

6 MR. SANTOS: You might not get all the
7 decision on the branches, as is stated with the code,
8 in the example Myron brought up. You just simply do a
9 straight statement coverage, just you know, one after
10 the other.

11 CHAIRMAN BROWN: If one, do 'x'. If two,
12 do 'y'?

13 MR. STATTEL: Is one and two correct?

14 MR. SANTOS: Right.

15 MR. STATTEL: I think it's less --

16 CHAIRMAN BROWN: Well, that is a
17 questioning of input. I mean, that is --

18 MR. STATTEL: Right, it's not a question of
19 whether you're covering the branches. It's whether
20 covering the branches is sufficient, to ensure the
21 correctness of the code, right.

22 CHAIRMAN BROWN: What if one and two?

23 MR. STATTEL: Right, I have always viewed
24 this as the unit testing in -- of itself, is not adequate
25 to ensure correctness, but there is also different

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 levels of testing, validation testing that are done
2 downstream of that.

3 So, in conjunction with that, that is where
4 we get our reasonable assurance. Actually, we put a lot
5 more weight on the validation tests, as far as verifying
6 the correctness of --

7 CONSULTANT HECHT: Let me expand on my
8 example. There are some things which are due to
9 external conditions.

10 In other words, if the threshold is set on
11 the basis of a set point, that would be true, but there
12 are other things that are based on the internal condition
13 of the machine, which are not really related to the set
14 points.

15 In those conditions if, for example, a disk
16 gets full. Let's use that as an example. That is not
17 a set point. That is not an input, or if there is an
18 overflow condition on a variable in the code, or if there
19 is corruption.

20 Those are things which have to be dealt with
21 internally, and you want to be sure that they're handled
22 correctly.

23 The NRC, I think has stated it correctly,
24 the current Reg Guide has stated it correctly, saying
25 that branch coverage is not sufficient, but they haven't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 -- so, they've set the floor, but they haven't set the
2 ceiling.

3 MR. THORP: Well, if I can offer -- I don't
4 know if this is helpful or not, because I have not read
5 these references.

6 But there is certainly a pointer to
7 references 14 and 17, one of which, 17 speaks to software
8 testing techniques and the other speaks to our research
9 document on high integrity software.

10 I don't know whether applicants or
11 licensees would find some degree of clarity or better
12 unambiguity in looking at those references, but I see
13 at least we've pointed toward those, as an aide in this
14 Reg Guide to, I would assume, to point to the discussion,
15 and my -- it's a gross assumption on my part, that
16 perhaps, the -- we've already said what is not enough,
17 but perhaps, these references would point to things that
18 could be used.

19 CONSULTANT HECHT: Well, I know the Bazer
20 book, and the Bazer book is a general book, and it won't
21 help in this condition.

22 CHAIRMAN BROWN: Okay, let me -- I want to
23 -- this is pretty subtle, but why doesn't the last
24 statement that says, "The licensee should identify and
25 justify the coverage criteria that it will use."

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I mean, at some point, somebody has got to
2 say, "What are we going to use," as opposed to just saying
3 'statement coverage'.

4 So, at least, somebody has got to identify
5 what the -- whatever the ceiling is, or whatever it is.
6 You may or may not agree with it, but at least they have
7 something to take issue with.

8 So, even though we're -- I agree, this is
9 a pretty vague statement, to say that coverage is blah,
10 blah, blah, is insufficient for measuring, but if -- but
11 they have it put in there, that the licensee has to
12 identify to us, what his criteria is going to be.

13 CONSULTANT HECHT: Well, I guess that is
14 fine, as long as the staff and the licensee agree on what
15 that is.

16 CHAIRMAN BROWN: Well, they don't -- they
17 can argue about it.

18 CONSULTANT HECHT: Yes.

19 CHAIRMAN BROWN: I think if they didn't
20 agree, they would argue about it.

21 You know, I understand the vagueness, but
22 I also think there is a ceiling that is something is put
23 in, on that -- in this particular comment, unless
24 somebody else wants to disagree with me. I would -- so,
25 do you have any problem, John? I think we're -- let's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 go ahead and move on.

2 Don't take that wrong way. I hadn't thought
3 about that one, I was reading this one, because I did
4 read that one. Karl?

5 MR. STURZEBECKER: All right.

6 CHAIRMAN BROWN: Where are we?

7 MR. STURZEBECKER: We are looking at the
8 specific changes --

9 CONSULTANT HECHT: I had one other --

10 MR. STURZEBECKER: Okay, go ahead.

11 CHAIRMAN BROWN: Okay.

12 CONSULTANT HECHT: -- question on this.

13 MR. STURZEBECKER: Sorry.

14 CONSULTANT HECHT: And that was, I wasn't
15 quite sure where you handled the off-nominal conditions
16 on the unit testing.

17 In other words, what is typically done in
18 the Bazer book refers to is both boundary value testing
19 and clearly, above limits and below limits.

20 Where is that addressed in this thing, or
21 in this Reg Guide, or even in the standard?

22 MR. STURZEBECKER: Yes, I don't think it's
23 even in the standard. I don't think it's even in the
24 standard above.

25 CHAIRMAN BROWN: If you all can't answer

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 it, don't --

2 MR. STURZEBECKER: I don't think it's
3 there, honestly, but I don't know.

4 CHAIRMAN BROWN: You want to repeat it
5 again?

6 MR. STURZEBECKER: I'd have to do a search.

7 CONSULTANT HECHT: Okay, off-nominal
8 testing, so, if you have an input variable and --

9 CHAIRMAN BROWN: So, it's out of range,
10 below --

11 CONSULTANT HECHT: At the boundary above
12 and below.

13 MEMBER STETKAR: Yes, the standard does
14 address that to some extent. It says --

15 CHAIRMAN BROWN: Where?

16 MEMBER STETKAR: Section 3.2.2 of the
17 standard.

18 CHAIRMAN BROWN: Three-point-two, the IEEE
19 standard?

MEMBER STETKAR: The IEEE
20 standard, not the Reg Guide.

21 It does say, "Invalid and valid input data
22 must be selected." It doesn't necessarily -- I don't
23 know what valid and invalid mean.

24 CONSULTANT HECHT: Well, it kind of relates
25 to this.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: This kind of relates to
2 it.

3 It says, "When complete testing is
4 impractical, information regarding the expected use of
5 the unit should be used to determine selections,
6 identify the risk associated with unselected elements."
7 So, it kind of addresses that area.

8 CHAIRMAN BROWN: Which item? Where are
9 you reading from? Which item?

10 MEMBER STETKAR: You know, I write these
11 things down, so, I don't have to have 12 things open at
12 the same time.

13 CHAIRMAN BROWN: Okay.

14 MEMBER STETKAR: It's in Section 3.2.2, on
15 term and tasks, but as I said, I excerpted this, so, I
16 need to --

17 CHAIRMAN BROWN: I'm just -- I was looking
18 for the summary that you gave.

19 CONSULTANT HECHT: I was looking for the
20 word 'invalid', and I didn't get to it until an Appendix.
21 I see it in --

22 MEMBER STETKAR: There is it, 5, right.

23 CHAIRMAN BROWN: Yes, item 5.

24 MEMBER STETKAR: It's item 5 on page --

25 CHAIRMAN BROWN: Invalid and valid input

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 data must be selected.

2 MR. THORP: It almost sounds like in range
3 and out of range.

4 MEMBER STETKAR: I don't know what valid
5 and invalid means, because --

6 CHAIRMAN BROWN: I mean, come on. Yes, I
7 understand --

8 MEMBER STETKAR: But it kind of addresses,
9 I think --

10 CHAIRMAN BROWN: Valid, to me, is a
11 boundary condition -- out of range could become invalid,
12 in a way. That's is -- I've got simple mind, when it
13 comes to this kind of stuff.

14 So, if I've got a range of zero to 100, then
15 I would expect zero and 100 to be a valid piece of data,
16 but if it goes to 100.001 or --

17 MEMBER STETKAR: That is the way I think of
18 it, but one can also think of a string of bits that has
19 something that isn't recognized as a valid data
20 character, and therefore, it gets rejected as not even
21 read, because that is not a valid data string, regardless
22 of what value it's actually trying to present.

23 CONSULTANT HECHT: So, there is corrupt
24 data --

25 MEMBER STETKAR: There is corrupt data and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 then there is something within the expected range of a
2 parameter value.

3 CHAIRMAN BROWN: And you never know what
4 corrupt data is going to do to that input function.

5 CONSULTANT HECHT: Right.

6 CHAIRMAN BROWN: As I've made that
7 statement before.

8 CONSULTANT HECHT: Let me state
9 specifically, what should be -- what this kind of testing
10 should be getting to.

11 For the case of the corrupt data, which I
12 really wasn't considering, it's just that you have some
13 kind of a CRC check or some kind of a basic check to be
14 sure that this stuff which could crash your unit doesn't
15 do that.

16 For the case of the boundary condition, it
17 comes down to whether you have a greater than or greater
18 than or equal or less than or equal. Did you do that
19 part right?

20 It also relates to, did you check for the
21 zero denominator condition, and of course, you also want
22 to check for the out of range, for -- in the language
23 where you have typed variables.

24 For example, water temperature, you should
25 know it should not exceed whatever the equation of state

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 says that water should evaporate at, and whatever
2 pressure you're at.

3 So, you should have those ranges properly
4 set, and once again, if you have unexpected values coming
5 into your module, you might get an unexpected result.

6 MR. STURZEBECKER: Right.

7 CONSULTANT HECHT: So, we have some general
8 statements in the code. I might suggest that maybe some
9 more guidance in that area.

10 MR. STURZEBECKER: Okay, I think we
11 deleted, in reference to this. There is a note.

12 MR. SANTOS: Myron, everything you
13 mentioned, we cannot incorporate in our review when
14 we're looking at the overall fault tolerance strategies
15 presented by an applicant.

16 CONSULTANT HECHT: I'm sure you do, I was
17 just looking at the document.

18 MR. SANTOS: Okay.

19 CHAIRMAN BROWN: Yes, I'm just trying to
20 look at the examples. I'm just trying to play with the
21 examples you gave. I'm doing my devil's advocate
22 routine.

23 I mean, the 'divide by zero' is obviously
24 an invalid --

25 CONSULTANT HECHT: You need to check for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that.

2 CHAIRMAN BROWN: Well, yes, but I mean,
3 that -- if they ask, you know, you've got to look at
4 invalid, as well as valid input data type things, so that
5 you're not asking something.

6 I mean, those are results, and I always
7 hesitate to get -- trying to get so specific, as to
8 specific circumstances to deal with, how you cover that
9 in a more general -- in a more general thought process,
10 because I mean, I don't even -- you know, CRC's are fine
11 for data transmission, except if the data is corrupt when
12 it starts and you calculate a CRC based on the corrupt
13 data, then you end up with corrupt data at the other end,
14 and the CRC says it's just fine, and you boil your system
15 up, or it locks up the process or whatever it is.

16 So, a CRC check is not necessarily a
17 cure-all or --

18 CONSULTANT HECHT: No, it's not. All of
19 the --

20 CHAIRMAN BROWN: Yes, I understand that.
21 So, I think --

22 MR. STATTEL: I would also like to make an
23 observation.

24 With a typical PLC system that uses function
25 block diagrams, this level of testing that we're really

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 dealing with here, would be at the function block or what
2 some people call primitive levels.

3 So, and 'and gate', you know, and multiplier
4 module, that type of thing, and typically, we see those
5 -- those code at -- when we review platforms, when we
6 review the platform level, not the applications, and
7 typically, those are very widely used, not just in this
8 industry, but they're used throughout multiple
9 industries.

10 They have a lot of usage, so they have a lot
11 of runtime with them.

12 So, some credit is taken for the application
13 and the history of those primitives, and typically,
14 those are part of libraries, approved libraries that are
15 incorporated in the particular version of the PLC that's
16 being implemented.

17 It's just an observation, because I know
18 we're kind of thinking of code. We're kind of thinking
19 of the old fashion C-Code or something like that. You
20 know, are we getting down to the --

21 CONSULTANT HECHT: Here, we're talking in
22 general about a unit, and the --

23 MR. STATTEL: But it's defined
24 differently, depending on what type of technology you're
25 dealing with.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CONSULTANT HECHT: Sure.

2 MR. STATTEL: FPGA is another matter all
3 together.

4 CONSULTANT HECHT: Well, but we're not
5 talking about FPGA's here. We are think -- I think
6 function blocks are in scope, but even there, we're not
7 talking about what the vendor is providing in his COTS.
8 That is a separate discussion.

9 What we're talking about here is that in
10 that function block, there should be input checking, and
11 the off-nominal testing should be checking for the
12 completeness and correctness of that input checking, or
13 those limits, prior to actual executing the function
14 within the block.

15 MR. STATTEL: Okay, well, I'm not really
16 referring to COTS here.

17 CONSULTANT HECHT: And this is application
18 stuff. I mean, this is stuff that --

19 MR. STATTEL: Well, I understand that, but
20 I'm not referring to COTS, in particular, because the
21 platforms that we reviewed, the platforms that are being
22 used for safety applications, those function blocks
23 actually perform those -- these types of data checking
24 and validity checking.

25 It's really -- you have to really go behind

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the application and see how that is implemented within
2 the platform.

3 CONSULTANT HECHT: Well, you said it was
4 provided by the vendor.

5 MR. STATTEL: It's provided by the vendor,
6 but it's not COTS. We review the vendor. We review
7 their processes for developing those primitive elements
8 of the software.

9 CONSULTANT HECHT: Well, okay, if it's
10 being developed for a specific plant --

11 MR. STATTEL: No, no, not for a specific
12 plant.

13 It may be -- there may be a library or
14 functions within a library, that those functions are
15 shared between the paper industry, aviation, what not,
16 and they use those for -- they credit those and they put
17 them in the qualified library for the nuclear
18 applications.

19 But really, when you pull the string back
20 and see where -- you know, where are these -- where is
21 the validity established for these off-range checking,
22 boundary checking, it's established, you know, at the
23 development of that primitive element and by the vendor.

24 It's not COTS. We don't consider that
25 COTS. We consider that within the scope of our review.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 We review those processes and how they develop those.

2 CONSULTANT HECHT: So, that is part of the
3 unit testing?

4 MR. STATTEL: In a lot of cases, that is how
5 it's defined.

6 I'm not going to say in all cases, because
7 different vendors handle it differently and they draw
8 different boundaries for what they consider to be unit
9 testing.

10 But certainly, we've seen a couple of
11 instances at least, with PLC type devices, where they've
12 defined those primitive elements as being the -- this
13 level of testing, this unit testing.

14 CHAIRMAN BROWN: Unit testing.

15 MR. STATTEL: Software unit testing.

16 CHAIRMAN BROWN: At that level.

17 MR. STATTEL: Correct, and then when you
18 get down into actually, drawing the lines between the
19 function blocks and putting your system together, you're
20 getting down into more -- more into the validation level
21 testing.

22 MR. STURZEBECKER: So, is that clause right
23 there, is that sufficient, you're saying, or not? I
24 mean, valid --

25 CONSULTANT HECHT: About invalid testing?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Yes.

2 CHAIRMAN BROWN: Invalid and valid input
3 data must be selected for the test.

4 CONSULTANT HECHT: I'll just make that
5 point in my report, and you guys can decide what to do.

6 CHAIRMAN BROWN: Okay, that works. That
7 works.

8 MR. STURZEBECKER: We did delete it,
9 because we thought it was redundant. I did find my notes
10 on that, to that paragraph that -- but for that
11 particular line, I mean, doesn't mean we're not
12 incorporating it. It's just redundant.

13 CHAIRMAN BROWN: Well, you mean, you didn't
14 repeat it, from the standard --

15 MR. STURZEBECKER: Right.

16 CHAIRMAN BROWN: -- into the Reg Guide, so
17 it was --

18 MR. STURZEBECKER: It was dropped off of
19 here.

20 MEMBER BLEY: That's okay, I don't have any
21 trouble with that.

22 MR. STURZEBECKER: Yes.

23 CHAIRMAN BROWN: We don't need to repeat
24 the Reg Guide, I mean, the standard into the Reg Guide.
25 I agree with -- where you have exceptions, or what have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 you, or where you've had additions --

2 MR. STURZEBECKER: Right.

3 CHAIRMAN BROWN: -- excuse me.

4 MR. STURZEBECKER: So, that sentence isn't

5 --

6 CHAIRMAN BROWN: Okay, yes, just put it in
7 there and explain it, and then we can munch around on
8 it, okay?

9 MR. STURZEBECKER: No, it's still 1987.

10 CHAIRMAN BROWN: Okay, where are we?

11 MR. STURZEBECKER: I think we're just at
12 the final end of this. Any of the specific changes to
13 the guide and the standard, we're ready for Reg Guide
14 1.170, which is a big one.

15 (OTR comments)

16 CHAIRMAN BROWN: So, it's 1.171, right?

17 MR. STURZEBECKER: Yes.

18 MEMBER STETKAR: We just finished that.

19 CHAIRMAN BROWN: Yes, I just turned the
20 page. We're back on schedule, okay.

21 With that in mind, we will recess until,
22 what does this schedule call for, 1:00 p.m. See you all
23 back here bright-eyed and bushy-tailed.

24 (Whereupon, the above-entitled matter went
25 off the record at approximately 11:55 a.m. and resumed

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 at approximately 1:05 p.m.)

2 CHAIRMAN BROWN: We are now back in
3 session, and I guess it's with RG 1.170, and you may
4 start.

5 MR. STURZEBECKER: Okay.

6 CHAIRMAN BROWN: Karl?

7 MR. STURZEBECKER: I have to find my notes.

8 (OTR comments)

9 CHAIRMAN BROWN: You ready, Karl?

10 MR. STURZEBECKER: Yes, I'm ready.

11 CHAIRMAN BROWN: Okay.

12 MR. STURZEBECKER: This Reg Guide is based
13 upon 829.

14 Originally, when we started on this, we were
15 off of the interim 1998, and I changed that I think, to
16 catch up with the 2008 version because of its
17 significance.

18 Literally, between the two standards, from
19 the original, where the Reg Guide is based on, the 1983
20 version to the 2008, it's doubled in size.

21 CHAIRMAN BROWN: The IEEE standard?

22 MR. STURZEBECKER: Yes, the IEEE standard
23 has doubled in size.

24 It's not as, shall I say, messy as 1074, in
25 the sense that it scrambles everything around.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 This one is kind of neat, because it
2 expands, goes from really simple one-dimensional, here
3 is the documentation flow that you go through, to almost
4 a three-dimensional aspect, where it adds more document
5 -- hierarchy of documents, and you'll see this when we
6 get into it, where you have a master test plan versus
7 just test level, and it introduces integrity into the
8 situation, and the different levels, even though we're
9 holding at level four for that.

10 So, that is kind of the overview. Let's see
11 here, what is going on with that.

12 So, like I was saying, the major additions
13 here, like the third bullet there you've got integrity
14 levels that is in Clause 4, document strategies, 6 and
15 process directions.

16 It's also -- in our Reg Guide, we have quite
17 a few exceptions, probably the highest number of
18 exceptions of all the standards that we took to this
19 particular standard update.

20 But they're simple. They're not too
21 difficult.

22 So, like I was saying, it has an overarching
23 process that -- it has a master test plan that you're
24 going to use, and it also -- for the standards in sync
25 with 1074 and the whole idea of your software project

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 life cycle process.

2 What is neat about this standard is that it
3 improves -- you have multiple levels of testing that you
4 can build, and I think because of that, it gives you this
5 opportunity to handle more complex projects, if you may.
6 It can be scaled down or scaled up. So, it has some good
7 flexibility, in that sense.

8 I forgot to add the last bullet there. It
9 has a -- I'd say a test loop, but a formal documentation
10 process for anomalies, which is -- which wasn't present
11 in the original, and that is in Clause 8.

12 So, what has changed in the Reg Guide?
13 First two -- the first three are all in Position 1, Reg
14 Guide Position 1, and that is where we massaged into that
15 first Regulatory Position, the whole idea of integrity,
16 we're asking for integrity level four.

17 There was a public comment on how we had
18 addressed that. There was a question on -- hold up, I've
19 got to get back to that.

20 The point that they made was they didn't
21 like the paragraph under -- just before you get to your
22 A through G items under Regulatory Position 1, test
23 program.

24 But that paragraph, as a minimum, the
25 information additions highlighted below, with the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 master test plan, provides an acceptable approach.

2 There was some confusion in the sentence
3 before, so, we've updated that. So, it's an
4 understanding that these items below go along with the
5 master test plan, when you're producing your test
6 program.

7 So, A through G are -- is also what we're
8 looking for.

9 There is a new sub-reg -- or Regulatory
10 Position 1G, we added that new paragraph there, to note
11 that there is now the test -- level test log Clause 13
12 and 14, that the licensee should be aware of, and that
13 highlights the anomaly reporting along with that, the
14 documentation, which is new also.

15 The next is Regulatory Position 2, where
16 we're looking at documentation for deviation policy.
17 That is 8.2.3. -- I've got to look that up, sorry.

18 Yes, on that Regulatory Position software
19 documentation, we added that second paragraph there, and
20 the last line, "Any variations needed to follow and
21 establish deviation policy as discussed in Clause
22 8.2.3.3."

23 So, what this is saying is that if you're
24 going through your testing, you go through your test case
25 and you have a deviation in the software or something

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 that has to be changed, we want you to look at that new
2 Clause 8.2.3.3 and record what has happened.

3 So, again, this standard gives that ability
4 to document changes that happen, as they're going
5 through the different test levels, if you're starting
6 with unit tests or component tests or system tests.

7 And E, we've provided -- that is an
8 interesting one, because the Regulatory Position 3 on
9 documentation, there was a clause in the standard, say
10 in Clause 6.4, where they were given the option, you
11 could combine documentation by lowering the integrity
12 level, and we're saying no, we want integrity level
13 four maintained.

14 CHAIRMAN BROWN: You said that is in E?

15 MR. STURZEBECKER: That's E, yes.

16 CHAIRMAN BROWN: One-E?

17 MR. STURZEBECKER: No, I'm sorry, it's on
18 the slide, it's E, but in the actual Reg Guide, it's
19 Regulatory Position 3 --

20 CHAIRMAN BROWN: And six?

21 MR. STURZEBECKER: -- the second
22 paragraph.

23 CHAIRMAN BROWN: Well, it's also in six,
24 isn't it?

25 MR. STURZEBECKER: Six?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: It says, "The
2 licensee/applicant should assign integrity level four
3 or according to software use in nuclear plant safety,
4 as demonstrated by its mapping."

5 MR. STURZEBECKER: I'm sorry, okay. Which
6 one?

7 CHAIRMAN BROWN: Six.

8 MR. STURZEBECKER: Six, it was on six, too?
9 Yes, on six, Regulatory Position 6 is integrity level.

10 So, yes, that is our main -- that was a new
11 added Regulatory Position, but we have it here, under
12 'test documentation', because the idea is that if they
13 go through the standard in six, the clause in the
14 standard in six, it talks about documentation and
15 different ways you can use the documentation, yes, I see
16 that.

17 So, there is -- we're talking to integrity
18 in Regulatory Position 3 at the same time, if you could
19 follow what I'm saying.

20 CHAIRMAN BROWN: Correct me if I'm wrong,
21 but I thought under the test documentation, the standard
22 allowed some variability, in terms of the integrity
23 level at which they could make a decision -- they could
24 -- in other words, they could reduce it or change it,
25 and you all just effectively said no.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Right, you just hold it
2 at four.

3 CHAIRMAN BROWN: Based on the criteria that
4 they had thrown in there.

5 MR. STURZEBECKER: Right.

6 CHAIRMAN BROWN: So, that was the
7 highlight. That was the -- to me, that was the highlight
8 of that particular exception.

9 MR. STURZEBECKER: Right, in six.

10 CHAIRMAN BROWN: Then you re-emphasize the
11 fact that -- as you did earlier, that doing anything
12 other than four, you'd emphasize that twice in six.

13 MR. STURZEBECKER: Yes, it's in Regulatory
14 3 and it's also in 4 -- in 6, correct.

15 So, it -- but it's specific -- I mean, you
16 could say it is a duplication.

17 CHAIRMAN BROWN: No, that's okay, we'll
18 duplicate that one.

19 MR. STURZEBECKER: I think considering --
20 and at the same time, the next paragraph that follows
21 it, under Regulatory Position 3, we do give the option
22 -- or point out that, you know, you can use open-entry
23 type test logging for documentation when you're going
24 through things.

25 So, I mean, we understand, you know, that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the documentation can be quite, you know, arduous, but
2 at the same time, we still want to maintain this level
3 four, you know.

4 CHAIRMAN BROWN: What do you mean by an
5 open-entry?

6 MR. STURZEBECKER: That is if you have a
7 test log and it's standard paragraphs with -- and you're
8 going through test and you have a little spot that's
9 open, and you enter in the test data.

10 Then you go to the next transmitter you're
11 going to check, or whatever, if it's a code that you're
12 doing, you can enter -- you can reproduce that same --

13 CHAIRMAN BROWN: Okay.

14 MR. STURZEBECKER: Yes, so, it's the same
15 spot. It's just repeated over and over and over again,
16 and it's --

17 CHAIRMAN BROWN: In what way? In order to
18 the previous --

19 MR. STURZEBECKER: You're not letting --
20 right, you're just -- right.

21 CHAIRMAN BROWN: It's like a number of
22 different data sheets. I mean, you just have a new data
23 sheet for each --

24 MR. STURZEBECKER: Yes.

25 CHAIRMAN BROWN: Okay, okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Yes.

2 CHAIRMAN BROWN: I didn't get --

3 MR. STURZEBECKER: Yes.

4 CHAIRMAN BROWN: All right, okay, got it.

5 MR. STURZEBECKER: Yes, it's -- I think
6 sometimes it's in tool -- you'll find it in tools.

7 CHAIRMAN BROWN: Well, you're implying that
8 this is done with a software tool or something.

9 MR. STURZEBECKER: Correct.

10 CHAIRMAN BROWN: As opposed to paper and
11 pencil.

12 MR. STURZEBECKER: Could be done with paper
13 and pencil, yes.

14 CHAIRMAN BROWN: Or pen, I should say.

15 MR. STURZEBECKER: Yes, so, it's open, yes.
16 So, that takes care of slide 34. Like I said, we had
17 quite a few here.

18 Slide 35, now, this is where we start moving
19 into the new Regulatory Positions we added, like six,
20 and that is the first one, integrity levels, and we're
21 taking exception to the table in B3, where they have
22 those -- the risk assessment scheme, and I'm trying to
23 recall what this was.

24 Yes, we took exception to that, because they
25 -- I think they mixed -- I have to look it up.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: Well, that is just -- you
2 used -- it allowed you to evaluate software at a level
3 lower than level four.

4 MR. STURZEBECKER: Right, but we want --
5 you can go to occasional type, the likelihood that it's
6 going to happen at occasional or unlikely, they started
7 giving that option of three and we're saying no, we're
8 just keeping it at four. Catastrophic is catastrophic.

9 MEMBER STETKAR: What I wanted to
10 understand from this, Karl, is -- I agree with you taking
11 exception to the table, because I understand what
12 likely, probably, occasional and unlikely means in the
13 grand scheme of the world.

14 So, without -- they do define catastrophic,
15 critical, marginal and negligible, in terms of the
16 consequences, but on a frequency axis, I have no idea
17 what those words mean.

18 However, and this -- the same question on
19 1.168, where you also take exception to this notion of
20 a risk approach to characterizing the integrity levels.

21 The statement in C.6 says, "The NRC staff
22 takes exception to the Table B.3, risk assessment scheme
23 in Annex B. The IEEE Standard 829-2008 statement about
24 the Table B.3 illustration for determining the
25 likelihood in evaluating software integrity level lower

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 than level four is not acceptable." I understand that.

2 MR. STURZEBECKER: Okay.

3 MEMBER STETKAR: Then it says, "The
4 probability of occurrence is likely to cause
5 catastrophic consequence."

6 MR. STURZEBECKER: Okay.

7 MEMBER STETKAR: "And thus, the breadth or
8 depth of testing and documentation should adhere to the
9 proper activities for nuclear software safety system
10 products."

11 This seems to tell me that even if something
12 is infinitely unlikely of occurring because the
13 consequences should be -- could be catastrophic, I have
14 to assign that as the highest level. Is that --

15 MR. STURZEBECKER: That is pretty much it,
16 yes.

17 MEMBER STETKAR: Okay, does our software
18 protect us against meteorite strikes?

19 See, this whole notion that just because I
20 can assign whatever unlikely means, you're not accepting
21 that as a rationale for rank-ordering things.

22 MR. STURZEBECKER: Right.

23 MEMBER STETKAR: And I guess, how does that
24 meld with the overall agency's risk informed approach
25 to things?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Considering that it's
2 digital and we really don't have a so-called risk idea,
3 from what I understand --

4 MEMBER STETKAR: Yes, but you don't even
5 review that non-safety related digital stuff, because
6 we know that is unimportant.

7 MR. STURZEBECKER: Right, right.

8 DR. ARNDT: We've made a conscious decision
9 that in this particular kind of risk assessment, that
10 the agency's position, and it's articulated in several
11 places, including the Standard Review Plan, is that for
12 safety related systems, we will consider them in the
13 highest quality category.

14 MEMBER STETKAR: And I have no problem with
15 that, because like I said, I have no idea what these
16 frequency terms mean, at all, and until I understand
17 that, you know, they don't mean anything to me.

18 However, why do you need to belabor the
19 point, by saying that simply because there is a
20 probability of an extreme consequence, you won't accept
21 it?

22 DR. ARNDT: Good comment.

23 MR. STURZEBECKER: Right.

24 DR. ARNDT: We will look at that, and see
25 whether or not --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Because the statement
2 already says, you want it to be four.

3 DR. ARNDT: Right.

4 MR. STURZEBECHER: Yes.

5 DR. ARNDT: We can look at -- we'll present
6 it and --

7 MEMBER STETKAR: Look at that in six and
8 look at it under C.1, in 1.168, because the same type
9 of comment is made there about --

10 DR. ARNDT: Yes, we may have been trying to
11 be overly verbose for something that is better stated
12 --

13 MEMBER STETKAR: Just so you want it --
14 number four regardless, and that is --

15 CHAIRMAN BROWN: You may want to delete
16 sentence three in that paragraph.

17 MEMBER STETKAR: You just want to delete
18 sentence three?

19 CHAIRMAN BROWN: I'm trying to --

20 MEMBER STETKAR: I'm not going to tell you
21 how to write your own Reg Guide.

22 (OTR comments)

23 DR. ARNDT: We understand the comment and
24 it is --

25 MR. THORP: I'd like to work with Karl on

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 that sentence. The sentence itself is a little bit
2 awkward. So, I think we'll --

3 MEMBER STETKAR: Well, there is a similar,
4 but worded slightly different in 1.168, but the same
5 concept is there.

6 DR. ARNDT: We understand.

7 MEMBER STETKAR: Thanks.

8 MS. ANTONESCU: What sentence is that?

9 CHAIRMAN BROWN: Sentence three in
10 sub-paragraph two, and it's integrity levels.

11 (OTR comments)

12 MR. THORP: The probability of occurrence
13 is likely to cause catastrophic consequences and thus,
14 will represent the testing. I think we can work with that
15 one to produce the --

16 CHAIRMAN BROWN: I'd just delete it, if you
17 -- it's very clear, you don't agree, it's not acceptable
18 to determine the likelihood of evaluating integrity.
19 The licensee should use level four.

20 I mean, it's just so crisp, instead of
21 bundling it way in the middle.

22 CONSULTANT HECHT: I didn't see much of a
23 difference between integrity level three, four and the
24 tasks that are --

25 CHAIRMAN BROWN: You don't like that word?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I can spell it.

2 MEMBER STETKAR: I don't want you to spell
3 it.

4 MR. STURZEBECKER: All right, deleted.

5 CHAIRMAN BROWN: The way I read that, as I
6 said, we're not doing risk assessment schemes for
7 software, bottom line.

8 MEMBER STETKAR: Well, but they are,
9 because they're saying --

10 CHAIRMAN BROWN: But they took that out.

11 MEMBER STETKAR: They're saying they only
12 look at consequences, which is some element of --

13 CHAIRMAN BROWN: Not if they take it out.

14 MEMBER STETKAR: -- partial risk
15 assessment.

16 MR. STURZEBECKER: Okay.

17 CONSULTANT HECHT: Can I ask a couple
18 questions?

19 CHAIRMAN BROWN: Yes.

20 CONSULTANT HECHT: All right, thank you,
21 Mr. Chairman.

22 CHAIRMAN BROWN: As long as John is
23 finished.

24 CONSULTANT HECHT: Number one, actually,
25 it wasn't a question, but it was a comment.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 With respect to unit testing, you were
2 talking about the invalid inputs, or you know, what I
3 call off-nominal inputs, and somebody said, "But it's
4 covered in 829."

5 I wanted to point out that that discussion
6 was related to a different standard. That would -- that
7 comment was related to Standard 1008.

8 So, I will write in my report, I think my
9 comment still stands about off-nominal testing at the
10 unit level, even though it is mentioned here, with
11 respect to test documentation.

12 MR. STURZEBECKER: Okay.

13 CONSULTANT HECHT: The question that I had
14 was, how do we deal with regression testing?

15 MR. STURZEBECKER: It's one of the suites
16 of testing that goes on. I don't recall whether we
17 mentioned it specifically.

18 CHAIRMAN BROWN: Yes, regression testing
19 is mentioned in some places within the documents.

20 CONSULTANT HECHT: Right.

21 MR. STURZEBECKER: Okay.

22 MEMBER STETKAR: Pretty much under V&V.

23 CHAIRMAN BROWN: Yes, it says types of
24 testing and regression testing is identified as one of
25 the methods of testing.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Okay.

2 CONSULTANT HECHT: Well, it's not a method
3 of testing.

4 CHAIRMAN BROWN: Well, whatever it is.
5 I'm not that smart.

6 CONSULTANT HECHT: Well, it's -- how shall
7 I say it?

8 Something you got to do, and you got to spend
9 time and money on, because you made a change and you wish
10 had made the change before you started the test, so, you
11 don't have to do the testing over, and that is -- you
12 know, when does regression testing, and how much
13 regression testing one does is a -- is a significant cost
14 and schedule driver.

15 MR. STURZEBECKER: Absolutely,
16 understood.

17 CONSULTANT HECHT: So, and
18 the other question -- and the third question that I had
19 was, failure recovery testing.

20 Now, you know, you did mention failure
21 recovery testing with -- or failure recovery
22 requirements, with respect -- in the requirements Reg
23 Guide, but you didn't really address failure recovery
24 testing -- or I'm not going to ask it that way.

25 Where do you address failure recovery
testing in this standard?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STURZEBECKER: It would have to be in
2 the standard, because I don't --

3 CONSULTANT HECHT: Or in the Reg Guide?

4 MR. STURZEBECKER: Yes, it would have --
5 yes, I think it would have to be in the standard, and
6 I'm not -- I would have to look for it.

7 You know, I've kind of gone through the
8 deltas.

9 CHAIRMAN BROWN: Which one? This one?

10 (OTR comments)

11 CONSULTANT HECHT: And where I really saw
12 it was with respect to Regulatory Guide Position 4.

13 MR. STURZEBECKER: All right.

14 CONSULTANT HECHT: System testing, and it
15 says, you know, and the sentence says, "The licensee
16 should formally test all associated features of the
17 safety system following the recommended activity and
18 process outlined under Clause 5," and I look at Clause
19 5, and it wasn't really --

20 MR. STURZEBECKER: Well, the way Clause 5
21 works is, it steps through each of the activities for
22 the process for documenting, and I think we made that
23 association with this new standard, because we were
24 thinking -- and that frame of mind that, you know, the
25 testing would be listed into one particular area.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CONSULTANT HECHT: Fair enough.

2 MR. STURZEBECKER: You know, it --

3 CONSULTANT HECHT: But I guess --

4 MR. STURZEBECKER: Yes, it's -- it's a
5 system -- you know, system testing is one aspect -- I
6 mean, when you go through the standard, you're suppose
7 to be doing unit -- setting up your planning for unit
8 component and systems, the overall systems.

9 CONSULTANT HECHT: Right.

10 MR. STURZEBECKER: So, specifically, you
11 know, you're doing that triad all the time, and how many
12 times -- the iterations you're setting it up, you know,
13 it depends on --

14 CONSULTANT HECHT: Well, I would expect the
15 failure -- does that recovery failure something that
16 would happen above the unit and either at the component
17 and the system level, and therefore, the system level
18 would be the most general place to handle it.

19 Well, I guess my observation is that it
20 doesn't seem to be sufficiently or explicitly addressed.
21 Let me put it that way.

22 MR. STURZEBECKER: Yes, it isn't
23 explicitly --

24 CONSULTANT HECHT: And that is kind of
25 important in the safety system.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Yes.

2 CHAIRMAN BROWN: Okay, let me try and
3 understand. You may have to elucidate a little bit more
4 in your report.

5 But when I read that, I went back and I
6 looked at what did they mean, when they said 'outlined
7 under Clause 5'?

8 So, then I went and looked in Clause 5 of
9 this, of the Reg Guide, and it says at the end, "The test
10 documentation from Clause 8 through 17 should include
11 these references," and it goes back and talks about
12 various types of documentation, and if you go look at
13 the IEEE standard, then it's effectively saying Clause
14 8 through 17 are starting with the master test plan,
15 level test plan, level test design, level test cases,
16 all the way through.

17 So, that was the process I was thinking they
18 were referring to by -- that's all of those. So, what
19 I was looking for, a track from the -- here is -- they
20 look at Clause 5 and follow that process, and okay, well,
21 is that specified somewhere in it?

22 MR. STATTEL: I agree that this particular
23 guide does not specifically address regression testing.

24 Now, regression testing is obviously not
25 some suite of tests that always get performed.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Well, are you talking
2 about regression testing in this clause?

3 MR. STATTEL: That's what you were
4 referring to, is regression testing.

5 CONSULTANT HECHT: No, that was one topic.

6 CHAIRMAN BROWN: That was the previous
7 topic.

8 MR. STATTEL: Right, well, what I want to
9 mention though is, those issues are normally addressed
10 in the planning documentation, which really is covered
11 under a different guide, different guidance, right.

12 CONSULTANT HECHT: Well, isn't this the
13 documentation?

14 MR. STATTEL: Well, for instance, we have
15 a -- we evaluate a software test plan, and normally, the
16 process for addressing those types of test methods and
17 how to assess changes, the change process and determine
18 what tests need to be re-performed, for example, that
19 would be typically identified in the test plan, planning
20 documentation.

21 CONSULTANT HECHT: Well, this precisely --
22 isn't that precisely what this standard is dealing with,
23 what's in the master test plan and the level test plan?

24 MR. STATTEL: Well, that's more process.
25 This is the documentation. This is a guide for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 documentation of the tests -- of the performance of the
2 tests.

3 MR. STURZEBECKER: But you're right, it
4 does drop into -- academically, it drops into that one
5 -- whatever you're setting up that plan for. It's
6 suppose to reflect in the master test plan, and then it
7 -- whatever test levels you devise, then you've got to
8 follow through.

9 Supposedly, the test process in 5, where
10 you're running through each of the life cycles, it's --
11 you know, you step all the way through to the end, and
12 when -- and then when you set -- after you set the test
13 plan up, then you go through, like you were saying, and
14 you start with the units, migrate back to your components
15 and then probably hit the system all at the top point,
16 right, and that's where you're saying the failure -- how
17 do you recover from it?

18 CONSULTANT HECHT: Well, the planning
19 document should -- and I'll try to address this point,
20 in trying to distinguish between process and
21 documentation.

22 The documentation should describe how one
23 addresses failure recovery testing, how it's done, and
24 it doesn't necessarily fit into the normal -- how should
25 I say it? Traceability for requirements.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Those requirements in that area are not
2 clear. Failures don't follow the way we write a spec.

3 MR. STURZEBECKER: But if the requirements
4 were up front, then they would be written in the master
5 -- the whole process, and then the testing should -- this
6 document -- they should reflect this to what is -- that
7 requirement is, and that should become part of the master
8 test plan, and thus, part of the -- one of the attributes
9 of going through those tests, and those units --

10 CONSULTANT HECHT: Okay.

11 MR. STURZEBECKER: -- should not -- I mean
12 --

13 CONSULTANT HECHT: That should be clear.
14 Let's just deal with the real simple case. We have a
15 single failure criteria.

16 MR. STURZEBECKER: Okay.

17 CONSULTANT HECHT: That is basically the
18 ultimate source of all the failure recovery testing that
19 we need to do.

20 The single failure criterion may or may not
21 get completely and properly decomposed, because you
22 don't know how the system is going to be built when you
23 write the requirements.

24 MR. STURZEBECKER: Yes, now I know where
25 you're going.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CONSULTANT HECHT: So, you end up with the
2 system --

3 MR. STURZEBECKER: It's a Catch-22.

4 CONSULTANT HECHT: -- which has ethernet
5 and it has, you know, Rockwell or Schneider or whoever
6 it is, Siemens, PLC's and it has all these other things,
7 which you didn't know when you wrote the requirement,
8 and you still have to deal with.

9 MR. STURZEBECKER: Yes, I think I've heard
10 the paradox put that a unit testing isn't complete until
11 you've done the test, your system test. So, that is the
12 same idea.

13 CONSULTANT HECHT: Yes, so, that is why --
14 and failures don't occur hierarchically. They're real
15 nasty that way.

16 MR. STURZEBECKER: Right.

17 CHAIRMAN BROWN: Section 8.2.1 of the --
18 under -- that is details of master test plan.

19 MR. STURZEBECKER: Section 8.2.1., you're
20 in the standard, right?

21 CHAIRMAN BROWN: Page 39, well, it's PDF
22 page 39, but it talks about examples of possible
23 additional test levels include security, usability,
24 performance, stress, recovery and regression, and
25 that's under test processes, including definition of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 test levels.

2 Small systems may have fewer levels of
3 tests, it's just a statement, that combining e.g.
4 combining system and acceptance tests.

5 Then there is another paragraph, under
6 Section 9, level test plans, that makes a similar
7 statement, "Other possible examples of levels include
8 operations, installation, maintenance, regression and
9 non-functional levels, such as security, usability,
10 performance, stress and recovery."

11 "Any one of these may be more than one level
12 for it," so, in other words, there is reference to a
13 series, including recovery testing.

14 CONSULTANT HECHT: Right, I mean, it's in
15 there, certainly.

16 There are a lot of words in this document,
17 but the question is, what -- is the Reg Guide going to
18 be silent, saying that that's all you need to -- you know,
19 human interface, recovery, security, it's all kind of
20 one basket of non-functional issues, which -- all of
21 which are important. Failure recovery.

22 CHAIRMAN BROWN: Are you in -- are you
23 thinking that -- of more specificity, in terms of what
24 modes of recovery are?

25 CONSULTANT HECHT: I am thinking that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 particularly with respect to safety systems, which don't
2 have, for example, or don't have many human interfaces.
3 Failure recovery testing is more of an issue.

4 You want to be able to rely on your residual
5 heat removal system, when --

6 CHAIRMAN BROWN: Isn't that a higher level
7 than our software documents? I mean, this is --

8 CONSULTANT HECHT: Well, it -- failure --
9 being able to tolerate and recover from failures goes
10 all the way from requirements through implementation and
11 into tests.

12 Surely, it's a higher level. But here,
13 we're talking about tests, and so, in this test -- in
14 the test plans, are you going to be dealing, or should
15 you -- or should this -- should there be a position, or
16 should the position be enhanced, and I thought it might
17 be in that Position 4, I think, that you address it.

18 MR. STURZEBECKER: And make that a specific
19 item in there, okay.

20 CONSULTANT HECHT: In the system test.

21 MR. STURZEBECKER: As a system test, and
22 so, include the attribute there, okay.

23 CHAIRMAN BROWN: If I can find the page, I
24 had a question somewhere in here.

25 MR. STURZEBECKER: All right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Here it is. I don't know,
2 where are we, before I screw something up here? We're
3 still on -- we're on page 35?

4 MR. STURZEBECKER: Right, page 35.

5 CHAIRMAN BROWN: Helps a little bit.

6 MR. STURZEBECKER: We were talking about--

7 CHAIRMAN BROWN: Okay, before we change --

8 MR. STURZEBECKER: Testing tasks.

9 CHAIRMAN BROWN: Well, let's finish the Reg
10 Guide. I'll ask this when you get into the IEEE stuff.

11 MR. STURZEBECKER: Okay.

12 CHAIRMAN BROWN: Because I happen to have
13 the IEEE standard open, also.

14 MR. STURZEBECKER: Okay.

15 CHAIRMAN BROWN: That's where my question
16 comes.

17 MR. STURZEBECKER: Okay.

18 CHAIRMAN BROWN: So, I won't digress.

19 DR. ARNDT: If I can make a comment?

20 MR. STURZEBECKER: Yes, I did, I've got
21 Myron's comment down.

22 CHAIRMAN BROWN: Yes, I think what I've
23 got, we've got failure recovery testing covered in the
24 Reg Guide. Is that kind of the --

25 MR. STURZEBECKER: That is kind of the --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (OTR comments)

2 MR. STURZEBECKER: Right, and that should
3 be maybe an addition to Regulatory Position 4.

4 DR. ARNDT: Yes, we understand the comment
5 and we'll look at it.

6 CHAIRMAN BROWN: Okay.

7 MR. STURZEBECKER: Okay, so, G, we have a
8 new testing task, testing -- yes, testing task, I'll get
9 it straight, sorry, and that is Regulatory Position 7.

10 We took an exception to Table C.1. No, it's
11 not an exception, I'm sorry. It's an addition.

12 We were pointing to C.1, Table C.1, saying
13 that, you know, that the Clause 5 has some very good
14 information in that one particular section there, that
15 tabular form, but it's -- and it's amplified better in
16 Table C.1, for test tasks, inputs and outputs. There
17 is more information. So, we're suggesting to look at
18 that.

19 H, test tool documentation, this is an
20 exception that we took to Clause 6.3, that if a tool is
21 used, for any kind of electronic validation methods, and
22 so on, that the information could be stored on the tool,
23 but it really needs to be available for easy access to
24 -- for basis of any safety conclusions.

25 I, we have the secure analysis position

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 again, and this one requests that in the life cycle that
2 you find in Table 3 of Clause 5, that it's considered
3 up front with the acquisition supply planning and
4 concept. It's only noted after that.

5 So, we just asked that it's considered
6 throughout the life cycle, and J is the new Annexes that
7 were added to this particular Reg Guide. That is slide
8 35.

9 So, what changed in the standard? Okay,
10 so, the new process improvements start with Clause 5,
11 or 4 and 5, and those are the first two bullets there,
12 adding integrity and this life cycle focus, and there
13 is compatibility with again, this software project life
14 cycle plan.

15 The second two -- last two bullets there
16 reflect to Clause 8 and 9, and that is improving the test
17 documentation and retesting and resolution in 8, and
18 then Clause 9 talks to an overview methodology, and that
19 one included a --

20 CHAIRMAN BROWN: Where are you on your
21 bullets?

22 MR. STURZEBECKER: I'm right here, the
23 fourth bullet of the -- or the sub-bullet in here.

24 CHAIRMAN BROWN: Okay.

25 MR. STURZEBECKER: So, I'm kind of stepping

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 through it pretty quickly.

2 So, starting the next section there.

3 CHAIRMAN BROWN: Yes, I have a question on
4 that.

5 MR. STURZEBECKER: Okay.

6 CHAIRMAN BROWN: Clauses 4 to 7, there is
7 the listing of integrity levels.

8 Table 2, this is where you've assigned the
9 test process -- excuse me, that's not right.

10 Yes, test processes, and right before that,
11 you had defined all these consequence based integrity
12 schemes, four, three, two, one levels.

13 But Table 2 says, okay, these are all of the
14 things you're suppose to do for the various integrity
15 levels.

16 So, catastrophic, if you know where that is,
17 catastrophic says there is a whole list of stuff, master
18 test plan, there is about 10 or 12 items. Critical has
19 the exact same items.

20 MR. STURZEBECKER: Yes, they do.

21 CHAIRMAN BROWN: Marginal has exactly the
22 same items, but -- what?

23 CONSULTANT HECHT: I think it has a couple
24 less.

25 CHAIRMAN BROWN: Well, it might, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 negligible has a few less. I really didn't notice a
2 difference between the marginal. Maybe there is one
3 less.

4 But it just seemed to me -- not a whole lot
5 of difference at all, between catastrophic and critical.
6 Did I miss something?

7 MR. STURZEBECKER: No, that is --

8 CONSULTANT HECHT: There are 11 items for
9 both.

10 MR. STURZEBECKER: Right.

11 CHAIRMAN BROWN: In both of them? I think
12 they're identical. I started trying to read them up and
13 down and -- maybe it's not important, but you all decided
14 that catastrophic is the one you're going to deal with.

15 MR. STURZEBECKER: We could always go to
16 level five, which in influenza. You know what that is,
17 yes?

18 CHAIRMAN BROWN: I have no idea.

19 MR. STURZEBECKER: Bazer talks about level
20 five, where --

21 CHAIRMAN BROWN: Who does?

22 MR. STURZEBECKER: Bazer.

23 CHAIRMAN BROWN: Okay.

24 MR. STURZEBECKER: And influenza, and you
25 know, it's --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: That's good, he's got a
2 sense of humor then.

3 MR. STURZEBECKER: Yes, he does. I mean --

4 CHAIRMAN BROWN: He or she.

5 MR. STURZEBECKER: If I'm changing all my
6 micro-processes --

7 (OTR comments)

8 CHAIRMAN BROWN: Let's stay away from the
9 flu.

10 MR. STURZEBECKER: Okay.

11 CHAIRMAN BROWN: I am only worried about
12 what is in this document. So, I mean --

13 MR. STURZEBECKER: Yes, you're right, it is
14 the same.

15 CHAIRMAN BROWN: But is this out of
16 something -- is this out of a document in terms of
17 defining these, or you all didn't invent these?

18 MR. STURZEBECKER: I didn't invent these.

19 CHAIRMAN BROWN: I mean, IEEE pulled these
20 in. Their consensus standard developer pulled all
21 these in from a source? I didn't go back to the source,
22 but I presume they are defined somewhere.

23 MR. STURZEBECKER: Right.

24 CHAIRMAN BROWN: And it was decided that
25 these two levels would be roughly the same?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STURZEBECKER: That is correct.

2 CHAIRMAN BROWN: In terms of, they both
3 have to do everything?

4 MR. STURZEBECKER: True.

5 CHAIRMAN BROWN: Okay, all right. I
6 thought maybe I was missing something.

7 MEMBER STETKAR: I think if you get into it,
8 there are subtle differences. You have to do everything
9 for critical, but there might be subtle differences, in
10 terms of the level of -- I forgotten what terms they used.

11 CHAIRMAN BROWN: You have to go into it?

12 MEMBER STETKAR: Aggressiveness, if you
13 will.

14 MR. STURZEBECKER: That may be right, but
15 I agree with you, that some of the --

16 CHAIRMAN BROWN: It's another level down,
17 is where the difference is, is what you're saying.

18 MEMBER STETKAR: Yes.

19 MR. STURZEBECKER: Yes.

20 CHAIRMAN BROWN: But I didn't see it
21 anywhere, and I didn't care, since we said we're going
22 to use level four. Is it defined? Is the difference
23 between these -- no, I'm not interested. Let's keep
24 going here.

25 MR. STURZEBECKER: Okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Because it's beside the
2 point.

3 MR. STURZEBECKER: Okay.

4 MEMBER STETKAR: I care, because I looked
5 for --

6 MR. STURZEBECKER: You can see the
7 difference between 3 and 2, where they 'x' out
8 differences between the three and four, when you apply
9 it to the life cycle, but you know --

10 CHAIRMAN BROWN: That's all right, let's
11 keep on going. You've answered my question and they're
12 the same, and I'll go on from there.

13 MR. STURZEBECKER: Okay, so, this next
14 section here is -- talks about the new integrity level,
15 the process -- test process, test documentation.

16 So, that is Clauses 4 through 7. It kind
17 of sets up how you use this new document, and then you
18 have the master test plan, Clause 8, and it rolls through
19 with updates, minor updates to the original level test
20 plan, level test design, level test case and level test
21 procedure and the test log there.

22 The master test plan also -- master test
23 report was also adjusted. They do have -- like I
24 mentioned before, the new anomaly reports and this level
25 interim test status report, and there was a particular

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 topic.

2 I can't remember, another test from the
3 original one that they had deleted, and I can't remember
4 the name, but it was -- but this is pretty much the suite
5 of documents that you're going to follow through.

6 So, when you look at graphically, what has
7 changed, you can see from -- literally, from three, four,
8 five and six, from the original, drops into the center,
9 and they're only modified to keep up with what is going
10 on with the new integrity levels and the procedures and
11 so on, the processing that goes on.

12 So, there is the new anomaly report. So,
13 the test incident report was deleted, and that is the
14 one I was trying to recall, and also, this test item
15 transmittal report, which is gone also.

16 So, they've probably been re-morphed into
17 this, right here, the whole anomaly report and the level
18 test report.

19 So, this is the new standard, and you can
20 see, it's significant, the amount of changes.

21 How it applies to the Reg Guide, well,
22 excuse the spaghetti there, but what you see up front
23 here from A to E, was what we covered earlier, talking
24 about the integrity level. We added level -- Regulatory
25 Position 1, the addition of the level test level and the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 AR documentation to the Regulatory Position 1.

2 We have the software documentation, the
3 deviation policy that we wanted the licensees to
4 realize, and that comes -- that is back over in the master
5 test plan and test documentation, we don't allow
6 anything lower than the level four.

7 We had a couple public comments, I think I
8 told you about. The one, I put -- I put one in here that
9 we didn't agree with, and the comment was to complete
10 the documentation after operations, and it was kind of
11 like, well, I don't think that is workable.

12 You're really suppose to be setting up the
13 test plan and running things, and having this complete,
14 as you're working on the software.

15 Then F through I are those new sections, we
16 just stepped through, everything from integrity level,
17 testing tasks, the tool documentation and the secure
18 analysis.

19 CHAIRMAN BROWN: Very quick question.

20 MR. STURZEBECKER: Okay.

21 CHAIRMAN BROWN: You talked -- I was trying
22 to find comments, public comments that had actually --
23 and this is an extensive change to the standard, with
24 a lot of extra stuff for folks to comply with, even though
25 it's a "consensus standard" among those who develop the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 standard.

2 Doesn't necessarily mean that those who
3 have to use it are going to be as consensus oriented.

4 Quite frankly, I didn't have time to take
5 each and every comment and see where it fell into this
6 slot.

7 But you all have an awful lot of resolutions
8 which were 'do not agree'.

9 MR. STURZEBECKER: Yes.

10 CHAIRMAN BROWN: And I didn't disagree with
11 you not agreeing. You're perfectly -- that is what
12 you're here for.

13 MR. STURZEBECKER: Correct.

14 CHAIRMAN BROWN: But with these added
15 requirements, with which they have been asked to comply,
16 you know, all these red ones on the left-hand side, that
17 you're retained, I mean, you didn't take exception to
18 any of those, other than snippets, if any, in the Reg
19 Guide.

20 MR. STURZEBECKER: True.

21 CHAIRMAN BROWN: So, was there significant
22 disagreement with what the consensus standard was
23 requiring, and they were saying -- I couldn't figure it
24 out, from looking at the public comments, let's put it
25 that way.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STURZEBECKER: Well, a lot of the
2 public comments from one particular -- excuse me.

3 A lot of the comments were from one
4 particular originator, that was duplicated in every
5 standard.

6 CHAIRMAN BROWN: Okay.

7 MR. STURZEBECKER: So, I'd say almost 90
8 percent, 80 percent --

9 CHAIRMAN BROWN: We're being --

10 MR. STURZEBECKER: -- it was very easy to
11 say, 'do not agree'.

12 Now, there were points, I'll give credit
13 that, you know, "Add a comma here, fix this sentence,"
14 true, true, and there were some true points that -- like
15 we had the one that came in and said, "Why are you
16 starting with Clause 8 and 9, or referring -- discussing
17 items? Why don't you start at the beginning, at Clause
18 4 in the Reg Guide?"

19 You know, it was -- it's a question of how
20 you want us to begin things, and I think just from looking
21 at the guide and having to rearrange it, it was easier
22 to keep the structure we had up front, show the small
23 changes, and then add the integrity of the new positions
24 afterwards.

25 CHAIRMAN BROWN: So, the comment was, what

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 relative to organization and where they were located?

2 MR. STURZEBECKER: Yes, it's --

3 CHAIRMAN BROWN: Okay.

4 MR. STURZEBECKER: -- tomato/tomato kind
5 of thing, I guess.

6 CHAIRMAN BROWN: I'm not objecting. I was
7 just wondering.

8 MR. STURZEBECKER: Yes, I understand your
9 concern.

10 CHAIRMAN BROWN: They're just telling you
11 what the flavor was, that they weren't -- they weren't
12 as technical as they were, organizational. Is that it?

13 MR. STURZEBECKER: Correct, I don't think
14 they were as technical as -- you know, one comment was
15 very -- was right on, spot on. We did not have the same
16 statement about Annex B in this Reg Guide, as compared
17 to 1.168, and he was right on.

18 So, we repaired 1.168, took the same
19 paragraph that is in 1.170, and put in 1.168. So, now,
20 we're -- so, they caught it -- it was a good catch.

21 CHAIRMAN BROWN: Okay, so, that was a
22 consistency issue?

23 MR. STURZEBECKER: Yes, that was, from our
24 point --

25 CHAIRMAN BROWN: Not a technical

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 disagreement, a consistency issue?

2 MR. STURZEBECKER: Yes, right, it was more
3 of trying to put all six Reg Guides on the wall, and make
4 sure that they all connect, you know.

5 So, that is kind of how we went through this.
6 I mean --

7 CHAIRMAN BROWN: And you answered my
8 question.

9 MR. STURZEBECKER: Okay.

10 CHAIRMAN BROWN: I'll hold off now. Go
11 ahead.

12 MEMBER BLEY: I have a question, and I don't
13 mean this to be factitious, either.

14 There are the six Reg Guides. We're going
15 through our fourth one. You had to do a lot of work to
16 show the mapping, to show how these all work out.

17 I'm just wondering in a practical sense, for
18 the poor guy who is trying to apply these to a software
19 development program, how does it work?

20 I mean, just keeping track of them here to
21 discuss them, it's confusing enough. Have we
22 over-burdened them with requirements that you can't
23 quite -- I think we've developed the software instead
24 of tracking requirements.

25 I'm just a little -- it seems a little

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 overwhelming to me.

2 MR. STURZEBECKER: They follow it. I
3 mean, NASA follows it. Dan Derrico follows it for the
4 railroad, and he has to hold, and he always -- like I
5 was telling Myron earlier, that you have programmers
6 coming in, saying, "Here is the fix. You know, here is
7 the patch."

8 MEMBER BLEY: Yes.

9 MR. STURZEBECKER: He's not even done with
10 the full test, the test case, and they want to put the
11 patch in, but what association did that change, and he
12 refuses.

13 So, you have to -- he's one of the very few
14 people that -- you know, well, that holds to that point,
15 you know. It's a matter of ethics, I guess and --

16 MEMBER BLEY: Well, we've already --

17 MR. STURZEBECKER: He's doing this right.
18 I don't know what to say.

19 MEMBER BLEY: We've all seen the problem
20 with just throwing the patches in, as they come.

21 MR. STURZEBECKER: Yes, exactly.

22 DR. ARNDT: I think a broader answer to that
23 question is, that if you think of the one and two man
24 mom and pop software development shops --

25 MEMBER BLEY: Ain't going to do it.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 DR. ARNDT: -- this is a variable, but we're
2 applying this to safety grade nuclear software.

3 So, it's a large -- generally, it's a large
4 organization, with people who are specifically
5 dedicated to the V&V processes, to the testing
6 processes, to the architectural processes, and we want
7 that.

8 We want people to really have all this stuff
9 under their thumbs, as the old music term goes, and know
10 this stuff inside and out, on a routine basis, because
11 they're doing it every day.

12 When they're upgrading a process, to go back
13 and look at these recommendations, guidance documents,
14 so, yes, it is a lot of stuff and there is a lot of
15 guidance there, but we don't think it's there just to
16 be there. It there for a reason. We want them to be
17 able to understand this, as it all holds together.

18 That is another point. When you look at a
19 specific clause or a specific recommendation, you need
20 to look at it in the context of this entire area.

21 All these guidance work in conjunction with
22 each other, and when the consensus committees put them
23 together, they put them together knowing that there was
24 another guide for requirements and another guide for
25 V&V, and another guide --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: And those committees all
2 include the people who are having to use it.

3 DR. ARNDT: Exactly.

4 MR. STURZEBECKER: There is -- you can see,
5 when you go through this, you see the changes going on,
6 and you see them changing certain terms for another term,
7 just to fall into play.

8 So, what I've been trying to get across is
9 that it is refined, much more refined, which makes it
10 easier. It's getting better.

11 MEMBER BLEY: Go ahead.

12 MR. STURZEBECKER: Okay, so, the next
13 several slides are the specifics that have changed, and
14 so, if you have any questions at this point on them.
15 I'll just keep going through, and getting the next guide.

16 There is the public comments and the
17 specific changes to IEEE.

18 CHAIRMAN BROWN: Back that up again.

19 MR. STURZEBECKER: Okay, sure. There was
20 the one about the notice to --

21 CHAIRMAN BROWN: Oh, that is the public --
22 I'm sorry, I was looking at -- what page am I on here
23 anyway?

24 MR. STURZEBECKER: There is that noted
25 contradiction that I mentioned before.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 CHAIRMAN BROWN: Well, we've already been
2 through 39, I'm sorry, I lost pages.

3 MR. STURZEBECKER: You want to go to 39?

4 CHAIRMAN BROWN: No, no, we finished that.

5 MR. STURZEBECKER: Yes.

6 CHAIRMAN BROWN: So, okay, I lost track,
7 that's all.

8 MR. STURZEBECKER: All right, not hard to
9 do.

10 MEMBER STETKAR: I'm sure glad you're
11 leading this.

12 CHAIRMAN BROWN: Why, did you lose track?

13 MEMBER STETKAR: No.

14 CHAIRMAN BROWN: You didn't want to sound
15 as bad as me, in other words?

16 MEMBER STETKAR: Yes.

17 CHAIRMAN BROWN: Go ahead, Karl.

18 MR. STURZEBECKER: Okay, 41, no other
19 standard changes there. More detail. We've covered
20 some of these already.

21 Then finishing up at the end there, and this
22 is -- I was telling you, all the different new -- the
23 new sections.

24 CHAIRMAN BROWN: Anything else? So, I
25 read them all. Did you? Of course you did.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: You bet you. I was given
2 an assignment.

3 CHAIRMAN BROWN: I didn't ask you, Dennis.
4 Are you okay, up to here?

5 MEMBER BLEY: Yes.

6 CHAIRMAN BROWN: Okay, just wanted to make
7 sure we didn't move on until we had everybody here.

8 MEMBER STETKAR: Interpret 15 seconds of
9 silence as current, as concurrence.

10 CHAIRMAN BROWN: Yes.

11 (OTR comments)

12 MR. STURZEBECKER: Okay, 1.169. This
13 standard is configuration management.

14 Again, the Reg Guide follows directly
15 through it, endorses it.

16 The objective of my -- I thought I probably
17 wrote that out, yes.

18 So, this is one of the tools that works with
19 the software project life cycle process.

20 In 1074, in support of the section that I
21 mentioned before, it still maintains a small set of
22 activities about configuration management.

23 So, that is how they connect. So, this --
24 there wasn't a lot of changes to this standard.

25 They did add this release management and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 delivery, which it's -- you know, as a topic itself, it's
2 more about keeping track of whatever the next software
3 revision that you have, whatever you've developed. So,
4 that has been added, and the monitoring and recording
5 of the different iterations -- yes, for pre-existing
6 software, that was another topic added to the standard.

7 I think -- I wonder, we already have that
8 in our guide, but let me get further into it.

9 MEMBER STETKAR: Karl, before you flip back
10 to the old --

11 MR. STURZEBECKER: Yes.

12 MEMBER STETKAR: -- pretty picture there,
13 this is just for my own edification.

14 There are statements in the standard that
15 talk about reconfiguring the configuration items and
16 delivering new baselines of the software.

17 What defines a new baseline? Is that just
18 somebody saying, "Today, I shall have a new baseline,"
19 or is -- the reason I ask is that there is a lot of
20 discussion in here about configuration management and
21 testing and verification validation of changes to the
22 baseline, which implies exactly what it says, a change
23 to something that I call a baseline.

24 Now, there's been experience that I make a
25 change to a baseline. If I call that new thing now a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 baseline, and I make another change to that, I now have
2 two changes from the original, and maybe each change
3 individually doesn't do anything, and I don't recognize
4 necessarily, the compound effects of sequential
5 variations, and I am never forced to go back and look
6 at that, if all I'm doing is examining incremental
7 changes to something that I have arbitrarily called a
8 new baseline.

9 So, is there something -- what is a
10 baseline? This is -- I don't know. I mean, the concern
11 that I tried to elaborate on, the concern --

12 MR. STURZEBECKER: We had quite a big
13 discussion, and I can't -- I'd have to pull up my notes.

14 But on what -- what was the definition of
15 the baseline in this, and you know --

16 MEMBER STETKAR: I couldn't find the
17 definition, or maybe I missed it.

18 MR. STURZEBECKER: Yes, I mean, we had it
19 there. I don't think --

20 MEMBER BLEY: The standard of that
21 conversation tone, on this one, that we --

22 MR. STURZEBECKER: It was like a year and
23 a half ago, but we went back and forth on this, and we're
24 just -- we kept to the IEEE.

25 You know, it -- yes, it's subject to change

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 control. You know, I don't -- I don't know what else
2 --

3 MEMBER BLEY: I remember having a
4 discussion on this issue, in fact, during one of the
5 design certs, I think it was, and one of the folks
6 described that when you have a change, and I think that's
7 in here, you can't just look at locally, at the impact
8 of that change.

9 You have to look globally, and make sure
10 you're not interfering with some other parts of this
11 overall software, that would have an effect, and I --
12 at least it seemed to me, at that time, that if, in fact,
13 you look globally each time, you --

14 MR. STURZEBECKER: And I think --

15 MEMBER BLEY: -- you're kind of covered,
16 but certainly, it's an issue that can work -- can we stack
17 these up and get a --

18 MEMBER STETKAR: Yes, I know why I didn't
19 find it. It's not in this. All this standard does it
20 -- it says, "The following additional terms are used in
21 a manner consistent with their definition or usage in
22 IEEE EIA 12207.0."

23 MR. STURZEBECKER: Right.

24 MEMBER STETKAR: You know, and one of those
25 terms is baseline, and I didn't have the other one.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STURZEBECKER: I think the idea of the
2 down -- upward and downward adapt -- well, it used to
3 be tailored, but adaptation is the same idea that we have
4 in Regulatory Position 9, with the acceptance criteria.

5 You know, it's got to be traceable up and
6 down, you know, whatever the baseline where it started,
7 and you continue forward, you still got to be able to
8 track where it came, and I'm sure, you know, in the
9 original -- this model here for the process, we talked
10 about the organization, or asset processes that they
11 have.

12 That becomes part of the company, you know,
13 it's followed through with a new term -- or what do they
14 call it? What is the best way to -- examples like
15 standing on giants.

16 You slowly keep progressing, and you know,
17 the company grows. It has new assets. There was a
18 baseline. There was an original first Model-T, but it
19 expanded from there.

20 CONSULTANT HECHT: Can I talk about what
21 I've seen in terms of Defense contractors?

22 There is a baseline and the baseline is
23 basically the reference configuration of the product.

24 Now, baselines are established through a
25 change -- by -- they are kept under control of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 management, or management functions. It's called
2 configuration management. There is a change control
3 board, and at some point, the CCB can declare a
4 configuration to be a new baseline.

5 So, there are old baselines and new
6 baselines, but with respect to Dennis's comment about
7 handling things globally, the CCB, the change control
8 board, that is their responsibility, to look at a change
9 and consider the global impact, and that is why it's a
10 board, it's suppose to consist of all of the stakeholders
11 who have knowledge of the individual aspects and could
12 say, "Wait a second, making this change is going to
13 adversely affect the interests and my constituency," or
14 something like that.

15 CHAIRMAN BROWN: But who is a stakeholder
16 in this case? Is this other design guys, that have other
17 parts of the code, as part of the overall software?

18 CONSULTANT HECHT: It could very well be.

19 CHAIRMAN BROWN: It could very well be, but
20 do they go out to every plant that has -- or every
21 industry that has some of that software installed, and
22 their stakeholders and they get to have a voice in what
23 the new baseline is going to be?

24 CONSULTANT HECHT: Well, there is suppose
25 to be a person on the board, who might say that, and you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 know, a baseline is something -- is a development
2 activity. So, it's not necessarily for all of the
3 installed base.

4 But it's certainly -- I'll give you an
5 example.

6 In the Defense industry, you have people who
7 are not part of the program themselves, but who are
8 potential users and we say, "We want to remove the number
9 of operational positions from six to two," because we
10 want to save money.

11 Then a member of the user community might
12 say, "Wait a second, what is that going to do to us?"

13 We need those operational positions, and
14 they should have representation on the CCB.

15 So, that would be an example of when that
16 happens, but the CCB is basically, program and product
17 specific.

18 CHAIRMAN BROWN: This is very unsettling.

19 MR. STURZEBECHER: A baseline could be just
20 you know, PLC, here is your normal operating system.
21 It's been working for 15 years, and now, we're going to
22 upgrade.

23 CHAIRMAN BROWN: No, a position -- this is
24 way too -- put this down to where people -- where the
25 rubber hits the road.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Okay.

2 CHAIRMAN BROWN: The only software of
3 interest is what the operators have to deal with in their
4 plant, and knowing that it is the right one, whatever
5 the right one is.

6 Another plant could have another right one.
7 The guy who designed the stuff could be mucking around
8 with it back at his design facility, and that might be
9 his right one. But it's not the right one for Plant A,
10 B or C, and that is a terrible problem to have to deal
11 with, and we face that in spades, in our program, when
12 we were trying to define it.

13 I'll just tell you the story, because that
14 makes it -- that brings it -- the chickens home to roost
15 here.

16 The very first design we were doing, there
17 was a micro-processor in every instrument. There were
18 no integrated divisions or what have you.

19 It was an aircraft carrier, and it was a
20 CVN-72, the Abraham Lincoln, first installation of a
21 complete reactor plant control system. This is not
22 classified. So, I can talk about this.

23 There were 29 instruments in this one main
24 control cabinet, consisting of about -- individual
25 instruments, of which there were about seven or eight

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 different varieties, pressure, temperature, level,
2 flow, a couple of others, two or three, I'll just throw
3 a few other ones in there someplace, okay, and this is
4 by one vendor.

5 We had seven different computing --
6 computer CPU cards, and because it was the first, we had
7 that stuff installed in the -- for the test program in
8 the shipyard, and people were developing -- there were
9 problems identified, as we started into a test program,
10 and therefore, we had to develop code changes, software
11 revisions to take care of them.

12 I kept seeing all this traffic of paper
13 going back and forth from vendors, through our prime
14 contractor, down to -- I mean, all approved, you know,
15 people writing letters on them and all, and I finally
16 asked the lead guy on the project, I said, "How does the
17 operator know that he's got the right stuff installed
18 in his cabinet?"

19 He's being asked to run tests with equipment
20 that is suppose to be operational.

21 "Oh, it's all in the drawings." Okay, so,
22 I gave him the afternoon, to identify what the version
23 of the code was suppose to be in each and every one of
24 those instruments.

25 I asked this, it was right around lunch

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 time, and I said, "If it's so easy, you go tell me what
2 it is."

3 Two weeks later, they had still not been
4 able to identify on the drawings for the operator, to
5 what -- as to what the versions were.

6 So, we called a stop to all the testing. We
7 revised, went down and looked at what was installed,
8 revised the technical manuals to include a table that
9 identified what the programmer will read on the ship was,
10 and how it was labeled. It had a part number, and that
11 table, now, the operator could go to the manual, open
12 it up and look at the table, pull out the instrument,
13 look at the number, look at the table.

14 If it didn't agree, he had unsatisfactory
15 software and had to stop, and that would -- they're still
16 -- I don't know, at least when I retired, and the last
17 time I talked with my guys, this was about a month and
18 a half ago, the people I used to work with, they said
19 they're still doing it that way.

20 Now, that doesn't mean that the Abraham
21 Lincoln's version was the same as -- who is the 73, George
22 Washington? Whatever the next carrier was.

23 And so, there was -- there were nine
24 carriers, all from the 68 up through the 77, that all
25 had -- 10, I guess, that all had that initial -- well,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 no, the 77 had an advanced version.

2 But there were five or six or seven, two
3 plants each, and each one of those was controlled by a
4 specific version, and that was -- I didn't care what the
5 vendor had. It was what the operator had to use that
6 day, and what that ship had in place, and it didn't have
7 to be the same ship to ship.

8 We would probably upgrade them. I mean, if
9 we had fixed something in one carrier, we'd then bring
10 in a new set of plans, take them down to the other
11 carriers, take the old ones out, under change control
12 modes, you know, okay, all three -- authorized ship
13 changes.

14 Put the new ones in, run the test and that
15 -- now, they had the same as -- you know, Ship B had the
16 same as Ship A.

17 That was work that had to be -- and I'm
18 talking -- you talk about baselines, it was control,
19 right down to the -- now, in the factory, in order to
20 keep the vendors honest, we literally a master set of
21 software and it had a version on it, whatever was
22 approved by headquarters, that became the version.

23 Now, they could go do things with that, but
24 they could never modify that. You would have
25 engineering versions, that they probably had a different

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 label, totally separate from that, and they would never
2 incorporate and upgrade until they'd been through all
3 their testing.

4 That was one of the things of -- that
5 concerned me, about reading the list, is I don't know
6 how that translates into -- and I had 180 reactor plants,
7 actually, I only had about 120 at the time, that actually
8 had these things installed, and it was a very effective
9 way to do it.

10 Now, I am not advocating you guys go do that,
11 or else you've got a different way to -- I'm just saying,
12 it's very important, and you're at the beginning right
13 now, on safety systems.

14 I mean, how many plants have safety --
15 Ocone? Who else?

16 MR. STATTEL: There is probably a couple
17 dozen.

18 CHAIRMAN BROWN: Okay, that have reactor
19 protection systems that are micro-processor based
20 safety systems?

21 MR. STATTEL: Yes, there is about a dozen
22 Eagle 21 systems.

23 CHAIRMAN BROWN: Oh, that one is -- yes,
24 that's old.

25 MR. STATTEL: Micro-processor.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Yes, but it's the same.
2 It's the same principle, yes, I agree with that. I
3 understand that.

4 But you know, it just -- this almost applies
5 in my mind. The only words in here that refer to users
6 is the one line, control of software documentation, user
7 operating and maintenance documents. That is at the --
8 to me, I read that, that is the guy in the plant.

9 MR. STATTEL: Yes.

10 CHAIRMAN BROWN: The only one that is worth
11 anything is that one. All the rest of them, they weren't
12 addressing it, and to me, I'm just passing this on.

13 MR. STURZEBECKER: Right.

14 CHAIRMAN BROWN: I mean, it's up to the NRC,
15 to make sure that the plants have -- are not operating
16 with a version of code that has not been through all of
17 its hoops, and that it -- that an operator -- if you
18 walked into Oconee tomorrow, you ought to be able to go
19 down to their engineer, chief engineer and say, "What
20 version of code do you have in there, and how do you make
21 sure that is what is really in there," and within 20
22 minutes, they ought to be able to tell you that, and if
23 they can't, then you've got a system that is not working.
24 That was my conclusion.

25 MR. STURZEBECKER: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: So, that is my lecture.
2 Now, I don't know how to get that in to here.

3 MR. STURZEBECKER: Well, I think because in
4 the standard, if you go to the standard on page -- well,
5 it's 3.3.7 --

6 CHAIRMAN BROWN: You mean IEEE Standard?

7 MR. STURZEBECKER: Yes, the IEEE Standard
8 828.

9 CHAIRMAN BROWN: Let me get out of the
10 comments, and then I'll do that.

11 MEMBER STETKAR: Three-three-seven, did
12 you say?

13 MR. STURZEBECKER: Yes, 3.3.7, and it's
14 called 'release management delivery', and this is what
15 is new to the standard, compared to the old one, and it's
16 about build release delivery of the software product,
17 documentation that was formerly controlled, you know,
18 master copy, and it goes on.

19 CHAIRMAN BROWN: What section is that
20 again?

21 MR. STURZEBECKER: It's on 3.3.7.

22 CHAIRMAN BROWN: Page ten?

23 MEMBER STETKAR: Of the PDF?

24 MR. STURZEBECKER: Should be page ten.

25 CHAIRMAN BROWN: I'll go in there now.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 That is sub-contractor control and vendor control?

2 MR. STURZEBECKER: It should say --

3 CHAIRMAN BROWN: Three-three, page 10 of
4 the PDF file?

5 MR. STURZEBECKER:
6 Three-point-three-point-seven.

7 CHAIRMAN BROWN: Of 828?

8 MR. STURZEBECKER: Yes.

9 CHAIRMAN BROWN: Okay, additional release
10 management?

11 MR. STURZEBECKER: Yes, release management
12 delivery. The idea here is to control your different
13 versions of software. It's only a --

14 CHAIRMAN BROWN: Yes, but where?

15 MR. STURZEBECKER: -- a paragraph, but yes,
16 it's a start.

17 CHAIRMAN BROWN: The software control
18 management program? I forget the acronym.

19 MR. STURZEBECKER: Yes.

20 CHAIRMAN BROWN: The build release and
21 delivery, that is at the design agent.

22 MR. STURZEBECKER: Yes.

23 CHAIRMAN BROWN: Well, I'm interested --
24 where does the -- how does the operator -- I mean, who
25 keeps track of what each plant has? Who wants to --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. ARNDT: When the product is delivered
2 to the plant, it comes under the plant's quality
3 assurance program --

4 CHAIRMAN BROWN: I agree with that.

5 DR. ARNDT: -- and all this configuration
6 management interfaces through the vendor, through this
7 stuff that Karl is talking about right now.

8 They have version control of their version,
9 and they interface with the vendor, or their contractor
10 or their subcontractor or whoever.

11 So, they know what's in their plant and the
12 vendor knows what's in their plant, and when the -- there
13 is a requirement to update change whatever, and it's a
14 handshake.

15 MR. STATTEL: I can speak a little bit to
16 the operational plants.

17 The version control is a condition of an
18 operability determination for those systems.

19 So, for example, Oconee, actually, when
20 they do their channel functional tests, their quarterly
21 tests on their system, they're required to make sure that
22 all the set points are correct and they're also required
23 to verify that the correct versions of those -- of the
24 software is actually installed into that system.

25 CHAIRMAN BROWN: So, that have that as a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 quarterly check?

2 MR. STATTEL: They do.

3 CHAIRMAN BROWN: Do all -- do the other --
4 like, Eagle 21 do the same -- is that in the -- is that
5 an NRC requirement?

6 MR. STATTEL: Really, it's addressed on a
7 plant by plant basis, right, so, I can't answer that
8 across the board.

9 However, that is our expectation. When we
10 perform our reviews and -- because we have specific
11 evaluation criteria for operation and maintenance
12 phases of the development process, right, and the
13 question -- the types of questions we ask to address
14 those criteria are what you're saying.

15 Normally, we address those, like for
16 Oconee, we address those in inspection space.

17 So, the regional inspectors went out to the
18 plants, look at their procedures, and we had -- in our
19 safety evaluation, we had provided the region with
20 inspection criteria, to make sure that in their
21 procedures, in their operability determinations,
22 they're ensuring that the correct software is installed,
23 right, and that they maintain that configuration
24 management aspect in operation.

25 DR. ARNDT: Charlie?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STATTEL: And during maintenance.

2 DR. ARNDT: The design control part of
3 Appendix B --

4 CHAIRMAN BROWN: Appendix B of?

5 DR. ARNDT: It's the quality assurance --

6 CHAIRMAN BROWN: Oh, you're talking about
7 the overall --

8 MR. STATTEL: General criteria.

9 CHAIRMAN BROWN: Okay.

10 DR. ARNDT: This is one small piece of that
11 whole effort for the design control of the entire plant.
12 It's special for software because of the unique aspects
13 of software.

14 But there is an expectation that the plant
15 will maintain design control of the entire design of the
16 plant.

17 This is one piece of that, and as Rich
18 mentioned, when the inspectors, either the residents or
19 someone from the region goes out and looks at particular
20 areas, like digital controls, that is something they
21 look at.

22 We actually get inspection reports on this.
23 The inspectors are doing this.

24 MR. STATTEL: In addition, I'll just
25 mention this.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 There is also a self-diagnostic feature in
2 several of these systems, that we've evaluated, which
3 basically locks the software version in at the time of
4 installation and start up, and honestly, if the software
5 version changes, the system will self-identify that and
6 actuate alarms and basically, it just self-identifies
7 configuration changes.

8 CHAIRMAN BROWN: I never trusted that.
9 That is why we always stamp the chip.

10 MR. STATTEL: Right.

11 CHAIRMAN BROWN: Am I right then? Thank
12 you.

13 MR. THORP: I'd like to echo what Steven was
14 saying, that ever licensee, every plant has to have a
15 design configuration management program, design control
16 program, and keep up to date, their drawings,
17 specifications and all the numbers associated with every
18 aspect of their plant designs, especially in the safety
19 related areas.

20 It also happens to behoove them, to maintain
21 design control in areas that are not safety related,
22 simply because of -- for financial reasons.

23 So, their interactions with the vendors are
24 key, and certainly, in aspects like digital
25 instrumentation and controls, with the major vendors,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 they view this as hugely important.

2 So, there is a number of different things
3 these operators "do" to ensure that things are good with
4 them, including their own set of audits and evaluations
5 of the suppliers.

6 Our inspectors, looking at a major I&C
7 upgrade, get a very thorough look at the initial, if you
8 want to call it baseline installation of the digital
9 instrumentation control package, and then following
10 that, regional inspectors and resident inspectors, just
11 doing their Appendix B routine inspection of processes
12 and sometimes special team inspections for design
13 control, etcetera, get a chance to examine how the
14 controls are being implemented at every licensee.

15 CHAIRMAN BROWN: That is all --

16 MR. STATTEL: We have --

17 CHAIRMAN BROWN: That is awfully global,
18 and I am not -- I don't -- vendors, I'm really more
19 interested in the plant, in the plant, in the plant, and
20 I'm talking about a baseline at a plant.

21 It could anywhere -- whatever the latest
22 version is, is a baseline, and it's not amorphous. It
23 should have a specific version or something assigned to
24 it, and I've heard the terminology, you know, all these
25 plants get controlled by drawing.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Well, that is what we thought in the nuclear
2 program, all of our configurations were controlled by
3 drawings. Turned out, that didn't work.

4 MR. THORP: It's not that we haven't had
5 problems in the industry.

6 MR. STATTEL: Well, we share those same
7 concerns.

8 CHAIRMAN BROWN: Well, pipes just don't get
9 changed and valves don't get ripped out, for the most
10 part. It's kind of hard to do that without somebody
11 knowing what is going on.

12 MR. THORP: Right.

13 MEMBER BLEY: Happens more in our world
14 than your's.

15 MR. STATTEL: But we have the same
16 concerns, because when we issue our safety evaluation,
17 anything that happens after that, it's out of control,
18 you know, it's out of our view.

19 So, for instance, with Oconee, we put into
20 place, inspection items for the regional inspectors to
21 follow up, because we issue our safety evaluation and
22 that system was still --

23 CHAIRMAN BROWN: No, I understand.

24 MR. STATTEL: -- that system was still in
25 Germany.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: I fully agree. I
2 understand that, and I don't -- I know, I understand
3 that.

4 MR. STATTEL: But when it got delivered to
5 the plant, when it got installed in the plant, there were
6 specific inspection items for our inspectors to go make
7 sure that those -- the correct software was re-installed
8 into that system.

9 MR. THORP: I would liken that to sort of
10 our operating plant equivalent to a new plant
11 construction ITAAC, essentially, where we're doing
12 inspection items to ensure that what was installed was
13 what we approved in the SER.

14 MR. STATTEL: Right.

15 CONSULTANT HECHT: Can I ask a question?

16 CHAIRMAN BROWN: Now, you can ask your
17 question, yes.

18 CONSULTANT HECHT: Okay, well, you know,
19 just to refocus the discussion here.

20 There is configuration control and
21 configuration management and the establishment of
22 baselines, which is being done by the software
23 developer, in order that he knows what he has, that a
24 version that came from the team doing the PLC operating
25 system and the one doing the interpreter of the function

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 blocks, and you know, the protocol stacks, all of which
2 have different version numbers.

3 But together, that was the baseline for PLC,
4 and that is what I think is what we're dealing with in
5 this entire set of standards and Reg Guides here, as
6 opposed to a different configuration management
7 problem, which is a very important configuration
8 management problem, which is actually, what's installed
9 at the plant, as opposed to what is being tested and
10 developed and specified at the factory.

11 CHAIRMAN BROWN: Yes, but that also -- yes,
12 I understand that, but it also depends on the rigor.

13 For instance, if you've built one plant and
14 installed a set of software, couple years later, another
15 plant gets built, and another version, that has been
16 tested for that plant is put in, but it's the same
17 platform, just a later version of the software.

18 It might be two or three versions later than
19 the one that was in Plant A, and then two years later,
20 you get another one. That might be two or three versions
21 later than what was in Plant B.

22 Now, you need to go back and make a change
23 to Plant A, and they say, "Oh, we've got this approved
24 version," but the mapping between A and D is critical
25 to know that something has not been left out, or some

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 nuance in Plant B didn't have a different software loop
2 installed that's not necessary for Plant A, and that can
3 -- that is -- so, starting, you know, with the control
4 at the vendor's plant is not necessarily the right
5 starting point for determining whether you've got the
6 right stuff. It can create a problem.

7 I know that personally, because with having
8 multiple stuff go out, we did have -- ran into the case
9 where we -- had made a software change and didn't quite
10 catch it at -- the change, because there was a nuance
11 of mechanical plant changes, that required something
12 else to be done, in the third one down, and we didn't
13 pick it up, and we found out a different way.

14 Fortunately, it was not a problem, but we
15 found it in testing, when we finally put it in, that
16 something didn't do what it was suppose to do, before
17 we went to operation.

18 So, this is -- well, I don't know, we're
19 beating a dead horse, and I just was really interested
20 in having a little bit of the stuff, relative to how they
21 do it.

22 It will be interesting, Rich, if somebody
23 went down spur of the moment, just went down to one of
24 the plants, walked in and tell me, "Show me now, what
25 version of software you're suppose to have and prove to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 me that it's right," and if they can't do that within
2 20 or 30 minutes, then there is a problem.

3 CONSULTANT HECHT: Yes, I agree.

4 CHAIRMAN BROWN: So, I'll stop with this.
5 Go ahead.

6 MR. STURZEBECKER: So, there have been
7 quite a few additions, did some word changes in the
8 standard. I'm trying to remember what they were.

9 They were, like I was telling you before,
10 adaptation was now the new word versus 'tailoring' and
11 they took the word 'audit' out and used 'evaluation'.
12 Little things like that, and I think it's trying to line
13 up with the software process.

14 As I recall -- or mentioned before, we've
15 got the release management and delivery sub-clause, and
16 the 3.3.7, which has also been added to the Reg Guide.

17 The guide is kind of following it -- along
18 with the standard. It's kind of enhancing that, by
19 pointing to that part of the standard.

20 What else do we have here? I guess just
21 overall, you know, there -- like I said, there is just
22 minor changes to this standard.

23 The Reg Guide expands with -- you know,
24 we're supporting that whole release management idea, and
25 I think this standard also kind of pointed out that it's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 -- acknowledges that it -- that you can use this for
2 pre-existing software.

3 Okay, so, specifically what changed in the
4 guide?

5 Regulatory Position 4. I have to look that
6 up and see.

7 We added a paragraph, repeating the
8 expectations of the release management delivery. We
9 included configuration management of contractually
10 developed or qualified software products. There was a
11 public comment.

12 CHAIRMAN BROWN: Where is the part of the
13 contractually developed? I missed that somewhere in
14 here.

15 MR. STURZEBECKER: Yes, I have to look,
16 myself.

17 CHAIRMAN BROWN: Is that under four?

18 MR. STURZEBECKER: Let me get my --

19 CHAIRMAN BROWN: Under the configuration
20 management? I was looking for -- oh, I found it, never
21 mind.

22 MR. STURZEBECKER: Got it?

23 CHAIRMAN BROWN: Yes, no, it's the last
24 paragraph.

25 MR. STURZEBECKER: Last paragraph, okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I have my sheets here.

2 There was a public comment about deleting
3 a statement or a line item in our guidance.

4 That was -- it's under configuration
5 management Regulatory Position 4, we had a sub-bullet
6 there, that said, "Commercial software items that are
7 safety software -- or safety system software," and it
8 was sort of repetitive because that is what the
9 inclination of the opening phrase is, you know.

10 I mean, you're looking for the minimum set
11 of safety system software activities, so, why are we
12 repeating it? So, we took that out.

13 In the same token, we added item I, there,
14 control building and release and delivery of products,
15 and we had this whole idea of release management.

16 CONSULTANT HECHT: Can I ask, with respect
17 to item four, one of the things I didn't see there was
18 what we dealt with, with 829, and that is there is test
19 documentation that wasn't considered as a configuration
20 management asset, at least not directly.

21 MR. STURZEBECKER: That's interesting.
22 That's a good point.

23 CHAIRMAN BROWN: Say that again.

24 CONSULTANT HECHT: Well, basically, the
25 test plan and the test cases and the test results that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 go with a particular version should be kept with that
2 version and should be under CM.

3 MR. TRUONG: It's covered under 4D, sir,
4 the Clause 4D says 'control of software documentation'.

5 There is just some examples of documents
6 that were used by operating maintenance --

7 MS. ANTONESCU: Can you state your name,
8 please?

9 MR. STURZEBECKER: Okay, so, it is.

10 MR. TRUONG: My name is Tun Truong from the
11 Office of New Reactors.

12 CHAIRMAN BROWN: Can they -- can the Court
13 Reporter hear him?

14 MR. TRUONG: It is in there, too. It's
15 covered.

16 CONSULTANT HECHT: You say that it's
17 covered under item D, and I see 'user operating and
18 maintenance documents'.

19 MR. TRUONG: Right, it goes by examples.
20 Those are examples.

21 CONSULTANT HECHT: Well, perhaps test
22 documentation should be put in there explicitly.

23 MR. STURZEBECKER: Right.

24 CONSULTANT HECHT: That's what you want to
25 be able to do with a version, if you want to be able to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 evaluate and recover that version, is you want to be able
2 to run test cases on that documentation --

3 MR. TRUONG: I don't disagree. Those are
4 controls. That is under control.

5 MR. STURZEBECKER: Okay, so, to Regulatory
6 Position 4 and --

7 CHAIRMAN BROWN: Four-D.

8 MR. STURZEBECKER: Four-D, test
9 documentation. Do you want to get explicit, and say,
10 "Just all of them," or just test cases?

11 CONSULTANT HECHT: Well, if --

12 MR. STURZEBECKER: Just an example, but --

13 CONSULTANT HECHT: If you say test
14 documentation, that relates directly to 829, and then
15 --

16 MR. STURZEBECKER: Perfect.

17 MEMBER STETKAR: Doesn't that --

18 CONSULTANT HECHT: -- that negotiation --

19 MEMBER STETKAR: Doesn't number six cover
20 that?

21 CHAIRMAN BROWN: Position 6?

22 MEMBER STETKAR: Position 6, under
23 documentation.

24 CONSULTANT HECHT: Position 6?

25 MEMBER STETKAR: "Test software

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 requirements, designs or codes used in testing, test
2 results used to quantify the software -- qualify
3 software."

4 CONSULTANT HECHT: I see it, yes.

5 MR. TRUONG: Yes, sir.

6 MEMBER STETKAR: Six F and G?

7 CHAIRMAN BROWN: Does that cover your
8 concern?

9 CONSULTANT HECHT: I'm just looking for the
10 test cases.

11 MEMBER STETKAR: It doesn't specifically
12 say test cases.

13 CONSULTANT HECHT: And the test programs,
14 so --

15 MR. STURZEBECKER: Test results, test
16 software requirements, code design used in testing.

17 CONSULTANT HECHT: So, this is all of these
18 -- the set up that you need to do the test, but not the
19 test cases and test procedures.

20 MR. STURZEBECKER: Okay.

21 CONSULTANT HECHT: And results, so it is --

22 MEMBER STETKAR: And analyses and results
23 used to qualify the software.

24 CONSULTANT HECHT: Yes, it can go in either
25 place, and maybe it's implied there, but I would venture

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to say that a diligent applicant and a diligent regulator
2 could miss that, if they just --

3 DR. ARNDT: We'll look at that, to see
4 whether or not it --

5 MR. STURZEBECKER: Right.

6 DR. ARNDT: -- a revision is necessary.

7 MR. STURZEBECKER: Yes, I noted it.

8 CHAIRMAN BROWN: So, that was either under
9 F or G or H, of six, 6F, G or H, is what you're talking
10 about, for the test cases.

11 MR. STURZEBECKER: All right.

12 CONSULTANT HECHT: And under 4D, if you
13 just say 'test documentation'.

14 MR. STURZEBECKER: Okay, and since we're on
15 six, yes, okay.

16 So, I removed that duplication that was
17 under -- it's letter C there I was on, about removing
18 the duplication from the public comment.

19 Okay, letter D, Regulatory Position 7, this
20 is where we added a paragraph that references the EPRI
21 topical report. It kind of fit right into that
22 location.

23 CHAIRMAN BROWN: Now, you all have agreed?
24 I'm trying to remember. That EPRI report actually
25 defines a method for dedicating that commercial grade

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 software or something?

2 MR. STURZEBECKER: Yes.

3 CHAIRMAN BROWN: A process, a way to do
4 that, and you all have written an SER on that?

5 MR. STURZEBECKER: SER, in July 17, 1997,
6 I believe it was, yes.

7 CHAIRMAN BROWN: Okay.

8 MR. STURZEBECKER: According to the
9 endorsement, that's the endorsement date, and that's the
10 public comment --

11 CHAIRMAN BROWN: Nothing has changed since
12 then?

13 MR. STURZEBECKER: Nope, yes, since then.

14 CHAIRMAN BROWN: Well, I know it hasn't
15 changed.

16 MR. STURZEBECKER: Yes.

17 MEMBER STETKAR: In the real world.

18 CHAIRMAN BROWN: Yes.

19 MR. STURZEBECKER: It's baseline. Okay,
20 and E is the public comment about that, so, that was added
21 to that part also, and then we have the new Regulatory
22 Position 12 release management and delivery, which we
23 know is 3.3.7., and last is the Annex A and B.

24 So, there is minimum changes to the 2005
25 version of 828.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 There is a Clause 324, where they talk about
2 management of software configuration management, costs,
3 surveillance and activities that go in -- that are
4 involved with doing your configuration management.

5 It also added 3.3.7, which we talked about
6 just a second ago, and I already mentioned about the
7 tailoring, adapting and audit to the evaluation, so,
8 very small changes.

9 So, I could put this one all together in one
10 sheet. You can see, there is minor revisions here,
11 between overview and definitions from introductory,
12 Appendix becomes an Annex, and then you go from the 2000
13 version, 2005 version that is.

14 You can see that we have quite a few changes
15 of our's, just to highlight the whole idea of this
16 building -- controlling the building release of delivery
17 of products, this release management delivery idea, and
18 we put the public comments there too, that we talked
19 about, minor, and the one section there on F, the section
20 we added for that.

21 It's pretty basic. You know, it's nothing,
22 and these are the specific changes, to try to detail
23 every change that was there, almost every change, if
24 there's any questions on them.

25 MR. TRUONG: Karl, really, I didn't have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the baseline definition, but maybe the members are still
2 interested in learning what the actual definitions are,
3 I can read it out loud.

4 CHAIRMAN BROWN: What?

5 MR. STURZEBECKER: The baseline
6 definition.

7 MEMBER STETKAR: Good, yes.

8 MR. TRUONG: Do you want me to read it out
9 loud to you?

10 CHAIRMAN BROWN: That would help, if you
11 read it slowly.

12 MR. TRUONG: Slowly, yes, sir.

13 MEMBER STETKAR: With sufficient clarity
14 and volume to be heard.

15 CHAIRMAN BROWN: Which IEEE standard is
16 this?

17 MR. TRUONG: This is 610, sir.

18 CHAIRMAN BROWN: Okay, I don't have it on
19 here.

20 MR. TRUONG: So, the first part is the
21 specification or product that has been formally reviewed
22 and agreed upon, and that thereafter, serves as a basis
23 for further development, and that can be changed only
24 through a former change control procedure, like through
25 CCB, like was mentioned earlier in this discussion.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 The second part is, a document or set of such
2 documents formally designated and fixed at a specified
3 time during life cycle of a configuration item and note
4 baseline, plus approved changes when that baseline
5 constitutes the current configuration identification
6 for that particular item.

7 CHAIRMAN BROWN: That's it?

8 MR. TRUONG: Yes, sir.

9 CHAIRMAN BROWN: There is nothing in there
10 that says it must have a unique identifier that
11 characterizes it and ensures that its variation is
12 different from any earlier baseline definition?

13 MR. TRUONG: I think that falls under the
14 configuration identification.

15 CHAIRMAN BROWN: Is that -- did you say
16 that, as part of that discussion?

17 MR. TRUONG: Well, it's part of it. I said
18 baseline plus the approved changes from this baseline
19 constitute the current configuration identification.

20 CHAIRMAN BROWN: Say that again, the
21 current configuration?

22 MEMBER STETKAR: Identification.

23 MR. TRUONG: Baselines, plus the approved
24 changes from those baselines, constitute current
25 configuration identification for that particular

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 software item.

2 CHAIRMAN BROWN: Hold it. That's not a
3 unique identifier. That just says all the things they
4 did internally, will define it as a specific --

5 MR. TRUONG: I'll get to it. In real
6 world, like when I was doing software at Motorola, we
7 used a --

8 CHAIRMAN BROWN: That's suspect, right
9 away, by the way.

10 MR. TRUONG: Fair enough.

11 CHAIRMAN BROWN: I'm just teasing you.

12 MR. TRUONG: We used conversion control
13 software that helps us enumerate our software changes,
14 you know, major/minor releases, and so, when you make
15 changes to software, you can increment the minor changes
16 or the point changes you want to do, and that is
17 everything -- that's all tracked and controlled, through
18 a software tool, for example.

19 So, that's how one can do it in real life.

20 CHAIRMAN BROWN: Okay.

21 MEMBER BLEY: But I think this doesn't
22 really help with issue John was raising.

23 MEMBER STETKAR: No, it doesn't, but that's
24 -- I understand. Thank you.

25 CHAIRMAN BROWN: Just my point. Whatever

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the position was, the one we had, on my earlier question.

2 A unique identifier. If you have a version

3 and you go in and change one line of code --

4 MR. TRUONG: Yes.

5 CHAIRMAN BROWN: -- it gets a new version.

6 MR. TRUONG: That's correct.

7 CHAIRMAN BROWN: If you change the flowing

8 point to fixed point numbers for whatever, for some

9 particular function, that gets a new version.

10 MR. TRUONG: Right.

11 CHAIRMAN BROWN: And that's what I mean by

12 --

13 MR. STATTEL: I think you're getting into

14 areas that are going to vary one, by the technology being

15 implemented and two, by the actual application and the

16 process being used.

17 As an example, at the plant, one of the

18 software baselines that we maintain was, the unique

19 identifier was based on the time of compilation of the

20 code, to the second, right.

21 So, you could re-compile the exact same

22 source code, the exact same source files, and come up

23 with exactly the same file, but it would have a different

24 time.

25 CHAIRMAN BROWN: But it would have the same

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 file name.

2 MR. STATTEL: Same file.

3 CHAIRMAN BROWN: But a different -- that's
4 bad.

5 MR. STATTEL: But it would be different.

6 CHAIRMAN BROWN: No, no, no, no.

7 MR. STATTEL: It's a different file.

8 CHAIRMAN BROWN: It should have a different
9 file name.

10 MR. STATTEL: Right, but it's unique.

11 CHAIRMAN BROWN: It's like me getting an
12 email from you one day with an attachment, and you send
13 me another one five minutes later with the same
14 attachment. Is the new one new, or is it the old one?

15 MEMBER STETKAR: Everybody does that?

16 CHAIRMAN BROWN: Pardon? I know,
17 everybody does that. Drives me crazy.

18 (OTR comments)

19 MR. TRUONG: It doesn't necessarily work
20 that way.

21 For like, if you have a C++ file, because
22 you use that many times, but let's say you have a 'Hello
23 World' program, okay.

24 CHAIRMAN BROWN: A what?

25 MR. TRUONG: A 'Hello World' program. It

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 doesn't -- you don't distinguish by the file name. You
2 distinguish by the version number.

3 CHAIRMAN BROWN: It's a unique identifier.

4 MR. TRUONG: Yes.

5 CHAIRMAN BROWN: I am not -- a unique
6 identifier for it, for any change. That's all I'm
7 saying, and not a time stamp, but a -- you know, it's
8 because you could have a different time stamp.

9 It's just like if I download a file from
10 somebody today, it's time stamped in my folder for today.

11 Tomorrow, if somebody sends me the same --
12 a slightly different file with just the same file, it
13 can even be the same file, and not -- and I load it
14 someplace else, it's going to have a different date, but
15 I put it in two different places.

16 MR. STATTEL: That's a different
17 identifier.

18 CHAIRMAN BROWN: No, but they're the same
19 file. All the --

20 MR. STATTEL: The point is --

21 CHAIRMAN BROWN: It's implied as the same.

22 MR. STATTEL: The point is, it is required
23 to have a unique identifier, however that is handled.

24 CHAIRMAN BROWN: Well, I just never saw a
25 unique identifier anyplace in here, for configuration

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 management.

2 MEMBER BLEY: The date and time on your
3 email is not a good one, but there are places -- some
4 systems in which the date is part of the identifier.

5 CHAIRMAN BROWN: When you download an
6 attachment, it puts a date by it.

7 MEMBER BLEY: You better not be using that
8 as any part of your identifier.

9 CHAIRMAN BROWN: Then you get another email
10 later, okay, and if you download that attachment again
11 and happen to put it in a different location, now, you're
12 trying to figure out whether it's the same thing, and
13 if you look at the file size, even that won't be the same.

14 So, anyway, I'm just complaining. Unique
15 identifier, it's not in here anywhere. That's all, for
16 any change.

17 MEMBER STETKAR: Can I go back to my --

18 CHAIRMAN BROWN: Yes.

19 MEMBER STETKAR: -- and I apologize for
20 asking what a baseline is, but Myron helped, and if I
21 go back -- and as I understand it, at this high level,
22 the configuration control board can say, "Yay, I
23 declare a new baseline today," for whatever reason they
24 decide to do that. It seemed like a good idea a the time.

25 I understand that, and that the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 configuration control board, as you explained it, has
2 the responsibility for this, if I can call it a global
3 perspective, on the accumulative effects of changes,
4 either within an evolution of a specific baseline or
5 across different baselines, as they evolve, and I
6 understand that.

7 According to the standard, it says that,
8 "The plan shall identify each configuration control
9 board and its level of authority for approving proposed
10 changes." So, it establishes that.

11 The configuration control board may be an
12 individual or a group. That's a little different from
13 your characterization as a multi-disciplinary set of
14 stakeholders, because this says -- this seems to say one
15 person, who is omniscient can, in deed, control this
16 whole process.

17 It goes onto say, "Multiple levels of
18 controlled CCB's may be specified, depending on the
19 degree of system or project complexity and upon the
20 project baseline involved."

21 "When a multiple CCB is used, the plan shall
22 specify how the proper level is determined for a change
23 request, including any variations during the project
24 life cycle."

25 But as I read this, the standards says one

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 person can sit there and say, "Yes, I think it's time
2 for a new baseline, and yes, I think I thought about
3 everything, and everything is okay."

4 CONSULTANT HECHT: I submit to you that
5 that is the most common form of configuration management
6 and control.

7 MEMBER STETKAR: Okay.

8 CONSULTANT HECHT: And I'll give you an
9 example.

10 MEMBER BLEY: It doesn't really matter.
11 What we're interested in is what will be configuration
12 control in a nuclear power plant, using this software.

13 MEMBER BLEY: Right, right, but I'll just
14 give you an example of what I'm talking about.

15 If I am part of a software development team,
16 and I'm responsible for a particular unit, and
17 typically, units are assigned to individuals, and
18 somebody says to me, "All right, it's time to do -- it's
19 time to gather up all the components. We're going to
20 start our first level of integration testing.
21 Everybody, give me their stuff."

22 Then I might be working on something, which
23 is a later release, or some -- or my next version, but
24 I'm going to give them the version that I completed last
25 Friday, and I might call that Version G or Version I,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 and I'm going -- and I better know exactly what that
2 version is, and I better keep it in a safe place, so if
3 they want to look at it two months later, I can say what
4 Version G or Version I is.

5 That can often be done using a configuration
6 management system, where you know, something like
7 subversion, which is commonly used, but it can be done
8 that way, and it's often done that way.

9 That is not what you would use for having
10 the executable operational software on the safety system
11 at a nuclear power plant, but it might be used in the
12 course of developing a software component of that
13 nuclear power plant.

14 MR. TRUONG: Mr. Stetkar, what's the
15 question, sir, about the CCB?

16 MEMBER STETKAR: The basic concern is what
17 process in this configuration management, and I don't
18 care whether it's CCB's or whether we call it a baseline
19 or a revision or what alphabet soup we give to anything,
20 is that if software is being modified over time, I've
21 installed a set of software in my plant, and I've given
22 it a name. It's 'Ralph Revision 1.2.7' whatever
23 alphabet soup you want to give to it, and I understand
24 what that means, it's installed in my plant.

25 As soon as I start operating my plant, I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 discover that there are things that need to be changed
2 in that software, and in deed, the software supplier has
3 discovered things that I don't even know about, that need
4 to be changed, because I didn't even -- I wasn't even
5 aware of them.

6 So, changes start, and a change is made from
7 what I have to address a particular concern, and it fixes
8 that concern.

9 Another change is made to address another
10 concern, and it fixes that concern.

11 However, changes A and B together can create
12 a third problem, that I didn't even think about. I
13 didn't think about it. The software developer didn't
14 think about it, and that's my concern is, who oversees
15 that process?

16 CONSULTANT HECHT: There should be
17 integration --

18 MEMBER STETKAR: That compound effect of
19 changes, and I don't care if I declare a new baseline
20 every time I change a single bit of coding. I could do
21 that. I mean, I don't know why I would do that. I could
22 do that.

23 CONSULTANT HECHT: There should be, as part
24 of the configuration management process, there should
25 be integration testing, particularly when you're taking

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 components from various vendors, and we see it all the
2 time.

3 MEMBER STETKAR: But as long as you only
4 test it to make sure that the fix -- each individual fix
5 that you put in, solved the problem that you thought
6 about trying to solve, does the integration testing pick
7 up the compound effects of change number one and change
8 number two, creating a problem that you didn't know
9 about?

10 CONSULTANT HECHT: IEEE 829 and Reg Guide
11 1.171, I guess it is. It's got to be considered
12 together, but --

13 MR. TRUONG: But typically, they also
14 perform --

15 CONSULTANT HECHT: By the way, that's the
16 importance of the test cases that I was talking about
17 before.

18 MR. STURZEBECKER: You're supposed to
19 create a traceability matrix when you create your
20 process.

21 MEMBER STETKAR: Yes, but everything I said
22 is fully traceable.

23 MR. STURZEBECKER: Yes, right, but how they
24 interact, yes --

25 MEMBER STETKAR: How they interact is the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 problem.

2 MR. STATTEL: These are all very good
3 questions, and they're the very questions we ask, when
4 we evaluate their processes.

5 I don't think the answers are in the Reg
6 Guide. I think --

7 MEMBER STETKAR: The answers aren't in the
8 Reg Guide, and I was mostly --

9 MR. STATTEL: I think the answers are in the
10 actual implemented processes that we evaluate. So, for
11 example --

12 MEMBER STETKAR: But that is really
13 incumbent upon --

14 MR. STATTEL: For example, a vendor submits
15 a software program manual.

16 I would expect, when I evaluate that
17 program, I would expect that it would have the answer
18 to that, how do you process simultaneous concurrent
19 changes that are being made to a version of the software?

20 MEMBER STETKAR: Is that left up to our
21 inspectors to have that knowledge?

22 MR. STATTEL: I think a lot of it is, yes,
23 and the --

24 MEMBER STETKAR: Over time, you know,
25 because these things might occur over, you know, a five

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to 10 year period.

2 MR. SANTOS: In new plants, yes.

3 DR. ARNDT: But you also have to think about
4 this. It is -- you've got to think of this particular
5 kind of question in the context of all of this
6 requirement.

7 We have a requirement for a complete and
8 appropriate regression testing. Regression testing
9 doesn't mean, just go test the fix. It means, go look
10 at all the different functional requirements and make
11 --

12 MEMBER STETKAR: If that is -- okay, if
13 that's the way it's implemented.

14 DR. ARNDT: But that is part of the whole.
15 You can't look at -- you shouldn't look at these
16 particular requirements in --

17 MEMBER STETKAR: Isolation.

18 DR. ARNDT: -- isolation. They should be
19 part of the whole context.

20 Yes, if the regression testing, if the
21 integration testing, if the configuration management,
22 if all the different pieces aren't working correctly,
23 then you can have that problem.

24 If your hazard analysis, which should be
25 feeding into your regression testing, wasn't complete,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 then you can have that issue, and what Rich was
2 mentioning is, when you go out and evaluate this, you
3 ask those questions, well, how about this, how about
4 that, and you pull the string.

5 Well, if this hazard wasn't identified, it
6 didn't get into the regression testing, it didn't get
7 into the integration testing, it didn't get into
8 configuration management.

9 So, that is really how we try and address
10 these particular kinds of issues.

11 MR. STATTEL: And some of that, some of
12 those evaluation techniques are driven by the standard
13 review plan.

14 BTP 14 has certain criteria for that, and
15 we, as a practice in AICB, we have a standard set of
16 questions that we ask the vendors, when we perform our
17 audit activities. I just got done doing one of those.

18 MEMBER STETKAR: Okay, thank you.

19 CHAIRMAN BROWN: Okay, we're going to take
20 a break right now, since one of our members left us with
21 a minor quorum here. Fortunately, John and I are here.
22 We'll take a recess for 15 minutes. Be back at ten
23 after, 12 after, excuse me.

24 (Whereupon, the above-entitled matter went
25 off the record at approximately 2:55 p.m. and resumed

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 at approximately 3:20 p.m.)

2 CHAIRMAN BROWN: We're back in session.
3 We are re-adjourned. No, no, we are back in order,
4 excuse me, please.

5 (OTR comments)

6 CHAIRMAN BROWN: Go ahead.

7 MR. STURZEBECKER: I was going to ask if we
8 could step back just for a second, to 1.169, for Myron's
9 comment.

10 CHAIRMAN BROWN: Which one?

11 MR. STURZEBECKER: The one on test case.

12 CHAIRMAN BROWN: Which one?

13 MR. STURZEBECKER: Test case.

14 CHAIRMAN BROWN: Oh, test cases?

15 MR. STURZEBECKER: Yes, test cases.

16 CHAIRMAN BROWN: That's for 4D.

17 MR. STURZEBECKER: Tung found the section
18 in the standard that -- we do have it. You want to read
19 it for them?

20 CHAIRMAN BROWN: In the Reg Guide or in the
21 standard?

22 MR. STURZEBECKER: Standard.

23 MR. TRUONG: In the 828, the standard.

24 CHAIRMAN BROWN: Which one is that, the
25 828?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. TRUONG: Eight-twenty-eight-2005,
2 Clause 3.3.1.

3 CHAIRMAN BROWN: Hold on a second, 3.3.1.
4 We'll see if these words coalesce.

5 MR. TRUONG: Yes, sir. See, about the
6 fourth sentence down?

7 It says, "These items include outputs of the
8 process."

9 CHAIRMAN BROWN: Hold it, hold it.

10 MR. TRUONG: Holding.

11 CHAIRMAN BROWN: Okay, first paragraph,
12 fourth line?

13 MR. TRUONG: Yes, starting with --

14 CHAIRMAN BROWN: "These items include
15 outputs."

16 MR. TRUONG: So, for example, what the
17 gentleman earlier raised concern about, the
18 identification of test plans and test cases.

19 So, those are highlighted there. I'm just
20 putting it out, although it's not in our Regulatory
21 Guides, we haven't -- we have endorsed this standard
22 here.

23 CHAIRMAN BROWN: Yes, sir. Which guard
24 are you in?

25 (OTR comments)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Okay, did you find that,
2 Myron?

3 CONSULTANT HECHT: It says, "This is the
4 configuration identification."

5 CHAIRMAN BROWN: Yes, go down to the fourth
6 line.

7 CONSULTANT HECHT: Yes, I saw that, and I
8 saw that, "Controlled items may be," --

9 CHAIRMAN BROWN: "These items include."

10 CONSULTANT HECHT: Look, I'm not going to
11 argue that there are illusions to it, there are points
12 to it. I was just trying to -- there are lot of words
13 in various places.

14 This isn't a question of, can you find it.
15 This is a question of, is it there for a person of average
16 skill and ability, looking at the Reg Guide, to know
17 what's expected, and to know what to expect?

18 MR. THORP: Myron, your suggestion is it be
19 just included as one of the examples in the Reg Guide?

20 CONSULTANT HECHT: As an example. You
21 know, one of the enumerated items in either paragraph
22 four or six.

23 MR. THORP: Okay, for emphasis, I guess.
24 We will do it for emphasis then.

25 MR. STURZEBECKER: Okay, good enough.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. THORP: Thank you.

2 CHAIRMAN BROWN: All right, back to 1.168.

3 MR. STURZEBECKER: Yes.

4 CHAIRMAN BROWN: As soon as you get all your
5 stuff put together.

6 MR. STURZEBECKER: Yes, I've got to get in
7 the right order here.

8 Okay, 1.168, verification, validation,
9 review and audits.

10 The objective here is based on two
11 standards, 1012 and 1028. I have the objectives there.

12 Engage in the verification -- the V&V plans,
13 that follows the software project life cycle process and
14 to ensure an objective assessment of software safety
15 systems.

16 The second part is, "Provide expectations
17 for inspectors performing walk-thru, reviews and
18 audits," and it's based on their conduct of doing it.

19 But I wouldn't say it's just narrowly for
20 the inspectors either. It's combined together, because
21 we do use the V&V for software development.

22 It follows a common framework here with the
23 life cycle process. We did add integrity level -- or
24 it was added to the standard, and there is something we
25 should note about this.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 This is the only Reg Guide that is -- the
2 1.168, that is a Rev 1. So, it was updated in 2004. So,
3 there are not a lot of changes to it, but still, we'll
4 go through that.

5 So, we're now applying the life cycle to the
6 software life cycle and pre-existing or pre-developed
7 software, that is also kind of a highlighted item that
8 the Reg Guide picks up.

9 Here we go. So, general overview of
10 changes, we can read through this.

11 The minimum changes to the standard -- or
12 to the guide, that is. Both standards were revised and
13 some items in there.

14 Off the cuff, 1028, let me just -- there's
15 quite a few changes, but not as -- I didn't really --
16 wasn't really intending to make -- the changes that I
17 found in 1028, that the team found, really didn't
18 transfer over to the guide. They were -- we'd just
19 accept them as they were. Let's see.

20 CHAIRMAN BROWN: Let's see, what page are
21 you on, 53? Which one are you just referring to?

22 MR. STURZEBECKER: Ten-twenty-eight. No,
23 on the bullets there, I was kind of going off -- I was
24 expanding on the general idea of the changes, but it's
25 -- I don't think I have it written down here. I was kind

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 of freelancing on that.

2 CHAIRMAN BROWN: Page 53?

3 MR. STURZEBECKER: Page 53. So, the
4 Regulatory Guide, we have some exceptions and additions,
5 and they sort of reflect the same items we've seen in
6 other -- in the other Regulatory Positions, that we've
7 gone through earlier today.

8 Like, 1.170, you know, we're adding
9 integrity again. There is independence clarification.
10 I think in one of the -- well --

11 CHAIRMAN BROWN: You want to talk about --

12 MR. STURZEBECKER: Yes, I'm on the third
13 bullet.

14 CHAIRMAN BROWN: -- it now or later?

15 MR. STURZEBECKER: You know, I think I just
16 want to skip right to what the changes are, then trying
17 to, you know, run through this here, because I'm just
18 going to end up repeating myself.

19 CHAIRMAN BROWN: Okay.

20 MR. STURZEBECKER: So, if you don't -- if
21 you don't mind, just get right to it.

22 Okay, the first one, A, RP1, the original
23 title was 'software', or 'critical software' and we
24 changed it to 'software integrity'.

25 So, like I mentioned before, it's a matter

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 of mimicking what's going on with 1012 and just all of
2 the standards and the idea of introducing integrity into
3 the guidance.

4 The next one is the public comment about the
5 contradiction and -- between 1.168 and 1.170, and this
6 is where we put in that paragraph, and I believe this
7 is going to be the same comment you had in --

8 CHAIRMAN BROWN: Which paragraph was that?

9 MR. STURZEBECKER: In Regulatory Position
10 --

11 CHAIRMAN BROWN: Was it in one?

12 MR. STURZEBECKER: One.

13 CONSULTANT HECHT: It's the final
14 paragraph on page six, I think, right?

15 MR. STURZEBECKER: Yes.

16 CHAIRMAN BROWN: The long one?

17 MR. STURZEBECKER: The long one. So, that
18 was added, because the Annex B in 1012 is very similar
19 to the Annex B in 829.

20 MEMBER STETKAR: Similar, but surprisingly
21 not identical.

22 MR. STURZEBECKER: Right. So, we had the
23 same exception to that particular table.

24 MEMBER STETKAR: A similar exception, but
25 surprisingly enough, not identical.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STURZEBECKER: Yes.

2 CHAIRMAN BROWN: Are you trying to make a
3 point, that he -- do you want him to say something else?

4 MEMBER STETKAR: No.

5 CHAIRMAN BROWN: Okay.

6 CONSULTANT HECHT: I think it's about
7 configuration management.

8 MR. STURZEBECKER: Just want to make sure
9 there wasn't anything, that I didn't bring any
10 likelihood into this one. I don't think I did.

11 MEMBER STETKAR: What?

12 MR. STURZEBECKER: The likelihood comment
13 that we had in that one paragraph.

14 MEMBER STETKAR: It's in there, also.

15 MR. STURZEBECKER: It's in there?

16 MEMBER STETKAR: Yes, C.1, "The potential
17 of occurrence is likely to cause catastrophic
18 consequence with no mitigation possible, and thus, the
19 breadth or depth," the words are slightly different, but
20 the --

21 MR. STURZEBECKER: Okay.

22 MEMBER STETKAR: -- the same concept is
23 there.

24 CHAIRMAN BROWN: Should be deleted.

25 MR. STURZEBECKER: Deleted, okay, done.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Yes, because the
2 preceding sentence says, "Software integrity level
3 lower than level four is not acceptable."

4 MR. STURZEBECKER: All right, okay. The
5 likelihood, okay.

6 All right, so, we'll take care of that.

7 So, if we move onto the next letter there,
8 C, and Regulatory Position 3, we took an exception to
9 Annex F, there was a Figure F.1 there, that added three
10 blocks on the bottom, and what we were finding was there
11 is a lot of confusion from the licensees.

12 We were getting phone calls, from what I
13 understanding, to understanding this whole idea about
14 independence, and those three bottom boxes, what we're
15 saying is we don't recognize them.

16 CHAIRMAN BROWN: That was in 1012?

17 MR. STURZEBECKER: Yes, in 1012 Annex --

18 CHAIRMAN BROWN: Number 3? Pardon?

19 (OTR comments)

20 CHAIRMAN BROWN: That was in 1012, right?

21 MR. STURZEBECKER: Yes, 1012, page 103,
22 Annex F, the staff takes an exception to.

23 CHAIRMAN BROWN: Okay, at 103, Annex F?

24 MEMBER STETKAR: Is that true? Do you have
25 it?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: Yes.

2 MEMBER STETKAR: The picture?

3 CHAIRMAN BROWN: We're trying to decode it.

4 MR. STURZEBECKER: Okay.

5 CHAIRMAN BROWN: On the top three
6 relationship boxes?

7 MR. STURZEBECKER: Right, the bottom
8 three.

9 CHAIRMAN BROWN: Effort? Okay, so, those
10 bottom three, you throw out?

11 MR. STURZEBECKER: Right, we threw out
12 development staff, quality assurance staff and V&V
13 staff.

14 CHAIRMAN BROWN: Okay, I'll ask my question
15 here.

16 After they go through and -- the first
17 paragraph, where it says -- I guess the standard allows
18 some reductions in independence, somewhat, and then you
19 go on in the second paragraph to say, "Any organization
20 which reviewer is performing the verification should be
21 -- should not be part of the design organization's
22 development efforts, should utilize independent
23 organizational structure with regard to technical,
24 financial and managerial independence," which it -- the
25 standard gives you some wiggle room on that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STURZEBECKER: Right.

2 CHAIRMAN BROWN: And then in the next
3 paragraph you say, "However, regardless," it doesn't say
4 'however', by the way, it just says, "Regardless of the
5 approach, the applicant has the ultimate
6 responsibility," and if you read the next three or four
7 sentences, which effectively says, "Well, if you really
8 don't want to do it the way we tell you to do it, you
9 can tell us some other way you're going to do it."

10 That's the way I read the first three
11 sentences of the third paragraph.

12 MR. STURZEBECKER: The third paragraph,
13 okay.

14 CHAIRMAN BROWN: Yes, it says, "Regardless
15 of the approach selected," so, the first sentence
16 upwards says, "Hey, look, you've got to have
17 independence in both technical, financial and
18 managerial independence."

19 MR. STURZEBECKER: Yes.

20 CHAIRMAN BROWN: Well, you say 'should'.

21 Okay, down here, you say, "Regardless of the
22 approach selected for a given V&V task, the applicant
23 has ultimate responsibility for adequacy. This is
24 particularly important when an external organization
25 has performed it."

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STURZEBECKER: You know what I think
2 happened on this one, when we -- we inserted this
3 paragraph, we didn't catch the second -- the third
4 paragraph was really following the first, is my guess,
5 at this point right now.

6 Why the sequencing? You know, I don't
7 know.

8 CHAIRMAN BROWN: And the last says -- this
9 says, "Thus the applicant or licensee should verify that
10 the extent of independence between the organizations
11 responsible for design is for verification and checking,
12 meets the NRC's requirements in Appendix B of 10 CFR 50,"
13 which is --

14 MR. STURZEBECKER: Yes.

15 CHAIRMAN BROWN: -- somewhat -- is not
16 quite as crisp. It just seemed to be a dichotomy between
17 the two, one paragraph and the next, that's all.

18 MR. STURZEBECKER: Yes.

19 CHAIRMAN BROWN: One case, you phrase it
20 fairly firm, in which you say -- and the other one, and
21 I'm not going to use the words I wrote down in here, okay,
22 in my notes.

23 MR. STURZEBECKER: Okay.

24 CHAIRMAN BROWN: Then it goes on and says,
25 "This independent is to be sufficient to ensure that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 schedule and resource demands placed on the design
2 process do not compromise the V&V process."

3 In other words, hey, look, we're going to
4 allow you some leeway in the financial and managerial
5 world and schedule world, as long as it -- you can provide
6 is a valid -- validation is not going to conflict -- I
7 just, you know, you insist on it, and then you say,
8 squeamish.

9 DR. ARNDT: Well, the words -- we'll look
10 at the words, but the idea is, we don't want anything
11 associated with the level of independence, including
12 managerial and financial.

13 CHAIRMAN BROWN: And technical.

14 DR. ARNDT: And technical, especially
15 technical, but including that managerial and technical,
16 to negatively influence the process.

17 If you look at the literature, as Myron will
18 tell you, there is a lot of issues associated, well, if
19 it's reporting the same manager, it has the same budget,
20 etcetera, etcetera, there is potential impact on that.

21 CHAIRMAN BROWN: Seen it happen?

22 DR. ARNDT: Yes, we'll look at the wording,
23 to make sure it's --

24 MR. STURZEBECKER: Yes.

25 DR. ARNDT: -- clearer, but the intent

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there is very specific. We want to ensure that
2 independent V&V really is independent.

3 There are lots of different ways you can get
4 there, but --

5 CHAIRMAN BROWN: Only if they're truly
6 independent.

7 DR. ARNDT: Yes.

8 CHAIRMAN BROWN: There are not lots of
9 different ways. Only if they're truly independent.

10 DR. ARNDT: Well, organizational
11 structures that can satisfy independence.

12 CHAIRMAN BROWN: You start telling me I can
13 have inter-communication between my computational units
14 in four different divisions, and there is very different
15 ways to be independent, and that's still okay, which it's
16 not.

17 MR. SANTOS: You're still further
18 constrained by your requirements of Appendix B, when it
19 comes to independence, and those are the overarching
20 ones that always, you know, need to be present.

21 So, it's in that context, that we have to
22 look at that.

23 CHAIRMAN BROWN: Appendix B is very
24 general.

25 DR. ARNDT: Yes, potentially.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: That is the problem.
2 This is very specific in paragraph two, and then you're
3 saying, "Well, you don't have to be specific, because
4 we'll let you be more general."

5 That just seems to be a contradiction in
6 terms.

7 MR. STURZEBECKER: I think --

8 DR. ARNDT: We will look at the wording to
9 make sure it is self-consistent.

10 MR. STURZEBECKER: When we were doing the
11 modifications for --

12 CHAIRMAN BROWN: I know you, Steve. I've
13 heard those words before.

14 MR. STURZEBECKER: I think when the team
15 was -- I think we were -- we'll look at it. I think when
16 we put this in, we were -- Bill, we were kind of rushed,
17 weren't we, at this point? I forget.

18 MR. ROGGENBORDT: It wasn't, no.

19 MR. STURZEBECKER: No, because I don't like
20 the way it matches now. We just didn't see it. Go
21 ahead.

22 MR. ROGGENBORDT: Good afternoon. This is
23 Bill Roggenbordt, Office of New Reactors, Division of
24 Engineering.

25 The thought behind that was that we didn't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 want to pigeon-toe the applicants or the licensees
2 organizations, to say exactly how they must be
3 structured. That is the term of 'should', between the
4 use of that, again, to your point, that you must have
5 sufficient managerial separation.

6 So, for example, in a real world situation,
7 a recent review required that when we identified that
8 the V&V organization and the design organization
9 reported to the same manager, that was deemed
10 unacceptable, and it was through our QA organization,
11 through the vendor inspectors, to verify this, you know,
12 from a technical and then also, from a QA standpoint that
13 this was unacceptable, and then they -- that
14 organization ultimately modified their organization, so
15 there was sufficient managerial separation.

16 So, the thought behind this was that you
17 didn't want to pigeon-toe or force someone into a box
18 within their V&V organization, to match what you deem
19 as appropriate.

20 So, we felt the combination of both the Reg
21 Guide, in addition to Criterion 3 design control within
22 Appendix B was sufficient to guide, and to Rich's point
23 earlier, a lot of it also goes down to the implementation
24 phase of what you're inspecting and what you're seeing
25 in an organization, in addition to what you see on paper.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 DR. ARNDT: What we're simply trying to say
2 is, we want independence, but we don't care whether or
3 not you have a Vice President of independent V&V, or some
4 other managerial structure that is independent.

5 CHAIRMAN BROWN: Your first paragraph --

6 DR. ARNDT: I understand.

7 CHAIRMAN BROWN: -- just says they should
8 be independent, managerial independence.

9 The more you say, with all these other
10 caveats, it just gets mushed up, and this does not allow
11 -- this does not allow you to evaluate their structure,
12 and do just what you just said.

13 But the other part down here, it just opens
14 it up and says, "We invite you to tell us why this
15 unsatisfactory approach is really okay."

16 MR. STURZEBECKER: I don't think that was
17 the intent.

18 DR. ARNDT: It's certainly not the intent.

19 CHAIRMAN BROWN: I know it's not your
20 intent. I'm just reading it. It's like these other --
21 you insert these extra things in here.

22 You state what you want, very clearly, and
23 then you fuzz it up a little bit.

24 MR. THORP: I think you made a good
25 observation, Charlie.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: That's right.

2 MR. THORP: This is John Thorp. I'd like
3 to say that I'm going to go over this with Karl, and we
4 will read these paragraphs and we will conduct some
5 editing to make certain that it flows logically and
6 appropriately.

7 CHAIRMAN BROWN: That's fine.

8 MR. THORP: Yes.

9 CHAIRMAN BROWN: The sooner we see that,
10 the better off I am for the -- if I can see -- if we can
11 see that within the next week or two --

12 MR. STURZEBECKER: Right.

13 CHAIRMAN BROWN: -- or it can be resolved
14 at the full Committee meeting, which is just fine also.

15 MR. THORP: But that's in June, right?

16 CHAIRMAN BROWN: What did you say,
17 Christina?

18 MS. ANTONESCU: I'm going to die, one week.

19 CHAIRMAN BROWN: No, no, no. I'm putting
20 the pressure on you.

21 I mean, I guess we could -- you know, they
22 could present that at the resolution, at the full
23 Committee meeting.

24 MEMBER STETKAR: They could do that.

25 CHAIRMAN BROWN: They could. That could

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 be a problem.

2 MEMBER STETKAR: That has been done in the
3 past.

4 CHAIRMAN BROWN: Yes. So, anyway, that
5 gives you a little bit extra, gives you a little bit extra
6 time, and that way, I don't have to think about it until
7 everybody is yelling at me, at the full Committee
8 meeting.

9 MEMBER BLEY: And then all you have to do
10 is edit your letter.

11 CHAIRMAN BROWN: No, I won't edit it. I'll
12 defer that, or I'll get it delegated.

13 Okay, that was all I had. Thank you for
14 taking that under consideration. I just didn't like the
15 kind of stroke-dance that was doing, that's all.

16 MR. STURZEBECKER: Okay, I'm going to move
17 onto letter D, and this is again, repeat of that one
18 public comment. It's the NRC's citation of the EPRI
19 topical report, and that is Regulatory Position 4.

20 In E, we added secure analysis and the
21 Regulatory Position 7A, and adding discussion about the
22 SDOE, and that is because it's referencing the clause
23 in 1012-7.7.4.

24 There is just like a minor sentence there
25 about security, but we're identifying that, okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 We'll round things out with F, the new
2 Annexes for both 1012 and 1028, I think I've got them
3 both here, minor changes.

4 Regulatory Position 8, in that position
5 with the Annex is -- we did take an exception to Annex
6 C of 1012, Table C.1. Let me get that one.

7 CHAIRMAN BROWN: You're just insisting on
8 independence across the -- across all three categories,
9 that's what I remember in the table, okay.

10 MR. STURZEBECKER: Yes, let's see. That
11 comment on G is about this change that they had put in
12 the standard in 1012, where they call it 'conditional
13 independence', and we just don't like the term, what is
14 conditional independence? So, we're back to that
15 discussion.

16 Okay, so, what changed in the standard?

17 Again, we have some re-shuffling, basically
18 just existing figures and reports, that we kind of moved
19 around.

20 In 1012, again, or as I mentioned before,
21 it provides focus on the life cycle, and it's very
22 general type changes. The second sub-bullet down here,
23 you know, we're -- that one is done.

24 It's just a general philosophy that you're
25 doing your V&V and to be performed in parallel with the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 development, and it's a task that you incorporate, as
2 you go through things, with the testing.

3 The second to the last bullet, it supports
4 the integrity level, that's been added.

5 The very last sub-bullet, like I said, you
6 know, you got current life cycle process improvements.
7 So, there is just some general overall changes that have
8 been done. Nothing -- the integrity was the biggest
9 one.

10 Then if I move onto 1028, this standard did
11 some interesting things with -- it had a table with
12 anomaly classes, and the different kinds of taxonomies
13 of failures or -- I'm not even sure what you want to call
14 it, but they deleted that whole thing. It's gone.

15 They moved their anomalies ranking over to
16 6.8. So, they kind of re-shuffled things. It's just
17 minor, and then overall, there is just some new
18 descriptions put in here and there.

19 It sort of lines up again, with the life
20 cycle orientation. Nothing significant. If there is
21 any comments on that?

22 So, this graph here, or the -- shows the
23 anomaly ranking and how it was moved over to 6.8.3. The
24 top four bullets are just general overall updates, like
25 we went over, the one, 6.5, and it added this new

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 inspection rate table.

2 So, that was put in there. We really didn't
3 have any comments on that.

4 Finally, the anomaly ranking, like I
5 mentioned before, was moved.

6 Now, if we go to 1012, you can see on the
7 left-hand side, the two different figures I was talking
8 about that were moved down below. This major change
9 with 7.6 moved into 6.1 for reporting. It was just
10 re-shuffling of things.

11 I think the most important one was the five,
12 Clause 5 with the V&V intent -- well, above that, four,
13 software integrity level updated.

14 So, this standard, again, falls in place
15 with 1074.

16 They did add, in the life cycle, a bunch of
17 security analysis tasks, and that's 5.4, and that's
18 right there.

19 That is pretty much the generic's of the
20 changes. You'll see on the bottom there, I've kind of
21 outlined the Annexes we just talked about, Annex F that
22 we need to go correct, Annex C, and Annex B.

23 So, on this slide for 1012 --

24 CHAIRMAN BROWN: Go back one, because I
25 wanted you to explain one thing to me, that I guess I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 didn't understand when I read this thing.

2 MR. STURZEBECKER: Okay.

3 CHAIRMAN BROWN: Go back one more, one
4 more. There.

5 The inspection rate table that lists -- that
6 is on page 21 --

7 MR. STURZEBECKER: Okay.

8 CHAIRMAN BROWN: -- of the standard, and
9 it's got type of documented and inspected, and then it
10 says 'inspection rate'.

11 MR. STURZEBECKER: Yes.

12 CHAIRMAN BROWN: Two pages per hour. So,
13 if a guy goes one page per hour, he gets penalized? I
14 mean, I guess I don't -- what is the purpose of this?
15 That is what I did not understand.

16 MEMBER STETKAR: It was --

17 MR. STURZEBECKER: Help me with that.

18 MEMBER STETKAR: It's just an example for
19 resource estimation --

20 MR. STURZEBECKER: Yes.

21 MEMBER STETKAR: -- basically.

22 CHAIRMAN BROWN: That is what that's for?

23 MR. STURZEBECKER: Yes.

24 MEMBER STETKAR: Yes, it's --

25 MR. STURZEBECKER: I think so, yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: If you're a manager,
2 planning one of these things, that's sort of a nominal
3 basis for estimating time and resources.

4 CHAIRMAN BROWN: That is a function of age.

5 MEMBER STETKAR: Well, or grade level.

6 CHAIRMAN BROWN: Is that software age?

7 MEMBER STETKAR: Education? Physical? I
8 don't understand the words --

9 CHAIRMAN BROWN: Okay, all right.

10 MEMBER BLEY: He introduced this as part of
11 planning, this is how you plan.

12 CHAIRMAN BROWN: Yes, okay, all right.

13 MEMBER BLEY: It was faster.

14 CHAIRMAN BROWN: When I looked at your
15 previous stuff and said -- I looked at the table and said,
16 "What?"

17 MEMBER STETKAR: Yes, it gets into age.

18 CHAIRMAN BROWN: That is highlighted.

19 MEMBER STETKAR: It gets into reading
20 speed. It gets into comprehension, for example.

21 CHAIRMAN BROWN: Excuse me?

22 MEMBER STETKAR: It gets into all of it.

23 CHAIRMAN BROWN: All right, okay, go ahead,
24 Karl. I'm sorry. I got it, now.

25 MR. STURZEBECKER: Okay, so --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (OTR comments)

2 MR. STURZEBECKER: Okay, so, we -- I didn't
3 put up 1028. and its association to the Reg Guide. There
4 weren't any, really direct changes.

5 So, I have 1012 here.

6 MS. ANTONESCU: You have it here in this?

7 MR. STURZEBECKER: What's that?

8 MS. ANTONESCU: You have it here in this
9 slide.

10 MR. STURZEBECKER: Okay, I have it twice?

11 MS. ANTONESCU: Yes.

12 MR. STURZEBECKER: Where did I put it?

13 MS. ANTONESCU: I'm sorry, I thought you
14 said 1012.

15 MR. STURZEBECKER: No, okay, yes,
16 1012-204, yes. So, I didn't put 1028 up here, yes.

17 MS. ANTONESCU: Okay.

18 MR. STURZEBECKER: So, there is the list of
19 the different changes, you know, changed the title there
20 and then the public comment that we talked about, the
21 contradiction between the Annex B of Reg Guide 1.170,
22 and then the correction we need to do for the Annex F.
23 That was those three lower boxes, and we have to do some
24 work on that. So, that has been noted.

25 Your basic public comment, coming through,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 saying the NRC citation of EPRI topical report.

2 We added secure analysis to the Reg Guide,
3 and it references those new tasks that 1012 outlines in
4 5.4, Clause 5.4, and then we have the Annex 8, which I
5 mentioned before, and finally, Table C, which is the
6 conditional independence, which we don't -- we're not
7 -- we don't accept -- we took an exception to.

8 These are the specific changes outlined.
9 If there is any comments? Questions?

10 MEMBER STETKAR: Karl, I hate to -- I was
11 going to wait until you got to this.

12 MR. STURZEBECKER: Stay here?

13 MEMBER STETKAR: Just stay right -- stay
14 there. What I'm going to ask about is nothing that you
15 had on your slides.

16 It's more just again, curiosity, and in the
17 standard, there is this nice long Table 1, that lists
18 the various V&V tasks for each activity. You know, it's
19 a companion to 5.4, or whatever, and that's fine. It's
20 kind of neat, so, I read through it.

21 MR. STURZEBECKER: Yes.

22 MEMBER STETKAR: Each activity has listed
23 for it, something called a 'hazard analysis' and
24 something called a 'risk analysis', and the specific
25 words are slightly different, I don't know why, as you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 go along.

2 But the notion is, you started early and you
3 keep continuing it, as the process evolves.

4 A hazard analysis, it says, "Analyze the
5 potential hazards to and from the conceptual system.
6 The analysis shall identify the potential system
7 hazards." This is 'shall'.

8 "Assess the severity of each hazard.
9 Assess the probability of each hazard, and identify
10 mitigation strategies for each hazard."

11 Then down under 'risk analysis' it just
12 simply says, "Identify the technical and management
13 risks, provide recommendations to eliminate, reduce or
14 mitigate the risk."

15 My question is, because people seem to be
16 struggling with identifying hazards and assessing -- it
17 says, "Assess the probability," this to me, sounds like
18 software risk assessment.

19 The outputs are reports of the risk
20 analysis, the reports of a hazard analysis.

21 Are there any examples? Have you actually
22 done inspections or reviews or audits or whatever you
23 do of these things, and do you have examples of these
24 things, because I'd really actually be interested in
25 seeing one, because --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 DR. ARNDT: Let me start and then my
2 colleagues can elaborate.

3 What you need to understand about this
4 particular standard, it's not a nuclear standard. It's
5 a broad software standard.

6 So, when they talk about software risks, in
7 this particular standard, they're talking in much more
8 general terms than what you or I would refer to as risk
9 in the nuclear concept.

10 MEMBER STETKAR: Well, okay, I'll give you
11 the risk analysis, because it doesn't say anything, at
12 all.

13 But if I go back to the hazard analysis, the
14 hazard analysis identifies all of the elements --

15 DR. ARNDT: Right.

16 MEMBER STETKAR: -- of what I call a risk
17 analysis. It says, "Identify the hazards, assess the
18 probability and identify mitigation strategies for each
19 hazard."

20 DR. ARNDT: Right, but remember, this is in
21 a general software context. So, you're not necessarily
22 talking about at a plant level or even a system level.
23 You're talking about software.

24 MEMBER STETKAR: That's why I didn't want
25 to get into -- if there are examples of what people do

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 here --

2 DR. ARNDT: Okay, now, at this point, I'm
3 going to turn it over to my colleagues --

4 MEMBER STETKAR: -- I'd be interested to
5 see it.

6 DR. ARNDT: -- to get more specifically.
7 But understand that in that context, as you hear this.

8 MR. STATTEL: Well, when I was at the plant,
9 I performed several hazards analysis, myself, and it's
10 not entirely true to say that it doesn't address the
11 plant level, because basically, it's kind of a -- I kind
12 of always viewed this as like a beefed-up FMEA type
13 activity.

14 Because we identify the effects of the
15 failure, the postulated failure, but we also take it
16 beyond that, and we postulate, well, how is the operator
17 going to respond to that particular failure? What do
18 we expect the plant response to that failure to be, and
19 what challenges, in regard to the safety analysis that
20 has been performed?

21 So, we try to make the tie back to the actual
22 Chapter 15, the safety analysis, to see if there is any
23 hazards posed by that implication.

24 MEMBER STETKAR: That sounds --

25 MR. STATTEL: And that is typically, how I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 would perform a hazards analysis, and then as far as --
2 that is identifying the --

3 MEMBER BLEY: Do you have any sense, if
4 that's common in the industry, or is that just --

5 MR. STATTEL: That's a really good
6 question.

7 MEMBER BLEY: -- what you guys do?

8 MR. STATTEL: Because hazards analysis is
9 a concept --

10 MEMBER BLEY: I mean, if people are doing
11 this --

12 MR. STATTEL: -- that is not really
13 understood in the industry.

14 MEMBER BLEY: Yes.

15 MEMBER STETKAR: But people are doing what
16 you said you did --

17 MEMBER BLEY: They'd be a lot happier.

18 MEMBER STETKAR: -- that sounds like a
19 really good process and --

20 MR. STATTEL: Right.

21 MEMBER STETKAR: -- and for a variety of
22 reasons --

23 MR. STATTEL: I can't speak for the whole
24 industry.

25 MEMBER STETKAR: I think this is --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STATTEL: But what I can say is, since
2 I've been at the NRC, I've kind of gotten to this place
3 in the evaluation process, and I -- what I see is that
4 the applicant doesn't understand what a hazards analysis
5 is, right.

6 They don't understand where they're going
7 with that, you know, what the end result needs to be,
8 and so, inevitably, what I end up doing is, you know,
9 I write RAI's or I basically push back and say, "Look,
10 you know, this is what has to be addressed on hazards
11 analysis."

12 MEMBER STETKAR: Okay, quite honestly,
13 Rich, one of the notes that I read -- that I wrote to
14 myself was, "Ghee, this sounds interesting. I don't
15 understand what they're actually doing."

16 You know, what does this really mean in
17 practice?

18 MR. STATTEL: Right.

19 MEMBER STETKAR: You've answered that.
20 You've also answered the second question that I wrote
21 to myself --

22 MR. STATTEL: Right.

23 MEMBER STETKAR: -- which is, "Is there any
24 guidance available for," --

25 MR. STATTEL: Well, I'm going to mention

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that too, because --

2 MEMBER STETKAR: -- for doing these things?

3 MR. STATTEL: -- one of the activities
4 we're currently endeavoring on is on IEEE 7.4.3.2.

5 There is an Annex in there that is
6 specifically -- basically, identifies how to perform a
7 hazard analysis --

8 MEMBER STETKAR: Yes.

9 MR. STATTEL: -- and that is currently not
10 endorsed by the NRC, and it's one of the objectives of
11 the IEEE working group, is to basically beef that up,
12 and get it to the point where the NRC can endorse that
13 as an acceptable way to perform a hazards analysis, and
14 try to clear up the fog in that area, because honestly,
15 when I was at the plant, I really recognized the benefits
16 that the hazards analysis provided, because we were able
17 to take corrective measures, change designs, things like
18 that, to really eliminate those hazards.

19 MEMBER STETKAR: Well, and if it's
20 implemented the way this says, that --

21 MR. STATTEL: Right.

22 MEMBER STETKAR: -- in the beginning, you
23 start that process --

24 MR. STATTEL: But there is definitely some
25 --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MEMBER STETKAR: -- and then move to --

2 MR. STATTEL: -- standards development
3 work that needs to proceed with that, and we're doing
4 that with IEEE working group.

5 MR. SANTOS: Dan Santos. As you know, the
6 Office of Research is also working closely with NRR and
7 NRO on the development of guidance on how to evaluate
8 a hazard analysis and some of this.

9 I think you're going to get presentation
10 later in the year --

11 MEMBER STETKAR: We have early September,
12 first week in September.

13 MR. SANTOS: Okay, well, hopefully --

14 MEMBER STETKAR: We have a meeting
15 scheduled.

16 MR. SANTOS: Hopefully, the Standards
17 Committee can also leverage that.

18 CONSULTANT HECHT: Is this digital I&C
19 hazards or nuclear hazards?

20 MR. SANTOS: Yes, digital I&C, yes, digital
21 I&C in the context of the nuclear industry.

22 MS. ANTONESCU: And the staff is coming in
23 September.

24 MR. SANTOS: Okay, good.

25 DR. ARNDT: And before you get the wrong

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 impression --

2 MR. SANTOS: Yes, we want to give you
3 examples.

4 DR. ARNDT: -- and we'll get to it in a
5 second.

6 What I started out saying is, the standard
7 is written for general software.

8 When you put it into a nuclear context, then
9 you get the expectation that it be broader.

10 We'll talk about a couple of examples where
11 it wasn't so good as what Rich has done, in his previous
12 life as a licensee.

13 The real issue and the real reason why this
14 Committee actually recommended that we look at hazard
15 analysis more completely, in the context of 7.4.3.2,
16 which is a nuclear specific standard, is that this is
17 a big challenge because, as articulated earlier, many
18 licensees interpret it in a more general software
19 context, and I'll give a couple of quick examples.

20 MEMBER STETKAR: That is a good comment,
21 because if, in deed, the NRC has a different expectation,
22 and the industry is not interpreting that consistently
23 because of mis-communication or the way that this
24 standard has been traditionally interpreted by the
25 industry -- software people --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 DR. ARNDT: Right, and the --

2 MEMBER STETKAR: -- that communication is
3 important.

4 But the other side of that, just saying,
5 "Well, we have higher expectations for nuclear safety,"
6 doesn't help, if you don't have something to point to,
7 toward an acceptable methodology.

8 MR. SANTOS: That's right.

9 DR. ARNDT: And that's why that standard
10 work is going on.

11 MR. SANTOS: Right, and we also have the
12 EMPOWER pilot initiative. We'll have the work, and we
13 have the standard as vehicles to try to do that as a --

14 MEMBER STETKAR: Yes, but again, the
15 EMPOWER initiative is still at a relatively high level.

16 MR. SANTOS: Sure, right, but it tries to
17 do what you're talking about.

18 DR. ARNDT: There is a broad requirement in
19 7.4.3.2, which is the nuclear specific software
20 standard.

21 MEMBER STETKAR: But you already said that
22 the staff has not yet endorsed --

23 DR. ARNDT: It endorses the section in
24 7.4.3.2. that says you need a hazard analysis. It
25 doesn't endorse the --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SANTOS: Yes, the Appendix.

2 DR. ARNDT: -- the Appendix, that says how
3 to do it.

4 CHAIRMAN BROWN: It's Annex D.

5 MR. SANTOS: Right.

6 DR. ARNDT: Yes.

7 CHAIRMAN BROWN: I'm looking at it right
8 now.

9 DR. ARNDT: And if you go back to the
10 letters that the Committee wrote two years ago, three
11 years ago, something like that --

12 CHAIRMAN BROWN: That we asked you to look
13 at --

14 DR. ARNDT: Right.

15 CHAIRMAN BROWN: We termed it in terms of
16 FMEA type approach.

17 DR. ARNDT: Right.

18 CHAIRMAN BROWN: To this business, as
19 opposed to --

20 DR. ARNDT: And the reason it's not
21 endorsed is that we were uncomfortable with it as a
22 recommended way of meeting the requirement, because we
23 had some issues with it. Not that it's not bad, it's
24 just that it's not complete recommended process.

25 Did you still want to hear some examples of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the not so good version?

2 MEMBER STETKAR: That's up to you. I know
3 -- I think I know enough now, at least where we are from
4 a process perspective.

5 CHAIRMAN BROWN: It's interesting that you
6 mention Annex D, because -- and this is in the -- relative
7 to computer software types, although the lead in talks
8 about abnormal and computer development requires
9 identification of hazards.

10 Abnormal conditions and events or ACE's
11 that have the potential for permitting a safety
12 function, and it -- if you go and read on through this,
13 it talks about external, as well as internal components.

14 I mean, it could be a pump. It could be a
15 valve. It could be a switch. It could be any number
16 of things, which is -- and I'm not so sure when we had
17 this discussion before, we weren't thinking more in
18 terms of software hazards, as opposed to external events
19 being fed into the software --

20 MEMBER STETKAR: I think we're talking
21 about interfaces and the --

22 CHAIRMAN BROWN: Well, a general
23 discussion, about the lack of definition and the -- that
24 there was no process for doing a hazard -- you know, a
25 step-by-step thing that gave you a general process for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 it.

2 MEMBER STETKAR: Right.

3 CHAIRMAN BROWN: And this is not
4 overwhelmingly -- I mean, it talks about that hazards
5 can result from system considerations, design basis,
6 failure modes of system components, human error, the
7 whole smear.

8 MEMBER STETKAR: But I mean, the fact of the
9 matter is, the staff has not yet --

10 CHAIRMAN BROWN: This is just general
11 hazards.

12 MEMBER STETKAR: -- endorsed this and --

13 MR. SANTOS: Right, it's a good question,
14 I'm sure, I'm speaking for Research here. So, I'm
15 looking, is there anyone from Research here?

16 MS. ANTONESCU: Norbert is coming now, but
17 he had a class.

18 MR. SANTOS: Okay, but that is a very good
19 topic to cover during that presentation.

20 MEMBER STETKAR: I mean, we certainly want
21 to cover that in September.

22 MR. SANTOS: Right.

23 MEMBER STETKAR: But I -- for the purposes
24 of today's meeting, because it just does appear
25 repeatedly with some level of specificity, more specific

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 than a line item that says, "Yes, think about the risks
2 and what you thought about them."

3 MR. ROGGENBORDT: This is Bill
4 Roggenbordt. I can speak to actual inspection
5 experience.

6 About a year ago, where we ran into this
7 issue, and part of it is through our own doing, to be
8 honest.

9 That is because when we look at somewhere
10 in the software program manual, regardless of the
11 vendor, and we say, "Okay, that, we deem as an acceptable
12 methodology, outside of what we have set up for our
13 guidance," which is totally acceptable, because our
14 guidance is one -- merely one acceptable methodology to
15 do something.

16 So, we did that, but then when we got to the
17 new licensees, we found that within the confines of their
18 software program manual, their hazards analysis said,
19 "Well, we'll do a preliminary one. We'll just say prior
20 to the process, and then at the end of the process, we'll
21 do that."

22 Now, again, they're within their rights,
23 but then that became a larger training issue for their
24 staff, because again, when you think about nuclear
25 development processes and you think about software in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 a safety context, it's a relatively limited field.

2 So, if you were trained in an applicant's
3 organization, it's fair to consider that they may be
4 trained in how to do things per their software program
5 manual, but from a licensing commitment standpoint, that
6 was something of a new paradigm set for them, and in that
7 regard, we had to point them to the commitments made,
8 not for the platform of their software that they're
9 developing, but for the larger picture of the power
10 plants.

11 So, for example, in the commitment level for
12 Reg Guide 1.173, to which they had committed, we pointed
13 out that it says, "You shall conduct," and the word
14 'shall' is in the Reg Guide, versus 'should', a hazards
15 analysis at the completion of each phase, which would
16 be appropriate, especially for software.

17 So, we learned that, I think on both sides
18 of the fence, and we're taking steps to highlight that,
19 such that it -- you have to take the particular applicant
20 or licensees at this point, process, that we endorsed
21 through an SER.

22 Then the totality of all the documentation
23 for a given power plant to say, "This is what needs to
24 be done in regard to a hazard analysis," and not only
25 what is involved with it, but the frequency and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 periodicity of it, to verify that you're not creating
2 a failure of a different type, you know, throughout the
3 development process that we talked about earlier, in
4 configuration management. Thank you.

5 MEMBER STETKAR: Great, thank you.

6 CONSULTANT HECHT: Can I add something with
7 respect to that, because part of this is -- if you're
8 doing a top-down development approach, then that is
9 fairly easy.

10 You would have the hazards kind of vaguely
11 filled in at the beginning, and then you -- I mean, you
12 fill them in later on.

13 There are many of the, you know, system
14 developments, when you bring in COTS, you have hazards
15 being introduced by the COTS components and the
16 networking technologies and the infrastructures and the
17 platforms that are being brought in with that.

18 How does that work? How do you envision
19 that working in all of this?

20 DR. ARNDT: You have to go back and look at
21 the various pieces of the various applications.

22 In the COTS example, and you can do this,
23 whether it's a different part of your process, different
24 vendor, sub-vendor, things like that, in which case, we
25 would have an expectation that you import that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 particular piece of software, that particular piece of
2 hardware, that would come along with it.

3 The point is, you have to re-evaluate that
4 failure analysis at every phase. So, as you do your
5 integration, you're bringing in those additional
6 hazards, not only the hazards of the piece of software,
7 the COTS piece of software, but also all the integration
8 issues associated with that.

9 So, does everyone do a great job of it? No,
10 but that is a requirement, as part of whatever phase
11 you're bringing that particular either COTS or software,
12 from a different part of the organization into your
13 program plan, your program.

14 CONSULTANT HECHT: Well, you know, I just
15 -- I think that is a good general answer, but I would
16 point out that, you know, priority and version, which
17 is part of a COTS operating system, that is a failure
18 mode, if you will, of COTS software.

19 It has a different effect, depending on
20 whether it's a -- I don't know, certainly, controlling
21 a safety critical device, a pump or a valve, injecting
22 coolant or water someplace that should be injected to,
23 versus I don't know, operating the fan in the control
24 room.

25 So, it has got to be a combination of both

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the failure modes of the individual components that
2 you're bringing in and the effects on the system.

3 DR. ARNDT: Yes, and that is something we
4 evaluate, and if it's a major sub-component, then they
5 actually dedicate the piece of software or component or
6 whatever, through the commercial grade dedication
7 process, which includes evaluation of the failure modes.

8 CHAIRMAN BROWN: You're done? Stick a
9 fork in you, whatever?

10 MR. STURZEBECKER: Yes.

11 CHAIRMAN BROWN: I think we -- conclusions
12 are your conclusions.

13 MR. STURZEBECKER: You read the
14 conclusions, yes.

15 CHAIRMAN BROWN: Are there -- I guess I need
16 to open the bridge line, to see if there is any comments.
17 Somebody, go ask them to open it.

18 DR. ARNDT: While you're doing that, I
19 think I'm the last most senior person left in the room.

20 I want to thank the Subcommittee. We
21 appreciate your input. It's always good to have a fresh
22 set of eyes, particularly ones that are so knowledgeable
23 and experienced, as the group here.

24 We will take all of your comments under
25 consideration in preparing the final version of this,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and where we have made any revisions, prior to the full
2 Committee, we'll let you know, so, you're aware, and
3 include that in our presentation. What is our time
4 frame?

5 MS. ANTONESCU: June, I think the 6th or the
6 7th.

7 DR. ARNDT: Okay, we're fairly tight time
8 frame, because obviously, if we make a change, we have
9 to get you to concur and all that kind of good thing.

10 But we will take all your comments under
11 advisement and we appreciate the opportunity.

12 CHAIRMAN BROWN: Okay, I will have comments
13 here in a minute, after we check.

14 For those -- people still on the bridge
15 line, somebody say 'yes' or 'no'. Hello?

16 (OTR comments)

17 CHAIRMAN BROWN: Okay, you can go have him
18 close it, so we don't get the snap, crackle, pop here.

19 (OTR comments)

20 CHAIRMAN BROWN: Did you want to hear more
21 on that, John, on the FMEA and hazard analysis? Norbert
22 is down here. He can get working on it.

23 MEMBER STETKAR: Sure.

24 MR. CARTE: I had a quick question, and it's
25 actually more of a --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 I guess when I was presenting the ISG6,
2 there was a question about failure modes and effects
3 analysis, and how that relates to software, and then it
4 ended up in a recommendation and an SRM.

5 I was just sort of wondering if you could
6 elaborate a little bit more on that, so, because we're
7 currently discussing -- I'm currently discussing with
8 Research, and we have a difference of opinion, and I
9 don't want to sway it one way or the other.

10 I just would like you to expand a little bit,
11 what the intent was, and I guess, of looking at the
12 software FMEA's.

13 MEMBER STETKAR: Because if I remember that
14 --

15 CHAIRMAN BROWN: No, I remember that, but
16 I --

17 MR. CARTE: Do you want to revisit --

18 MEMBER STETKAR: No, I don't want any part
19 of that.

20 CHAIRMAN BROWN: No, it was the spring
21 board from one of John's observations, during the
22 meeting, that there were no standards for it, and when
23 we talked about FMEA, you all wanted to look at it from
24 a modeling standpoint, but there wasn't any way to
25 identify --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MEMBER STETKAR: But our concerns
2 traditionally have been, and I must admit, I don't recall
3 the specific recommendation and I don't have it in front
4 of me, so, I -- and I cannot pull it up here, quickly
5 here.

6 But our concerns traditionally have been
7 with regard to a coherent definition of what failure
8 modes are for software, because there seems to be a
9 varying interpretation of what a failure mode is.

10 Some people interpret it in a way that I
11 would call a failure cause. I program -- I wrote
12 something wrong, but that is -- it's a cause, and before
13 you can do an effective failure modes and effect
14 analysis, you have to know what a failure mode is, and
15 before you can do an effective risk assessment of the
16 software reliability, identify vulnerabilities, you
17 need that common understanding.

18 Now, as I said, I don't honestly recall the
19 exact recommendation, but I know that has been the
20 Committee's kind of nagging concern, whether it's in the
21 digital I&C world or in the risk assessment world, for
22 software risk and reliability assessment, it's kind of
23 focused on that topic.

24 MR. CARTE: Right, so, Research is sort of
25 halfway done addressing the SRM, and part of that is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 reflected in the NUREG-IA at number 254.

2 What they did is they discussed part of the
3 distinctions between failure and fault, and so, one of
4 the concepts being that we think of failure as being
5 something that works at one point, and then stops
6 working, and in essence, that doesn't happen with
7 software. So, it doesn't fail. It doesn't wear out.
8 It only has faults.

9 So, there is some concern about the
10 appropriateness about talking of software failures when
11 we're really talking about design faults, and so, that
12 is where some of the confusion or disagreement comes in.

13 MEMBER BLEY: Well, it's not so much
14 disagreement, but when we see people trying to analyze
15 these systems, and they assume failure modes or faults,
16 and then make up data to use in them, there is no basis
17 for what they're doing, and certainly, what you say is
18 true.

19 So, any model of how software fails has to,
20 I think, be built on the idea of exposing faults, and
21 that is a very different kind of model than a hardware
22 failure model, which a lot of people use for software.

23 So, we've been pushing people to define what
24 they mean, so that we can take the next step and begin
25 to understand and analyze --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. STURZEBECKER: Can I suggest --

2 MEMBER BLEY: -- and collect information
3 and data.

4 MR. STURZEBECKER: -- just that there are
5 good definitions there, and if you'd like, I can change
6 the --

7 MEMBER STETKAR: No, we've had that, and in
8 some sense, it doesn't make too much difference. I have
9 to be careful, because Dennis is going to hit me.

10 But in some sense, it doesn't make too much
11 difference, whose set of definitions you select. There
12 are several out there.

13 It's important to select a set of
14 definitions and have some rationale behind them and a
15 common understanding, the same way in hardware, that if
16 I have a valve, it can fail to open, it can fail to close,
17 it can open spuriously, it can close spuriously.

18 Those tend to be a fairly comprehensive set
19 of things that people understand, that that valve can
20 and can't do.

21 So, that, you know, selecting one set of
22 definitions of one -- what some people might call false
23 or failure modes, versus another one, as long as you're
24 fairly comprehensive, in terms of covering what the
25 stuff can do and what it can't do, and people start to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 use that as a framework for mapping things into, seems
2 to make a lot of sense.

3 Now, Dennis may disagree, but --

4 MEMBER BLEY: I think that is the starting
5 point.

6 MEMBER STETKAR: That's a starting point.

7 MEMBER BLEY: There are some models out
8 there, if you wanted to do the modeling side, that I sort
9 of like, but they're based on the idea of faults rather
10 than --

11 CONSULTANT HECHT: Can I make some
12 observations?

13 CHAIRMAN BROWN: You can in a second.

14 CONSULTANT HECHT: Yes, I can in a second?

15 MEMBER BLEY: But we're also interested, we
16 want the staff, when they talk to us about this, to deal
17 with failure modes and faults of the systems, including
18 the software, and those are really different things
19 there.

20 So, a coherent logic for how -- to look at
21 these, so that one could at some point in time, build
22 a model that might be useful, and so, that one can really
23 understand where the problems might lie, when you're
24 doing a review or a hazards analysis that isn't a
25 quantitative one. So, either way. Your turn.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 CONSULTANT HECHT: Okay, having been in
2 this business for a little while, there is some pitfalls
3 that I heard Norbert saying, and I heard some things that
4 you've been saying, and I just want to point out.

5 Number one, Norbert made the point about
6 causes, and then you started work -- started going into
7 details about the actual text in the software.

8 I want to make it clear that the observation
9 I made -- or realization I made about 10 years ago, after
10 getting very angry at people who would say to me, "But
11 software doesn't fail," so, I realized that they were
12 absolutely correct.

13 Software does not fail. It's text. The
14 most reliable software that has ever been written is
15 software that has never been executed. It has not
16 caused any failures.

17 So, the point, number one, is that when you
18 talk about causes and you're already worried about what
19 defects did you make in the design, you're going to end
20 up in total confusion.

21 Software reliability or software failures
22 is really a misnomer. It's the system failing because
23 the software is running on it, and so, you can't really
24 isolate the software from the system. It's a system
25 failure.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 Okay, the point number two. With respect
2 to cause, failure mode, that is related to your level
3 of indenture. So, that is a term, but it basically
4 relates to the level of an analysis.

5 Given the fact that we're already dealing
6 with the fact that we're looking at things that run time,
7 is an operating system failure, a cause? It's a cause
8 of a PLC failure, but in turn, the operating system has
9 failure modes, which you can analyze at that level.

10 So, you need to decide the level of at which
11 you do the analysis, which in Mil Standard 882, which
12 is the -- I'm sorry, Mil Standard 1682, which is the
13 mother of all of the FMEA standards, coming from the
14 Military, that is how one begins to address that.

15 You have to decide, and that may vary, based
16 on the design, but one of the questions that you have
17 to answer, in terms of your hazard analysis methodology
18 is, at what level you are going to perform the hazard
19 analysis, and that determines what's your cause, what's
20 your failure.

21 So, is your operating system or is your
22 network stack the cause of the failure or is it actually
23 a failure mode in and of itself?

24 Finally, the third point, when we get to
25 quantitative methods, most of what we've been doing, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 I'm guilty of this as anybody else, is dealing with
2 software failures of the stop-hang crash variety. In
3 other words, a system stopped working or it keeps
4 working.

5 In safety systems, we also have to deal with
6 the fact that you get the wrong answer, and so, you have
7 to distinguish probabilistically, between the fact that
8 the system just stops working and the fact that it
9 doesn't give you the right answer, and I don't think that
10 probabilistically, and this is one of the issues that
11 I've had for a long time, when people say, "You can't
12 quantify software failures."

13 I believe that you can quantify the failure
14 rates for the stop-hang crash variety, but you cannot
15 really quantify the incorrect answer, the incorrect
16 output variety as well, and for that, you really have
17 to rely on your software development process, including
18 all these standards we've been talking about today.

19 These are the deterministic failures which
20 -- whose probability is really determined by the
21 triggering certain -- these triggering events, that
22 would cause the wrong answer to be generated. In other
23 words, external to the software itself.

24 MEMBER BLEY: Finally, understand that
25 individual people sitting at this table, cannot speak

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 for the ACRS.

2 CHAIRMAN BROWN: Very large point.

3 MEMBER BLEY: Exactly, any of us.

4 CHAIRMAN BROWN: Any of us.

5 MR. CARTE: Right, I was just seeing -- I
6 think I've got my answer. I was just seeking additional
7 data, in order for us to resolve the SRM and the
8 recommendation. So, thank you.

9 CHAIRMAN BROWN: Okay, thank you, Norbert.
10 All right, phone lines are taken care of. Any other
11 public comments? Okay.

12 MEMBER BLEY: Sure, thanks for the day.
13 I've said anything that I really raised issues with.

14 I do want to thank you for the things you
15 have on the slides, to tie this rat's nest together, with
16 your color coding. That really helps. I kind of wish
17 I had had them before I started, but you didn't have those
18 yet, but it's helpful.

19 CHAIRMAN BROWN: Dennis? John? Excuse
20 me.

21 MEMBER STETKAR: And I'll echo what Dennis
22 said, I don't have anything else to add, and I really
23 appreciate it. You pulled together an awful lot of
24 really difficult, complex material for this
25 presentation, and did it really well.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. STURZEBECKER: I have to thank my team,
2 also.

3 CHAIRMAN BROWN: Okay, Myron, do you have
4 any other thoughts over and above?

5 CONSULTANT HECHT: No, other than this is
6 -- you -- I think the strategy or the tactic was to get
7 all of a very complex subject, handled very quickly.
8 There was a massive amount of material presented today,
9 and we acknowledge that.

10 CHAIRMAN BROWN: Okay, I will echo those.
11 I had to be -- I'm a little bit a fault for expanding,
12 because they did do a very good job, as I acknowledged
13 at the beginning of the meeting, on expanding this to
14 do -- and added those charts, which were quite nice, to
15 be able to see what maps to where, and having that in
16 advance was nice, it would have been nice, but --

17 MEMBER STETKAR: The Chairman gets things
18 that the poor Subcommittee --

19 CHAIRMAN BROWN: No, I didn't get that. I
20 got these at the same time you guys did, okay. I had
21 to grind through this the same way you did, John, and
22 look at just the summary of what was changing and what
23 was not changing.

24 So, I mean, that was very good. One thing
25 I would like to -- so, I wanted to thank you and like

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 I said before, having it ready for at least minute
2 effort, to get all that stuff together, I don't know who
3 else participated, but they can participate in the
4 global 'thank you'.

5 I have just a -- in anticipation of the full
6 Committee meeting -- go ahead.

7 MEMBER STETKAR: By the way, when -- before
8 the full Committee meeting, if any of the other Committee
9 members are interested in this, we should make sure that
10 they have those, at least those mapping slides, alert
11 them to the fact that they exist, because --

12 MS. ANTONESCU: Yes.

13 MEMBER STETKAR: -- that is useful.

14 CHAIRMAN BROWN: No, I was going to ask, and
15 that is a good point, and I would just have Christina
16 to send me --

17 MEMBER STETKAR: And just make sure you
18 alert people to that.

19 CHAIRMAN BROWN: Yes, this is what we did
20 at the Subcommittee meeting and there will be a subset
21 of this at the full Committee meeting.

22 I was trying to make some suggestions for
23 the full Committee meeting, in that -- in other words,
24 you've got to at least cover each Reg Guide. We'll
25 probably have about what, an hour and a half to two hours,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 something like that on the schedule? I've forgotten
2 what we talked about before. I think it was two hours.

3 So, try to allocate the time, I think,
4 correct me if I'm wrong, but 1.173, 1.170 and -- those
5 were the two with the most changes to the IEEE standards,
6 I think.

7 MEMBER BLEY: Yes, Charlie, if I could?

8 CHAIRMAN BROWN: Yes, go ahead.

9 MEMBER BLEY: If the full Committee, they
10 try to go through all six of the Reg Guides, I don't
11 think people will even get what is going on.

12 I think doing something up at this higher
13 level, about how the standards relate to each other, how
14 they relate to the Reg Guides, and maybe just one of these
15 charts to show, the stuff is disappearing, the stuff is
16 being added, I think that would really help people get
17 what this is all about, and talk about them more in
18 general, than in the details of Figure C.2 disappeared
19 and --

20 CHAIRMAN BROWN: No, I agree. I was trying
21 to get a -- what I was trying to get to was a general
22 approach, and that is a good suggestion.

23 But then what are -- because a lot of this
24 was just kind of -- it's not -- neither boilerplate not
25 cosmetic, but it was just bringing things up to date,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that there were two or three items amongst all of them,
2 maybe three or four, or whatever that number is, which
3 were the bigger ticket -- you know, there might be one
4 item or something like that, from any one of the Reg
5 Guides and standards that was revised.

6 Then say, "Hey, these are the big items.
7 These are the major changes that were made, and this is
8 how we reflect them in the Reg Guide."

9 Now, I don't how you all would consider
10 those, but -- and again, present a general presentation
11 about, "Hey, here is what we did. We had all these
12 changes going on, but we're trying to get them into these
13 six Reg Guides, and this is the changes and this is how
14 we mapped them in," and then the big hitters were --

15 MEMBER BLEY: There were two or three
16 things were talked about for 20 or 30 minutes today,
17 each, probably worth coming back to those.

18 CHAIRMAN BROWN: Yes, I think other members
19 will --

20 DR. ARNDT: I think we can put that
21 together. Would it be useful for the full Committee to
22 hear, these are the six guides, this is what their
23 position in the regulatory structure is, what they're
24 trying to accomplish as a whole, this is how the
25 requirements are allocated by Reg Guide, these are the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 major changes.

2 CHAIRMAN BROWN: Well, the titles pretty
3 much tell you.

4 DR. ARNDT: Pretty much, yes.

5 CHAIRMAN BROWN: Yes, I don't think you
6 want to go too much more, when you're talking about
7 either one of them, don't you agree? The titles pretty
8 much tell you how they're oriented, and you did it and
9 --

10 MEMBER STETKAR: There are some
11 subtleties, though that aren't --

12 CHAIRMAN BROWN: Yes, I know.

13 MEMBER STETKAR: -- necessarily apparent
14 by just reading the titles.

15 CHAIRMAN BROWN: Well, no, I understand,
16 that's why I said a couple of these have some bigger
17 inputs.

18 The things that changed or added to your
19 process, that you didn't have before, that is the point
20 I was trying to make, that you think added value, changes
21 that were made to the standards that added value, and
22 there is -- I mean, real value.

23 DR. ARNDT: We can structure it that way.

24 MS. ANTONESCU: Something visual, too.

25 CHAIRMAN BROWN: Yes, the visual.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. ARNDT: We'll have some visuals.

2 CHAIRMAN BROWN: Okay, and the loose
3 hanging -- you all were taking some notes? The six --
4 five items that I've got on here were the life cycle
5 process as applied to non-safety systems, for the
6 digital I&C for non-safety, and we're only covering
7 safety.

8 You know, where is our -- and I'm not sure
9 I'm phrasing that right --

10 MEMBER BLEY: For non-safety systems that
11 are important to safety.

12 CHAIRMAN BROWN: That are important to
13 safety, I'm sorry, okay.

14 MEMBER BLEY: These in between things.

15 CHAIRMAN BROWN: Yes, I didn't have that.

16 MEMBER STETKAR: RTNSS and RAP.

17 CHAIRMAN BROWN: Yes, non-safety systems
18 that are important to safety, RTNSS, or however you want
19 to phrase that, and those are kind of hanging out there,
20 because you only addressed the safety. That was the
21 first item.

22 The second was, I note that this is in 1.173,
23 that I felt there was a bit of an inconsistency between
24 the cyber words in 1.152 and the words in 1.173. We
25 ought to get that -- 1.173 ought to reflect what is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 already out there in 1.152.

2 MEMBER BLEY: And if you can come in and
3 say, that is the way that it -- they'll look in the next
4 round, that will be great.

5 CHAIRMAN BROWN: Yes, that will be fine.
6 That will work.

7 DR. ARNDT: I think that is a doable.

8 CHAIRMAN BROWN: Okay, the third item was
9 -- no, that's gone.

10 Then 1.170, that was where effectively
11 deleting -- that was that sentence between the
12 probability, the likelihood of the occurrence of a
13 severe catastrophic whatever --

14 MEMBER STETKAR: That's the risk --

15 CHAIRMAN BROWN: Yes, the risk statement
16 and the --

17 MR. STURZEBECKER: I got that.

18 MEMBER STETKAR: That is in 1.168 and
19 1.173.

20 CHAIRMAN BROWN: Yes.

21 MR. STURZEBECKER: Got it.

22 CHAIRMAN BROWN: Yes, I've got that noted
23 down here.

24 MEMBER STETKAR: For the integrity level.

25 MR. STURZEBECKER: Right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Then there was the failure
2 recovery testing, that was in 1.170, and that was
3 relative to Regulatory Position 4, I think, and then
4 there was the test documentation question in the list,
5 test cases, whatever it was, test cases and test
6 something. It will be in the transcript, I guess.

7 Then the last one that I belabored to
8 internal, on the independent, but then we waffled and
9 John, I think, suggested that you guys would look at the
10 second paragraph words, to try to make them a little bit
11 -- to make them consistent with each other.

12 So, those are the small pieces that are left
13 over.

14 Now, I take it, that you all had any other
15 notes?

16 MEMBER STETKAR: No, that pretty well
17 covers it.

18 CHAIRMAN BROWN: Okay.

19 DR. ARNDT: We will look at all of those,
20 as I mentioned earlier, we've got to come up with what,
21 if anything, we want to change, and we have to go through
22 the concurrence.

23 So, we may not be able to say definitively,
24 what if anything, we're going to change, but we'll see
25 what we can do, to address those.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Most of those are fairly straight forward
2 kind of fixes that I think we can get to.

3 CHAIRMAN BROWN: Yes, I'd like to have some
4 idea. I've got to write a letter report for you all out
5 of the full Committee meeting, and I'm not more happy
6 about having to do this in two and a half weeks, or 18
7 days, than you are, okay, I can guarantee you that.

8 But it will be done, and I just assume not
9 have to trickle some of things in. If I did, I'd
10 probably get my head handed to me, anyway, by the
11 Committee. But we'll find out.

12 MEMBER BLEY: It depends on how you include
13 them.

14 CHAIRMAN BROWN: Well, I have this
15 methodology for including stuff that tends to get
16 people's attention. So, intentionally.

17 So, anyway, if there is no more comments,
18 if I haven't forgotten anything, the normal Robert's
19 Rule of Order, I will adjourn the meeting. Thank you.

20 (Whereupon, the above-entitled matter
21 concluded at approximately 4:35 p.m.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

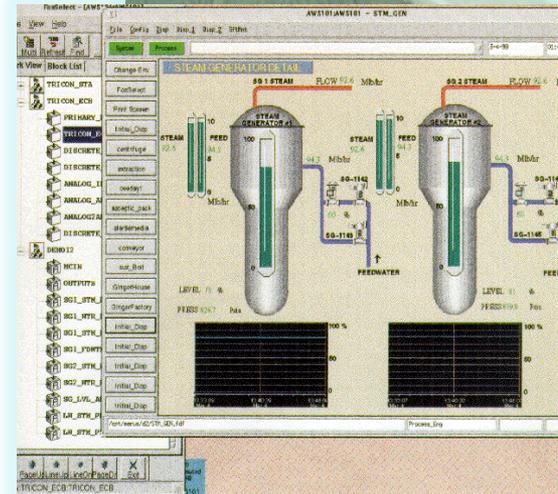
Software Regulatory Guidance

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
May 21, 2013

Karl Sturzebecher
Office of Nuclear Reactor Regulation
Division of Engineering

Purpose of Meeting

- Background
- Review 6 Regulatory Guides (RGs)
 - RG 1.173 Project Management
 - RG 1.172 Software Requirements Specs
 - RG 1.171 Unit Testing
 - RG 1.170 Test Documentation
 - RG 1.169 Configuration Management
 - RG 1.168 V&V Review Audits
- Conclusion



Background

- **Background**
- Review 6 Regulatory Guides (RGs):
 - RG 1.173 Project Management
 - RG 1.172 Software Requirements Specs
 - RG 1.171 Unit Testing
 - RG 1.170 Test Documentation
 - RG 1.169 Configuration Management
 - RG 1.168 V&V Review Audits
- Conclusion

Background

- What are these RGs for?
- How do they fit with NRC guidance?
- What are the common topics?

QA

Integrity

Tools Secure Analysis

Release Management & Delivery

- Who was involved?

NRC Team Members:

Norbert Carte NRR

Bill Kemper NRR

Eric Lee NSIR

Wendell Morton NRO

Tim Mossman NSIR

Khoi Nguyen NRO

David Rahn NRR

Gusharan Singh NRR

Richard Stattel NRR

Tung Truong NRO

Bill Roggenbrodt NRO

Karl Sturzebecher NRR

Oakridge National Labs

Learning experience from:

Martha Wetherholt – NASA

Gerald Holtzman – JPL

Thuy Nguyen – eDF

Dan Derrico – Railway Software Engineer

Jennifer Bayuk – Stevens Institute of Technology

MITRE Corporation Swa conferences

Army Office Research conferences

EPRI MOU on OpE

Public comments

Background

Regulatory Guide change matrix -

| Regulatory Guides | IEEE Standards | | | Change Complexity |
|-------------------|----------------|-----------|-----------------|-------------------------|
| | Previous | Interim | Update | |
| <u>RG 1.173</u> | 1074-1995 | 1074-1997 | 1074-2006 | 2 nd Highest |
| <u>RG 1.172</u> | 830-1993 | → | 830-1998 | IEC 29148 Low |
| <u>RG 1.171</u> | 1008-1987 | → | 1008-1987(2002) | Reaffirmed |
| <u>RG 1.170</u> | 829-1983 | 829-1998 | 829-2008 | Highest |
| <u>RG 1.169</u> | 828-1990 | 828-1998 | 828-2005 | 828-2012 Medium |
| <u>RG 1.168</u> | 1012-1998 | → | 1012-2004 | 1012-2012 Medium |
| | 1028-1997 | → | 1028-2008 | Medium |

- Background
- Review 6 Regulatory Guides (RGs):
 - RG 1.173 Project Management
 - RG 1.172 Software Requirements Specs
 - RG 1.171 Unit Testing
 - RG 1.170 Test Documentation
 - RG 1.169 Configuration Management
 - RG 1.168 V&V Review Audits
- Conclusion

Review 6 RGs

IEEE Standard

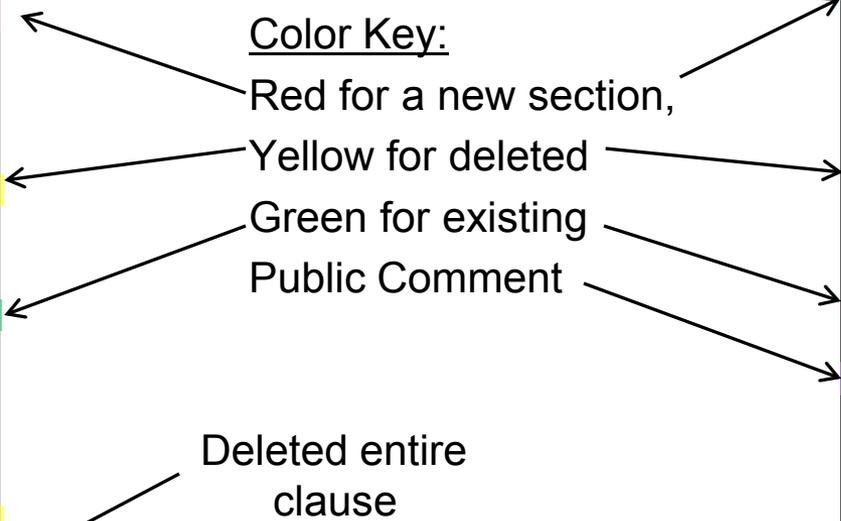
| |
|--|
| Overview 1 |
| Software LC Model Process 2 |
| PM Processes 3 |
| Pre- development Processes 4 |
| Development Processes 5 |
| Post- development Processes 6 |
| Integral Processes 7 |
| Bibliography |

Review Format:

Color Key:
 Red for a new section,
 Yellow for deleted
 Green for existing
 Public Comment

Regulatory Guide

| |
|--------|
| Part A |
| Part B |
| |
| |
| Part C |
| |
| |
| Part D |
| Ref. |



Deleted entire
 clause

Review 6 RGs

Review Format:

Illustration of how a standard clause/topic is directly applied to the Life Cycle or tailored by the regulatory guide, which can either take an exception and/or an addition to the clause/topic

IEEE Standard

| |
|------------------------------|
| Overview 1 |
| Software LC Model Process 2 |
| PM Processes 3 |
| Pre-development Processes 4 |
| Development Processes 5 |
| Post-development Processes 6 |
| Integral Processes 7 |
| Bibliography |

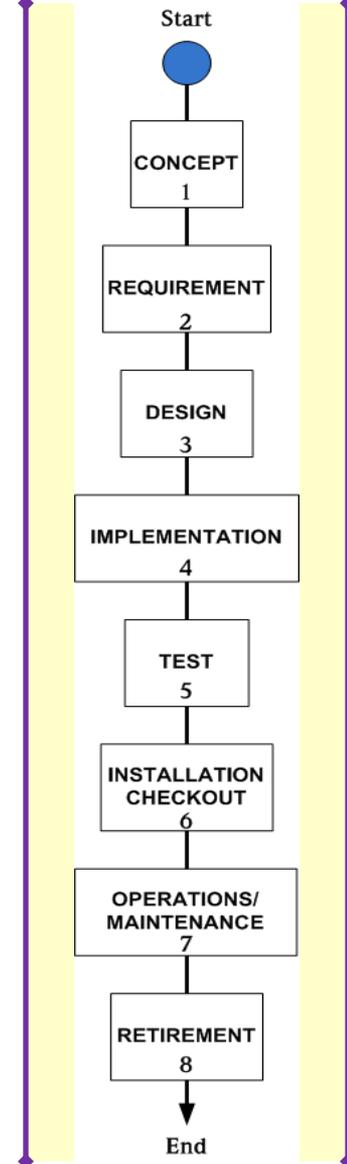
Regulatory Guide

| |
|--------|
| Part A |
| Part B |
| |
| Part C |
| |
| |
| Part D |
| Ref. |

Endorsed without exception

Variation (exception and/or addition)

Software Project Life Cycle Process



RG 1.173

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

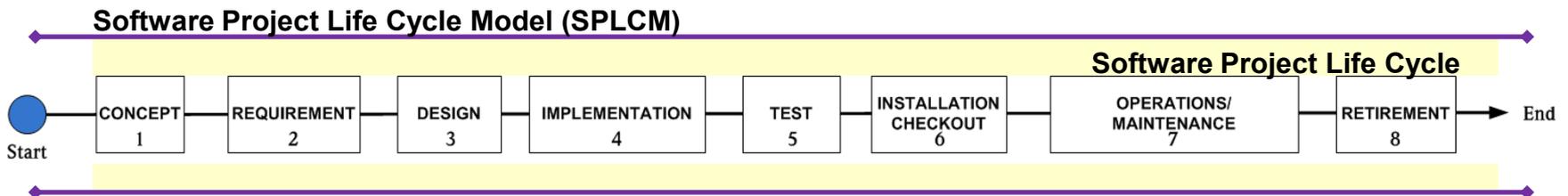
- Background
- Review 6 Regulatory Guides (RGs):
 - **RG 1.173 Project Management**
 - RG 1.172 Software Requirements Specs
 - RG 1.171 Unit Testing
 - RG 1.170 Test Documentation
 - RG 1.169 Configuration Management
 - RG 1.168 V&V Review Audits
- Conclusion

RG 1.173

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 1074-2006 directly
- Overview regulatory guidance
- Objective: Create a Software Project Life Cycle Process (SPLCP)
 - Establish requirements
 - Select a Software Project Life Cycle Model (SPLCM)
 - Develop Software Project Life Cycle (SPLC)
 - Establish SPLCP
 - Validate the process



Software Project Life Cycle Process



RG 1.173

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

General overview of changes -

- Minor variations to RG 1.173 Regulatory Positions based on the revised standard, no changes to the life cycle
- 1074 clarifies directions for building the SPLCP, uses “activities” vs. “processes”
- Updated standard sharpens focus on key elements to build an SPLCP and redistributes activities within existing framework inside and out
- New 1074 topics: security objective recognized, along with software importation and software release management
- The new evaluation activity group shows the importance of some seemingly small steps, such as informal peer to peer review

RG 1.173

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

What changed in the RG?

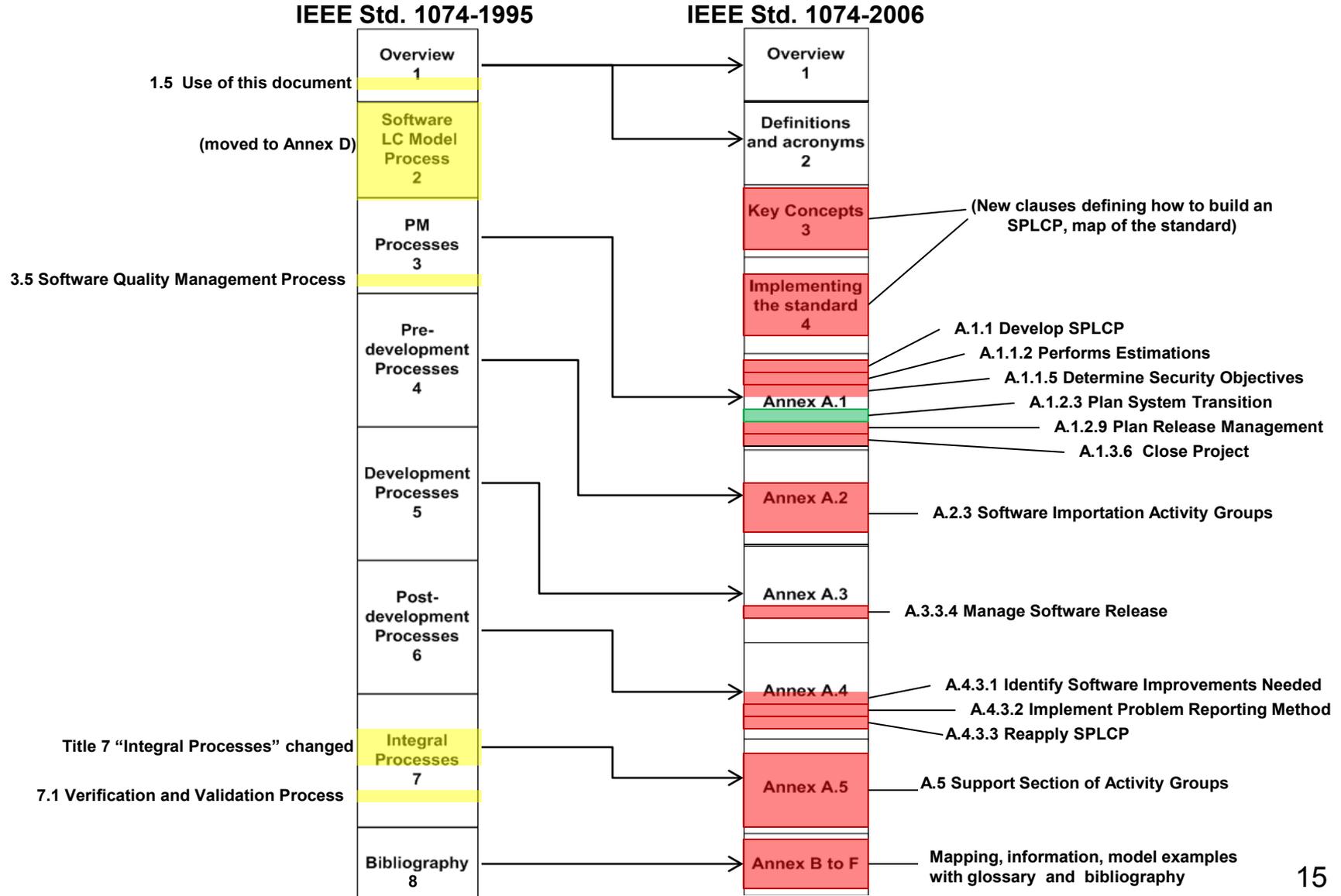
- Public comment adding an NRC citation of an EPRI Topical Report
- Provides new regulatory position on security objectives in the 1074 standard
- Adds new emphasis “System Transitions” for changes to safety systems [They must be 10 CFR 50.59 evaluated]
- New Annex (A to F)



Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

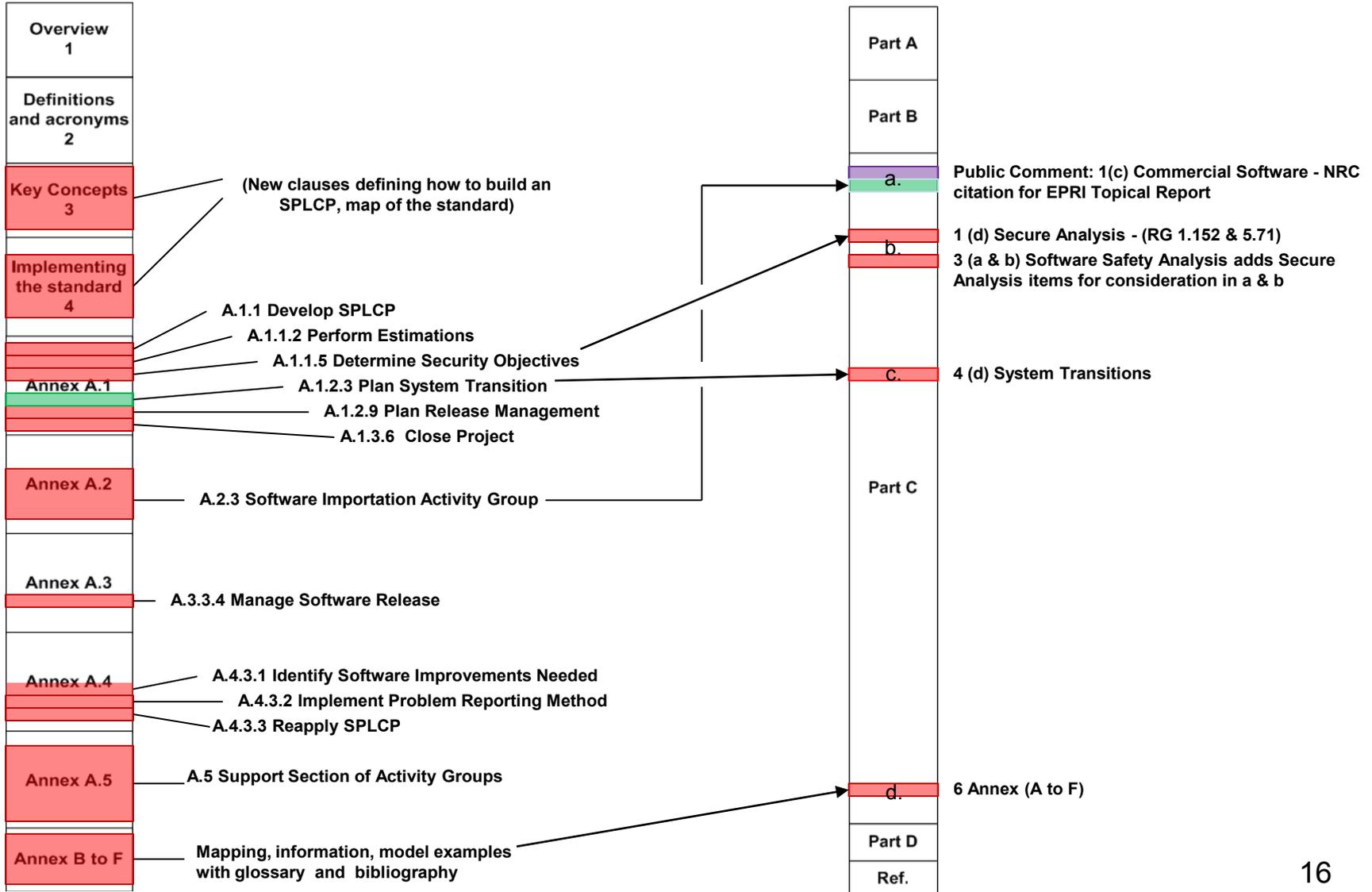
What changed in the IEEE 1074?

- Major shuffling of clauses and activities in new 2006 version
 - Clauses 1 to 4 on SPLCP mapping directions
 - Selection of a Model for SPLCM now in Annex D
 - Moving old “process” names as “activities” into Annex A
 - Different emphasis on quality management and integral processes
- Improvements to activities in Annex A
 - Focus with existing planning activities as part of the project management with new security objective, plan release management and close activity
 - Pre-development group has new software importation activities
 - Implementation group adds managing software release activity
 - Post-development group picks up quality improvement activities
 - “Support Section of Activity Groups” (old “Integral Process”) refocuses with a new “Evaluating Activity Group”



IEEE Std. 1074-2006

RG 1.173



RG 1.173

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

Specific changes in the RG:

- Part C, 1,(d) “Secure Analysis” – New exception and proper references for software security
- Part C, 3,(a)(5) “Input Information” – Adds new line on creation of a baseline for Secure Development and Operational Environment (SDOE) objectives
- Part C, 3,(b)(6&7) “Activity Description” – Adds 2 new lines for addressing of a threat model and overall software architecture
- Part C, 4,(d) “System Transitions” – New on existing standard topic
- Part C, 6 “Annexes” – New and adds A to F

RG 1.173

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

Public comments incorporated:

- Minor grammar corrections
- Part C, 1, (c) “Commercial Software” – Adds NRC letter endorsement

Specific changes in the IEEE Standard:

- Original IEEE Std. 1074-1995 followed by interim 1997 version...
- This RG endorses IEEE Std. 1074-2006 and has the following changes:
 - Clause 1 “Overview” – New expanded scope, audience, relationships, organization
 - Clause 2 “Definitions and acronyms” – Updated
 - Clause 3 “Key concepts” – New
 - Clause 4 “Implementing the standard” – New

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

Specific changes in Annex A:

- A.1.1 “Project Initiation Activity Group” – New process initiation with “Develop SPLCP,” “Perform Estimation” and “Determine Security Objectives” activities
- A.1.2 “Project Planning Activities Group” – Existing planning group with new “Plan Release Management” activity
- A.1.3 “Project Monitoring and Control Activity Group” – New activity “Close Project”
- A.2 “Pre-Development Section of activities groups” – New titles
- A.2.3 “Software Importation Activity Group” – New activity group
- A.3 “Development Section of activity groups” – New title
- A.3.2 “Design Activity Group” – New title
- A.3.3 “Implementation Activity Group” – New title with “Manage Software Release” activity

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

Specific changes in Annex A: (cont'd)

- A.4 “Post-Development Section of activity group” – New title
- A.4.2 “Operation and Support Activities” – New title
- A.4.3 “Maintenance Activity Group” – New title with “Identify Software Improvements Needs,” “Implement Problem Reporting Method,” and “Reapply SPLCP” activities
- A.4.4 “Retirement Activity Group” – New title
- A.5 “Support Section of activity groups” – New activity group
- A.5.2 “Software Configuration Management Activity Group” – New title
- A.5.3 “Documentation Development Activity Group” – New title
- A.5.4 “Training Activity Group” – New title



RG 1.172

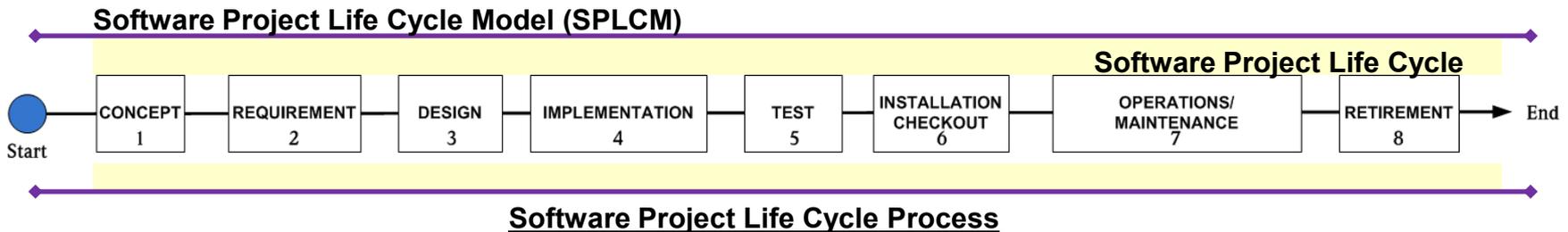
Software Requirement Specifications for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

- Background
- Review 6 Regulatory Guides (RGs):
 - RG 1.173 Project Management
 - **RG 1.172 Software Requirements Specifications**
 - RG 1.171 Unit Testing
 - RG 1.170 Test Documentation
 - RG 1.169 Configuration Management
 - RG 1.168 V&V Review Audits
- Conclusion

Software Requirement Specifications for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 830-1998 directly
- Objective: Create a Software Requirements Specification that delineates the function accurately without added constraints
- Traceability for both original baseline and future development
- Supports the SPLCP



General overview of changes -

- Very minor changes to the RG as it follows the standard
- Provides new emphasis on clear specifications and defines security

RG 1.172

Software Requirement Specifications for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What changed in the RG?

- Incorporates “Unambiguity” to Regulatory Position 2(h) so there can only be one interpretation
- Public comment requesting NRC improve description of “Unambiguity”
- Provides new overview on the “Secure Analysis” under Regulatory Position 6(b) as Subclause 5.3.6.3 is limited
- New Annex section (A & B)



What changed in the IEEE Standard?

- No substantial changes to IEEE Std. 830-1998

IEEE Std. 830-1993

| |
|---|
| Overview 1 |
| References 2 |
| Definitions 3 |
| Considering for producing a good SRS 4 |
| The parts of an SRS 5 |
| Annex A |

IEEE Std. 830-1998

| |
|---|
| Overview 1 |
| References 2 |
| Definitions 3 |
| |
| Considering for producing a good SRS 4 |
| |
| The parts of an SRS 5 |
| Annex A & B |

RG 1.172

| |
|--------|
| Part A |
| Part B |
| a. |
| b. |
| |
| c. |
| Part C |
| |
| d. |
| Part D |
| Ref. |



4.3.2 Unambiguous

5.3.6.3 Security

Adds Annex B
Guidelines to IEC 122207

2(h) New "Unambiguity" position
Public Comment: Improve the description

6(b) Secure Analysis; Added reference to RG 1.152 for SDOE

7 Annex (A&B)

RG 1.172

Software Requirement Specifications for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Specific changes in the RG:

- Part C, 2,(h) “Unambiguity” – New subsection
- Part C, 6,(b) “Secure Analysis” – New subsection because of Sub-Clause 5.3.6.3 “Security” in IEEE 830-1998
- Part C, 7 “Annexes” – New and adds B

Public comments incorporated:

- Minor grammar corrections
- Part C, 6,(h) “Unambiguity” – Improved description

Specific changes in the IEEE Standard:

- No substantial changes to IEEE Std. 830-1998

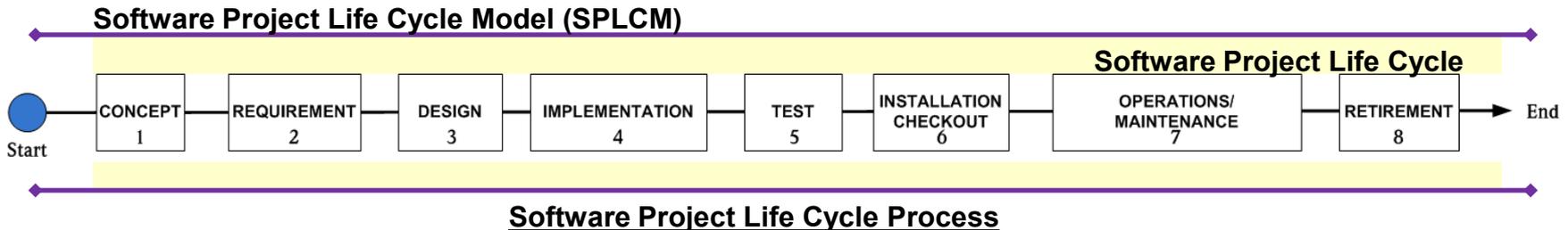
RG 1.171

Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants

- Background
- Review 6 Regulatory Guides (RGs):
 - RG 1.173 Project Management
 - RG 1.172 Software Requirements Specs
 - **RG 1.171 Unit Testing**
 - RG 1.170 Test Documentation
 - RG 1.169 Configuration Management
 - RG 1.168 V&V Review Audits
- Conclusion

What does this RG do?

- Follows IEEE 1008-1987 directly
- Objective: Provides emphasis on unit testing for software safety systems
- Smallest piece of software that can be independently tested



General overview of changes -

- Regulatory Position 5 changes noting 829 new levels of documentation for unit testing
- No change in standard

RG 1.171

Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants

What changed in the RG?

- a. Addresses references to new documentation in IEEE Std. 829-2008
- b. New title for Regulatory Position 5 where “Other Standards” becomes “Reference to ANSI/IEEE Std. 829-1983”
- c. New Annex (A to D)



What changed in the IEEE 1008?

- No substantial changes to IEEE Std. 1008-1987

IEEE Std. 1008-1987

| |
|------------------------------|
| Scope and References 1 |
| Definitions 2 |
| Unit Testing Activities 3 |
| Annex A to D |



RG 1.171

| | |
|--------|--|
| Part A | |
| Part B | |
| a. | References new documentation in 829 |
| b. | 5 References to ANSI/IEEE Std. 829-1983; acknowledges new levels of test documentation |
| Part C | |
| c. | 6 Annexes (A to D) |
| Part D | |
| Ref. | |

RG 1.171

Software Unit Testing for Digital Computer Software
used in Safety Systems of Nuclear Power Plants

Specific changes in the RG:

- Part C, 1 “Software Testing Documentation” – Adds IEEE Std. 829-2008 references with Clauses 10 and 17
- Part C, 5 “Other Standards” – New section “References to ANSI/IEEE Std. 829-2008”
- Part C, 6 “Annexes” – New; adds A to D

Public comments incorporated:

- Minor grammar corrections

Specific changes in the IEEE Standard:

- No change to IEEE Std. 1008-1987 (Reaffirmed in 2002)

RG 1.170

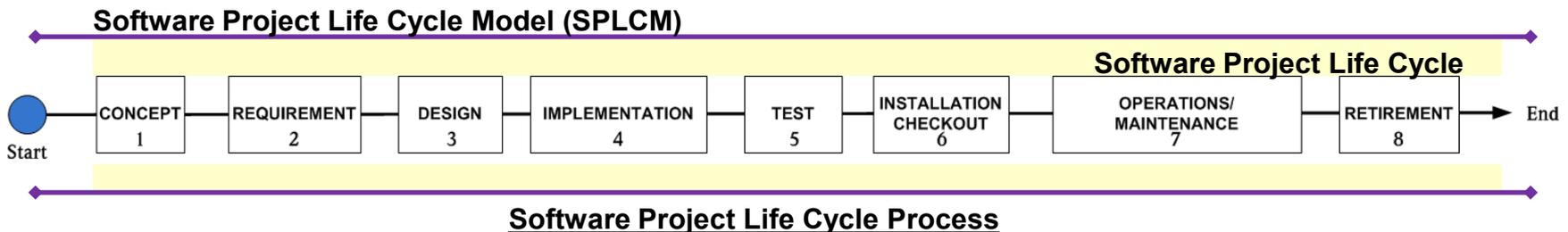
Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

- Background
- Review 6 Regulatory Guides (RGs):
 - RG 1.173 Project Management
 - RG 1.172 Software Requirements Specs
 - RG 1.171 Unit Testing
 - **RG 1.170 Test Documentation**
 - RG 1.169 Configuration Management
 - RG 1.168 V&V Review Audits
- Conclusion

Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 829-2008 directly
- Objective: Create a software test plan that methodically documents the software requirements with a reportable demonstration of the unit, component, system and acceptance testing
- Follows a common framework with life cycle processes
- Applies to developing software in the life cycle and/or preexisting or pre-developed software
- Uses Software Integrity Level 4 with traceability, when reporting anomalies



Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

General overview of changes -

- Major additions to RG 1.170 based on the revised standard while maintaining compatible to standards with the life cycle approach
- Old 829's framework now becomes sub-clauses to a new overarching process
- Process outlines integrity levels, documentation strategies, and process directions
- Overarching process builds a Master Test Plan (MTP) with new improved planning, reporting, interim and status reports for final Master Test Report
- Existing 829 framework sub-clauses also are adapted to the overall life cycle methodology
- Improves focus for multiple levels of unit, component, system and acceptance testing for large or small software projects
- Completes testing loop with formal documentation for anomalies

RG 1.170

Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What changed in the RG?

- Addition of Software Integrity Level 4 in Regulatory Position 1
- Public comment: Improved paragraph to include a. thru g. with the MTP in Regulatory Position 1
- General acknowledgement of new Level Test Log (Clause 13) and Anomaly Report (Clause 14) documentation
- Addresses new report documentation and need for deviation policy per Clause 8.2.3.3
- Provides expanded direction in Regulatory Position 3 on documentation reduction vs. integrity

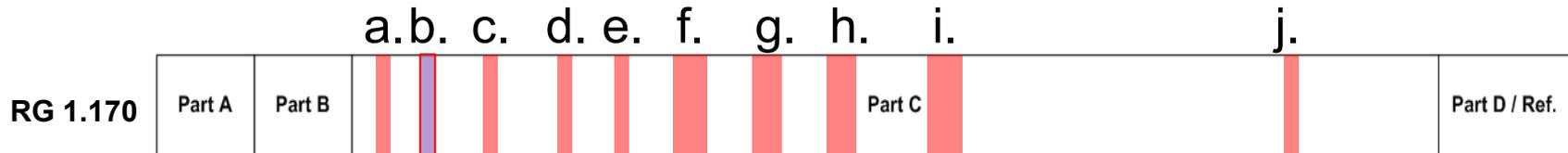


RG 1.170

Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What changed in the RG?

- f. Adds new regulatory position “Integrity Levels” while pointing to exception in Table B.3
- g. Adds new regulatory position “Test Tasks” with additional information in Table C.1
- h. Adds new regulatory position “Test Tool Documentation” with exception for easy accessible tool test information (Clause 6.3)
- i. Adds new regulatory position “Secure Analysis” with addition for early life cycle effort (Clause 5, Table 3)
- j. New Annex section (A to H)



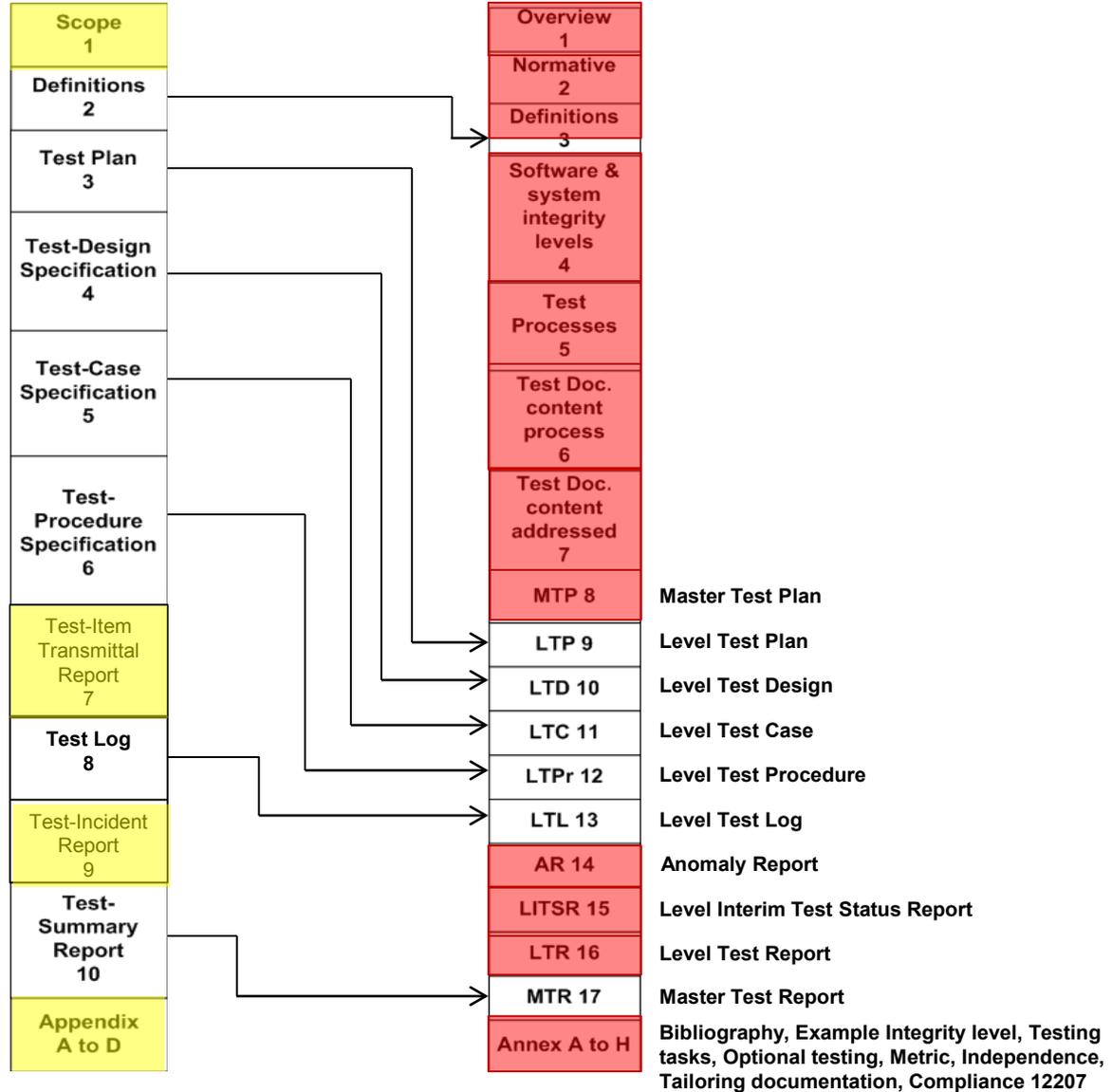
Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What changed in the IEEE 829?

- New process improvements with 2008 version
 - Provides life cycle focus and compatibility with SPLCP
 - New levels of integrity to address different types of software
 - Improves the testing documentation for retesting and resolution
 - Provides an overview methodology which includes QA [Clause 9.4]
- New documents for different testing levels, control and reporting
 - Directions for integrity level, test processes, test documentation strategies and content [Clauses 4 to 7]
 - New MTP [Clause 8]
 - Updates to Level Test Plan (LTP), Level Test Design (LTD), Level Test Case (LTC), Level Test Procedure (LTPr), Level test Log (LTL) and Master Test Report (MTR) [Clauses 9 to 13 & 17]
 - New Anomaly report (AR), Level Interim Test Status Report (LITSR), and Level Test Report (LTR) [Clauses 14 to 16]

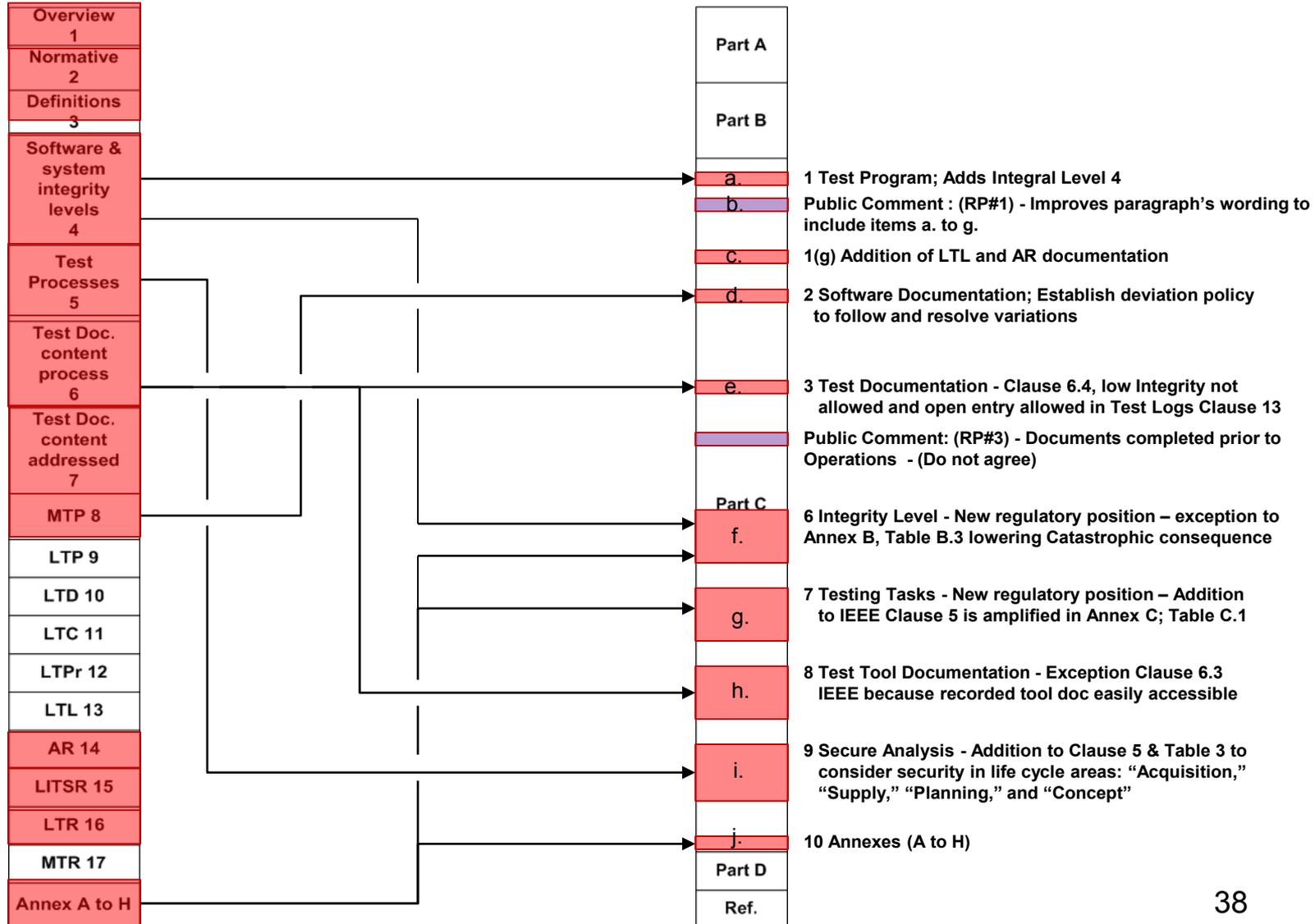
IEEE Std. 829-1983

IEEE Std. 829-2008



IEEE Std. 829-2008

RG 1.170



RG 1.170

Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Specific changes in the RG:

- Part C, 1 “Test Program” – Adds Integrity level, MTP, LTP, and new sub-clause (g) for adequate testing and error resolution
- Part C, 2 “Software Documentation” – MTP reflects suitability and sustainability and deviation is covered
- Part C, 3 “Test Documentation” – Enhance integrity exception
- Part C, 6 “Integrity Levels” – New; use Level 4, and Annex B, Table B.3, “Risk Assessment Scheme” is not acceptable
- Part C, 7 “Testing Tasks” – New; Clause 5 lists testing tasks per life cycle and Table C.1 for “Testing tasks, inputs and outputs”
- Part C, 8 “Test Tool Documentation” – New with exception to tools holding documentation
- Part C, 9 “Secure Analysis” – New; security issue task should be included on all life-cycle phases
- Part C, 10 “Annexes” – New; adds A to H

RG 1.170

Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Public comments incorporated:

- Minor grammar corrections
- Part C, 1 “Test Program” – Improved paragraph to include a. thru g.
- Part C, 3 “Test Documentation” – Document tests “prior...performing... safety functions..” (Do not agree)
- Part C, 6 “Test Program” – Noted contradiction on integrity between annexes in RG 1.170 and RG 1.168

Specific changes in the IEEE Standard:

- Original IEEE Std. 829-1983 followed by interim 1998 version...
- This RG endorses IEEE Std. 829-2008 and has the following changes:
 - Clause 1 to 3 – New outline expands plan and life-cycle orientation
 - Clause 4 “Software and system integrity” – New, defines levels 1 to 4
 - Clause 5 “Test processes” – New, provides life-cycle process directions for activities with software component (unit), component integration, systems and acceptance

Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Specific changes in the IEEE Standard: (cont'd)

- Clause 6 “Test documentation content selection process” – New, outlines needed documents and strategies for minimizing extra documents
- Clause 7 “Test documentation content topics to be addressed” – New, demonstrates test documentation multiple levels per software code
- Clause 8 “Master Test Plan” – New, outlines planning and test management through integrity schemes for all multiple levels of plans and reports
- Clause 9 “Level Test Plan” – Enhanced original clause 3 by adding new scope of purpose, traceability matrix, test management, interface with other parties and resources and QA
- Clause 10 “Level Test Design” – Enhanced original clause 4, includes direct link to Clause 9 with design approach
- Clause 11 “Level Test Case” – Enhanced original clause 5, adds generic information

RG 1.170

Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Specific changes in the IEEE Standard: (cont'd)

- Clause 12 “Level Test Procedure “ – Enhanced original clause 6
- Clause 13 “Level Test Log” – Enhanced original clause 8
- Clause 14 “Anomaly Report” – New title from original clause 9, and enhanced investigation of problems that occur
- Clause 15 “Level Interim Test Status Report” – New report
- Clause 16 “Level Test Report” – New report
- Clause 17 “Master Test Report” – Enhanced original clause 11
- In sync with changes to IEEE Std. 1074-2006 and 1012-2004

RG 1.169

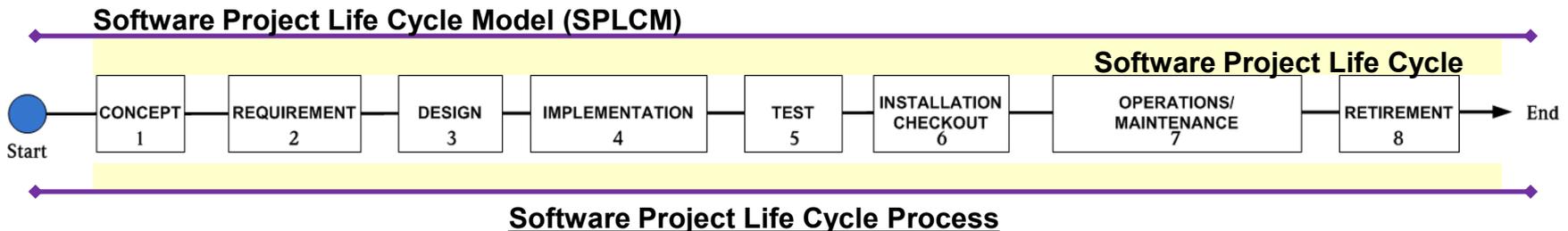
Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

- Background
- Review 6 Regulatory Guides (RGs):
 - RG 1.173 Project Management
 - RG 1.172 Software Requirements Specs
 - RG 1.171 Unit Testing
 - RG 1.170 Test Documentation
 - **RG 1.169 Configuration Management**
 - RG 1.168 V&V Review Audits
- Conclusion

Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 828-2005 directly
- Objective: Addresses an integral SPLCP need for Software Configuration Management (SCM) plan with activities for tracking and reporting software safety system history from baseline to final use
- Enables sustainability of software development with release management and delivery
- Monitors and records version iterations and extends this discipline to preexisting software



RG 1.169

Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

General overview of changes -

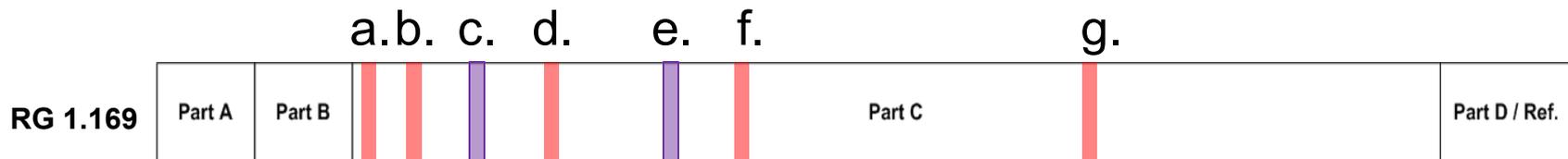
- New additions to RG 1.169 that complements supporting standard's associated changes
- 828 adds release management and delivery sub-clause
- Minor changes with management controls of SCM process
- The term changes in 828 also demonstrate alignment with the life cycle process
- RG 1.169 expands with supporting release management and preexisting software

RG 1.169

Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What changed in the RG?

- a. New activity on release management & delivery in Regulatory Position 4
- b. Includes software configuration management of contractually developed or qualified commercial software products for safety systems
- c. Public comment: remove duplication of commercial software item under Regulatory Position 6
- d. Regulatory Position 7 adds commercial grade software information on acceptance found in EPRI Topical Report (TR)
- e. Public comment: requesting NRC endorsement citation of EPRI TR
- f. New Regulatory Position 12 “Release Management and Delivery” notes Clause 3.3.7 to include sufficient control for correction of faults
- g. New Annex section (A to B)



Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What changed in the IEEE 828?

- Minimum changes to standard for 2005 version
 - Adds new Clause 3.2.4 for management of SCM's costs, surveillance of activities and types of risks
 - Covers new Clause 3.3.7 release management and delivery of software products
 - Term changes from “tailoring” to “adapting” and “audit” to “evaluation”

RG 1.169

Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Specific changes in the RG:

- Part C, 4 “Configuration Management” – Adds new activity for control of building, release and delivery of products
- Part C, 6 “Documentation” – Includes new item for data files used by software and appropriate use of regression analysis
- Part C, 8 “Development Tools” – SCM Plan should include tools
- Part C, 12 “Release Management and Delivery” – New regulatory position
- Part C, 14 “Annexes” – New, adds A & B

Public comments incorporated:

- Minor grammar corrections
- Part C, 6 “Documentation” – Dropped “k. commercial software items that are safety system software”
- Part C, 7 “Control of Purchase Materials” – Adds NRC letter endorsement

RG 1.169

Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Specific changes in the IEEE Standard:

- Original IEEE Std. 828-1990 followed by interim 1998 version
- This RG endorses IEEE Std. 828-2005 and has the following changes:
 - Clause 1 “Overview” – Dropped ANSI/IEEE 1042-1987 “IEEE Guide to Software Configuration Management”
 - Clause 3 “The Software Configuration Management Plan” – Improves control of organizational problem solving, SCM process, deviation and waivers, and software release management and delivery
 - Clause 4 “Adapting the plan” – Term “Tailoring” changed to “Adapting”
 - Annex A & B – New



RG 1.168

Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

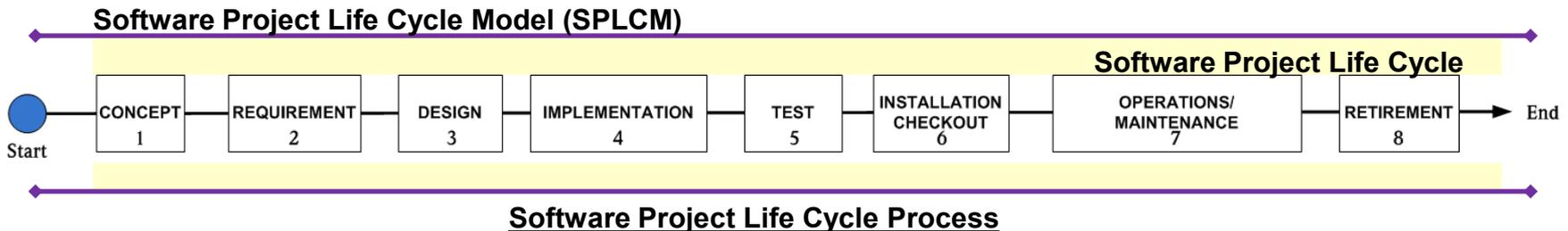
- Background
- Review 6 Regulatory Guides (RGs):
 - RG 1.173 Project Management
 - RG 1.172 Software Requirements Specs
 - RG 1.171 Unit Testing
 - RG 1.170 Test Documentation
 - RG 1.169 Configuration Management
 - **RG 1.168 V&V Review Audits**
- Conclusion

RG 1.168

Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 1012-2004 and 1028-2008 directly
- Objectives:
 - Engage in verification and validation plans that follows the SPLCP to ensure objective assessments of software safety systems
 - Provide expectations for inspectors performing walk-throughs, reviews and audits
- Follows a common framework with life cycle processes and integrity level
- Applies to developing software in the life cycle and/or preexisting or pre-developed software



RG 1.168

Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

General overview of changes -

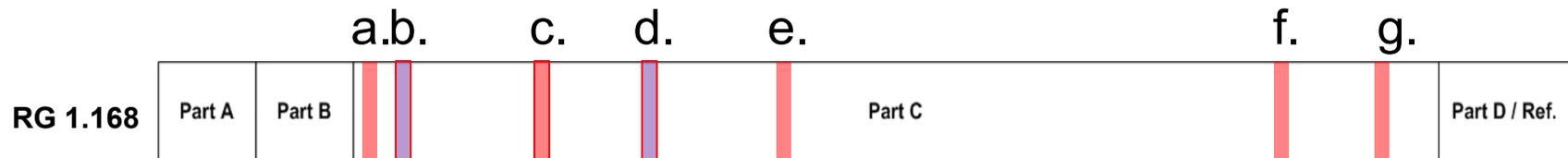
- Minimum regulatory changes to RG 1.168 with both revised standards
- These regulatory guide's exceptions and additions reflect same position on integrity and security as found in the other software regulatory guides
- Further independence clarifications are needed as the standards expand with new graded integrity options
- Both standards maintain their framework with minor sections moved or deleted
- Standards have adopted minor word and subject additions that keep the process current with software life cycle process

RG 1.168

Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What changed in the RG?

- a. New title “Software Integrity” in Regulatory Position 1
- b. Public Comment: guidance contradiction between RG 1.168 vs. 1.170
- c. Regulatory Position 3 exception to extra blocks in Annex F, figure F.1
- d. Public comment: Added an NRC citation of an EPRI topical report in Regulatory Position 4
- e. Provided new “Secure Analysis” for Regulatory Position 7(c) adding discussion of SDOE to 1012’s Clause 7.7.4
- f. New Annex: IEEE Std. 1012 (A to H) and IEEE Std. 1028 (A to B)
- g. Regulatory Position 8 takes an exception to Annex C, Table C1 conditional independence



Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What changed in the IEEE 1012?

- Re-shuffling of existing figures and reporting format with minor additions to the 2004 version
 - Provides life cycle focus and objective assessment of software products and processes
 - Maintains that software V&V be performed in parallel with software development, not at the conclusion of the development effort
 - Supports integrity level and corresponding software V&V effort
 - Adds current life cycle process improvement activities and tasks

What changed in the IEEE 1028?

- Updates to present IEEE Life Cycle nomenclature for 2008 version
 - Deletes “Anomaly class,” while moving “Anomaly ranking” to 6.8 “Data collection” and adds inspection rate table to 6.5
 - Overall updating with new descriptions and tasks for inspectors

IEEE Std. 1028-1997

| |
|-------------------------|
| Overview 1 |
| References 2 |
| Definitions 3 |
| Management reviews 4 |
| Technical reviews 5 |
| Inspections 6 |
| Walk-throughs 7 |
| Audits 8 |
| Annex A to C |

7.8.2 Anomaly Classes

7.8.3 Anomaly Ranking

Deleting Annex A

IEEE Std. 1028-2008

| |
|---------------------------|
| Overview 1 |
| Normative references 2 |
| Definitions 3 |
| |
| Management reviews 4 |
| |
| Technical reviews 5 |
| |
| |
| Inspections 6 |
| |
| |
| Walk-throughs 7 |
| Audits 8 |
| Annex A to B |

4.1 Introduction to management reviews adds plans & LC

5.1 Introduction to technical reviews adds specs & descriptions

6.1 Introduction to inspectors adds software topics to review

6.3 Inputs adds source docs, quality, & software history

6.5 Procedures adds inspection rate & author present at test

6.8.3 Anomaly ranking same as IEEE Std. 1012-2004 (no #s)

IEEE Std. 1012-1998

| |
|--|
| Overview 1 |
| Normative References 2 |
| Definitions, abbreviations, and conventions 3 |
| V&V software integrity levels 4 |
| V&V process 5 |
| Software V&V reporting, administrative and documentn requirements 6 |
| SVVP outline 7 |
| Annex A to H |

IEEE Std. 1012-2004

| |
|--|
| Overview 1 |
| References 2 |
| Definitions, abbreviations, and conventions 3 |
| Software integrity levels 4 |
| Software V&V process 5 |
| Software V&V reporting, administrative and documentn requirements 6 |
| Software V&V plan outline 7 |
| Annex A to H |

1.1 Scope & 1.3 Field of application

4 Software Integrity level updated level description with direction to select the integrity level

5 V&V intensity with integrity level

5.1 Process Management adds 4 process improvement tasks

5.4 Process Development adds LC Security analysis tasks

6.1 V&V Reporting Requirements adds 7.6 info

7 Software V&V Plan outline adds task, activity, anomaly, final and special reports

Figures 1 & 2 follow after Table 3

Exceptions to existing Annex F, Fig.1 & Annex B, Table B.3
 Exceptions to new Annex B, Table B.1 & Annex C, Table C.1

Figure 1 SV&V overview moved to after Table 3

Figure 2 Time phasing example follows Figure 1

7.6 moved to 6.1

IEEE Std. 1012-2004

| | |
|---|--|
| Overview 1 | 1.1 Scope & 1.3 Field of application |
| References 2 | |
| Definitions, abbreviations, and conventions 3 | 4 Software Integrity level updated level description with direction to select the integrity level |
| Software integrity levels 4 | 5 V&V intensity with integrity level |
| Software V&V process 5 | 5.1 Process Management adds 4 process improvement tasks 5.4 Process Development adds LC Security analysis tasks |
| Software V&V reporting, administrative and document requirements 6 | 6.1 V&V Reporting Requirements adds 7.6 7 Software V&V Plan outline adds task, activity, anomaly, final and special reports |
| Software V&V plan outline 7 | Figures 1 & 2 follow after Table 3 |
| Annex A to H | Exceptions to existing Annex F, Fig.1 & Annex B, Table B.3 Exceptions to new Annex B, Table B.1 & Annex C, Table C.1 |

RG 1.168

| | |
|--------|---|
| Part A | |
| Part B | |
| a. | 1 New title "Software Integrity" vs. old "Critical Software" |
| b. | Public Comment: (RP#1) - Contradiction resolved on Annex B, NRC takes an exception to Table B.1 & B.3 adding "critical" |
| c. | 3 Independence of software V&V - exception to Annex F blocks |
| d. | Public Comment: 4 Conformance of Material - NRC citation for EPRI Topical Report |
| Part C | |
| e. | 7(a) Secure Analysis - adds to IEEE Std. 1012-2008, Clause 7.7.4 with reference to SDOE for V&V activities |
| f. | 8 Annex (A to H) |
| g. | 8 Annex- Annex C, Tables C.1: adds "condition independence" which is not acceptable |
| Part D | |
| Ref. | |

RG 1.168

Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Specific changes in the RG:

- Part C, 1 “Software Integrity” – New title and maintaining Level 4
- Part C, 3 “Independence of Software Verification and Validation” – Diagram exception in Annex F
- Part C, 7,(c) “Secure Analysis” – New, expanding on new V&V tasks
- Part C, 8 “Annexes” – New, exception (1012) Table C.1 “Forms of IV&V”

Public comments incorporated:

- Minor grammar corrections
- Part C, 1 “Software Integrity” – Contradiction with RG 1.170, Annex B
- Part C, 4 “Control of Purchased Materials” – Missing endorsement

RG 1.168

Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

Specific changes in the IEEE Standard:

- This RG endorses IEEE Std. 1012-2004 and has the following changes:
 - Clause 4 “Software integrity levels” – Improves clarity on the integrity description and direction
 - Clause 5 “Software V&V process” – Adds optional Table 3 tasks and several new process tasks
 - Clause 6 “Software V&V reporting, administrative, and documentation requirements” – Moves V&V reporting requirements from 7.6 to 6.1
 - Clause 7 “Software V&V plan outline” – Adds “Reports” to SVVP outline

Specific changes in the IEEE Standard:

- This RG endorses IEEE Std. 1028-2008 and has the following change:
 - Clause 6 “Software V&V reporting, administrative, and documentation requirements” – Adds table of inspection rates with anomaly ranking



- Background
- Review 6 Regulatory Guides (RGs):
 - RG 1.173 Project Management
 - RG 1.172 Software Requirements Specs
 - RG 1.171 Unit Testing
 - RG 1.170 Test Documentation
 - RG 1.169 Configuration Management
 - RG 1.168 V&V Review Audits
- **Conclusion**

Conclusion

- RGs updated and support NRC guidance
- RGs provide cohesive approach
- Common topics contemplated
- Key public comments addressed
- RGs ready for publication

Acronyms

- **ACRS – Advisory Committee on Reactor Safeguards**
- **ADAMS – Agencywide Documents Access and Management System**
- **ANSI – American National Standards Institute**
- **AR – Anomaly Report**
- **CFR – Code of Federal Regulations**
- **DI&C – Digital Instrumentation and Control**
- **eDF – Électricité de France**
- **EPRI – Electric Power Research Institute**
- **IEC – International Electrotechnical Commission**
- **IEEE – Institute of Electrical and Electronics Engineers**
- **RG – Regulatory Guidance**
- **ISG – Interim Staff Guidance**
- **JPL – Jet Propulsion Lab**
- **LER – Licensee Event Report**
- **LITSR – Level Interim Test Status Report**
- **LTC – Level Test Case**
- **LTD – Level Test Design**
- **LTL – Level Test Log**
- **LTP – Level Test Plan**
- **LTPr – Level Test Procedure**
- **LTR – Level Test Report**
- **MTP – Mast Test Plan**
- **MOU – Memorandum Of Understanding**
- **NASA – National Aeronautics and Space Administration**
- **NEA – Nuclear Energy Agency**

Acronyms

- **NRC – U.S. Nuclear Regulatory Commission**
- **NRR – Office of Nuclear Reactor Regulation**
- **NRO – Office of New Reactors**
- **NSIR – Nuclear Security and Incident Response**
- **NPP – Nuclear Power Plant**
- **OpE – Operational Experience**
- **QA – Quality Assurance**
- **RES – Office of Nuclear Regulatory Research**
- **SCM – Software Configuration Management**
- **SDOE – Secure Development and Operational Environment**
- **SPLC – Software Project Life Cycle**
- **SPLCP – Software Project Life Cycle Process**
- **SPLCM – Software Project Life Cycle Model**
- **SRM – Staff Requirement Memoranda**
- **SRS – Software Requirements Specification**
- **SwA – Software Assurance**
- **TR – Topical Report**
- **SVVP – Software Verification and Validation Plan**
- **V&V – Verification and Validation**

References:

Beizer, B., *Software Testing Techniques*, Van Nostrand Reinhold, New York, NY, 1990.

Code of Federal Regulations (CFR), *Title 10, Energy*, Part 50,
“Domestic Licensing of Production and Utilization Facilities.”

Electric Power Research Institute (EPRI) Topical Report TR-106439,
“Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” EPRI, Palo Alto, CA, October 1996. (ADAMS Accession No. ML092190664)

IEEE Std. 1074-2006, “IEEE Standard for Developing a Software Project Life Cycle Process,”
IEEE, Piscataway, NJ, 2006.

IEEE Std. 830-1998, “IEEE Recommended Practice for Software Requirements Specifications,”
IEEE, Piscataway, NJ, 1998.

IEEE Std. 1008-1987, “IEEE Standard for Software Unit of Testing,” IEEE, Piscataway, NJ, 1987.

IEEE, Std. 829-2008, “IEEE Standard for Software and System Test Documentation,”
IEEE, Piscataway, NJ, 2008.

IEEE Std. 828-2005, “IEEE Standard for Software Configuration Management Plans,”
IEEE, Piscataway, NJ, 2005.

IEEE, Std. 1012-2004, “IEEE Standard for Software Verification and Validation,”
IEEE, Piscataway, NJ, 2004.

IEEE, Std. 1028-2008, “IEEE Standard for Software Reviews and Audits,” IEEE, Piscataway, NJ, 2008.

Backup

Change Comparison between Standards

1074-2006

| |
|--------------------------------|
| Overview 1 |
| Definitions and acronyms 2 |
| Key Concepts 3 |
| Implementing the standard 4 |
| Annex A.1 |
| Annex A.2 |
| Annex A.3 |
| Annex A.4 |
| Annex A.5 |
| Annex B to F |

830-1998

| |
|---|
| Overview 1 |
| References 2 |
| Definitions 3 |
| Considering for producing a good SRS 4 |
| The parts of an SRS 5 |
| Annex A & B |

1008-1987

| |
|------------------------------|
| Scope and References 1 |
| Definitions 2 |
| Unit Testing Activities 3 |
| Annex A to D |

829-2008

| |
|---|
| Overview 1 |
| Normative 2 |
| Definitions 3 |
| Software & system integrity levels 4 |
| Test Processes 5 |
| Test Doc. content process 6 |
| Test Doc. content addressed 7 |
| MTP 8 |
| LTP 9 |
| LTD 10 |
| LTC 11 |
| LTPr 12 |
| LTL 13 |
| AR 14 |
| LITSR 15 |
| LTR 16 |
| MTR 17 |
| Annex A to H |

828-2005

| |
|---|
| Overview 1 |
| Definitions and acronyms 2 |
| The Software Configuration Management Plan 3 |
| Adapting the Plan 4 |
| Conformance to the standard 5 |
| Annex A & B |

1028-2008

| |
|---------------------------|
| Overview 1 |
| Normative references 2 |
| Definitions 3 |
| Management reviews 4 |
| Technical reviews 5 |
| Inspections 6 |
| Walk-throughs 7 |
| Audits 8 |
| Annex A to B |

1012-2004

| |
|---|
| Overview 1 |
| References 2 |
| Definitions, abbreviations, and conventions 3 |
| Software integrity levels 4 |
| Software V&V process 5 |
| Software V&V reporting, administrative and document requirements 6 |
| Software V&V plan outline 7 |
| Annex A to H |

Backup

Change Comparison between Regulatory Guides

RG 1.173

| |
|--------|
| Part A |
| Part B |
| a. |
| b. |
| c. |
| Part C |
| d. |
| Part D |
| Ref. |

RG 1.172

| |
|--------|
| Part A |
| Part B |
| a. |
| b. |
| c. |
| Part C |
| d. |
| Part D |
| Ref. |

RG 1.171

| |
|--------|
| Part A |
| Part B |
| a. |
| b. |
| Part C |
| c. |
| Part D |
| Ref. |

RG 1.170

| |
|--------|
| Part A |
| Part B |
| a. |
| b. |
| c. |
| d. |
| e. |
| Part C |
| f. |
| g. |
| h. |
| i. |
| j. |
| Part D |
| Ref. |

RG 1.169

| |
|--------|
| Part A |
| Part B |
| a. |
| b. |
| c. |
| d. |
| e. |
| f. |
| Part C |
| g. |
| Part D |
| Ref. |

RG 1.168

| |
|--------|
| Part A |
| Part B |
| a. |
| b. |
| c. |
| d. |
| Part C |
| e. |
| f. |
| g. |
| Part D |
| Ref. |