

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
505th Meeting

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005

Docket Number: (not applicable)

Location: Rockville, Maryland

Date: Friday, September 12, 2003

Work Order No.: NRC-1069

Pages 1-52

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

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

TRO4

ORIGINAL

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) 505TH MEETING

+ + + + +

FRIDAY

SEPTEMBER 12, 2003

+ + + + +

ROCKVILLE, MARYLAND

The Committee was called to order at 8:30
a.m., at the Nuclear Regulatory Commission, Two White
Flint North, Room T2B3, 11545 Rockville Pike, Dr.
Mario V. Bonaca, Chairman, presiding.

COMMITTEE MEMBERS PRESENT:

- DR. MARIO BONACA, ACRS Chairman
- DR. GRAHAM B. WALLIS ACRS Vice Chairman
- DR. GEORGE E. APOSTOLAKIS ACRS Member
- DR. THOMAS S. KRESS ACRS Member
- DR. GRAHAM M LEITCH ACRS Member
- DR. DANA A. POWERS ACRS Member
- DR. VICTOR H. RANSON ACRS Member
- DR. STEPHEN L. ROSEN ACRS Member-at-Large
- DR. WILLIAM J. SHACK ACRS Member
- DR. JOHN SIEBER ACRS Member

1 ACRS STAFF PRESENT:

2 SHER BAHADUR Associate Director, ACRS

3 SATISH AGGARWAL NRR

4 RAMIN ASSIN RES

5 MARK BLUMBERG NRR/DSSA/SPSB

6 SAM DURAISWAMY Designated Federal Official

7 RALPH CARUSO ACRS Staff

8 O.M.P. CHOPRA NRR/DE/EEIB

9 CLIFF DOUTT NRR/DSSA/SPS

10 MICHELLE HART NRR/DE/EEIB

11 HOWARD J. LARSON Special Assistant, ACRS

12 PAUL LOESER NRR/DE/EEIB

13

I-N-D-E-X

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

AGENDA ITEM

PAGE

I. Opening Comments Chairman Bonaca

4

II. Presentation by Mr. Aggarwal

7

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

(8:30 a.m.)

CHAIRMAN BONACA: Good morning. The meeting will now come to order. This is the third day of the 505th meeting of the Advisory Committee On Reactor Safeguards. During today's meeting the committee will consider the following.

Draft final revision-1 to Regulatory Guide 1.53, application of the single failure criteria to safety systems.

Preparation for meeting with the NRC Commissioners. The subcommittee report on fire protection issues. Future ACRS activities and a report of the planning and procedures subcommittee. Reconciliation of the ACRS comments and recommendations; and proposed ACRS reports. Seven of those.

A portion of this meeting will be closed to discuss a proposed ACRS report on safeguards and security.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Sam Duraiswamy is the designated Federal Official for the initial portion of the meeting.

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

1 We have received no written comments or
2 requests for time to make oral statements from
3 members of the public regarding today's sessions. A
4 transcript of portions of the meeting is being kept,
5 and it is requested that the speakers use one of the
6 microphones, identify themselves, and speak with
7 sufficient clarity and volume so that they can be
8 readily heard.

9 Now, before we start on the first item
10 on the agenda, I would like to just make a brief
11 announcement regarding the agenda itself, okay? Dr.
12 Wallis has to leave by 3:00 p.m., and also Dr.
13 Apostolakis, I believe, shortly after?

14 DR. APOSTOLAKIS: No, before.

15 CHAIRMAN BONACA: So, what I would like
16 to do after the first presentation and discussion,
17 and before the preparation for the meeting with the
18 Commissioners, we will get a reading of Graham's
19 letter so that we can give him feedback, and back to
20 it in the early afternoon.

21 And also a reading of George's letter,
22 and hopefully we can even approve it maybe.

23 DR. APOSTOLAKIS: As far as I am
24 concerned, you can approve it right now.

25 CHAIRMAN BONACA: I don't want to pre-

NEAL R. GROSS

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

1 judge it. So with that, I will turn to Dr. Shack,
2 who is going to lead us through this presentation.
3 Be aware of the timing issue that we have. We have
4 a very tight schedule, and I am sure that you will
5 be policing this hour.

6 DR. SHACK: You kept such tight control
7 yesterday, right. You set such a good example
8 yesterday.

9 CHAIRMAN BONACA: I am not sure about
10 that.

11 MR. AGGARWAL: We will try to help you
12 and not ask too many questions.

13 CHAIRMAN BONACA: Today I will make a
14 better example.

15 DR. SHACK: One thing that I would like
16 to point out to the members is that our revised
17 draft final has been revised once more. You have a
18 memo from Mike Snodderly, which contains some last
19 minute changes.

20 These are mostly again to address the
21 possibility that every time you revise a reg guide
22 that there is always this concern about back fits,
23 and again this will -- the reg guide is intended for
24 essentially applications for all future discussions,
25 and can be adopted voluntarily by licensees who are

NEAL R. GROSS

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

1 making changes, but it is intended as a back fit.

2 In addition to Satish Aggarwal, who is
3 the author of the reg guide, we also have a
4 distinguished visitor today, Mr. David Zaprazny, who
5 is the Chairman of the IEEE working group.
6 Basically the reg guide endorses an IEEE standard
7 379-2000, and Mr. Zaprazny is the chairman of the
8 working group that developed the new standard, and I
9 will turn it over to Satish then to discuss the reg
10 guide.

11 MR. AGGARWAL: Good morning. Before I
12 provide the background on the reg guide, let me at
13 the outset state that the purpose of this briefing
14 today is to seek your concurrence with this staff
15 position in respect to single phase criteria to
16 safety systems.

17 So we are hoping at the conclusion of
18 our presentations that subsequently we will receive
19 a letter to that effect. Now, let me first of all
20 make it clear what is a single failure.

21 You all know power instrumentation and
22 control portion of each safety system consists of
23 more than one safety group, and any one of which can
24 complete the safety function.

25 Thus, a safety system must perform all

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

1 safety functions required for a design basis event
2 in the presence of any detectable failure within the
3 safety system. And in a nutshell is the single
4 failure criteria.

5 DR. APOSTOLAKIS: So the idea of a
6 single failure then applies to a well-defined system
7 and not a function?

8 MR. AGGARWAL: That's right.

9 DR. APOSTOLAKIS: So if I consider the
10 function of removing decayed heat, I will not
11 necessarily think in terms of a single failure that
12 I am losing one system, and therefore I have a
13 redundant system, right? That is a different kind
14 of concept?

15 MR. AGGARWAL: If you look at the safety
16 functions, and you look at your more than one group
17 that performs that safety function, and you fail one
18 of the functions, and show to me that you will still
19 be able to perform. I will present some more
20 examples as we proceed.

21 DR. APOSTOLAKIS: So it applies to
22 functions as well and not just systems?

23 MR. AGGARWAL: It applies to both.

24 DR. APOSTOLAKIS: So if my function is
25 to inject water under high pressure into the core, I

1 must have at least one way of doing this?

2 MR. AGGARWAL: Exactly. That is a given
3 design, and we are saying show it to us, and this is
4 single failure.

5 DR. APOSTOLAKIS: Even if the system is
6 highly redundant and meets the criteria and not the
7 system level?

8 MR. AGGARWAL: Right.

9 DR. APOSTOLAKIS: Wow.

10 MR. AGGARWAL: And the specific design
11 is nothing new. This has been there for years.
12 This is fundamental to a nuclear power plant design.

13 DR. LEITCH: But let's say, for example,
14 in a boiling water reactor, in George's scenario,
15 you want to inject water at high pressure. So you
16 have the HPSI system and if that fails, there is no
17 direct replacement for it.

18 What you have is an alternate means to
19 blow the reactor down to low pressure and then
20 inject. So --

21 MR. AGGARWAL: Exactly. You have to
22 show how you can accomplish that function by a
23 different matter.

24 DR. APOSTOLAKIS: So, wait, that is a
25 good example. You are not really accomplishing the

NEAL R. GROSS

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

1 function, because you don't have another way of
2 injecting water under high pressure.

3 MR. AGGARWAL: Right.

4 DR. APOSTOLAKIS: But you are getting
5 around it by reducing the pressure?

6 MR. AGGARWAL: Reducing the pressure and
7 then injecting the pressure.

8 DR. APOSTOLAKIS: So essentially you are
9 managing the accident --

10 MR. AGGARWAL: Right, mitigating it.

11 DR. APOSTOLAKIS: In more than one way.

12 MR. AGGARWAL: I just wanted to clear
13 where --

14 DR. APOSTOLAKIS: Well, you are doing a
15 very good job.

16 MR. AGGARWAL: Thank you.

17 DR. APOSTOLAKIS: But would this apply
18 to advanced reactors as well?

19 MR. AGGARWAL: It should apply to all.

20 DR. APOSTOLAKIS: Okay.

21 DR. LEITCH: I always thought to carry
22 that example a little bit further that single
23 failure was really that -- well, to continue to talk
24 about HPSI, for example, and a piece of
25 instrumentation on the HPSI system would not -- that

NEAL R. GROSS

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

1 is, the failure of a piece of instrumentation would
2 not render the HPSI system inoperable, and there
3 would be another piece of instrumentation that would
4 trigger the HPSI system to initiate, for example.

5 MR. AGGARWAL: By design all safety
6 related equipment should be able to perform its
7 function. Single failure is saying that you take
8 one system, one increment, fail it, and show me how
9 you can accomplish the purpose of the function and
10 mitigate the accident.

11 DR. WALLIS: This is a very difficult
12 thing, because a system is a meaningless word. I
13 mean, a system encompasses whatever you want it to
14 encompass. So I could say the ECCS system, and that
15 is everything, and that is accumulators, and --

16 DR. APOSTOLAKIS: That's why I went to
17 the function level.

18 DR. WALLIS: Yes, but even then you have
19 got to say how are you going to divide the
20 functions. I mean, keeping the core cool is a
21 function.

22 DR. APOSTOLAKIS: But the reality is
23 that the actual function -- well, I mean, what you
24 do is you are looking for the worst single failure.
25 So you are going sensitivities on individual trains,

NEAL R. GROSS

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

1 and not functions, until you find the one which is
2 the most limiting one, and then you assume that one.

3 DR. WALLIS: That is very different
4 though. You have got three trains and one is out of
5 order, you can still perform the function with two.

6 DR. APOSTOLAKIS: Exactly.

7 DR. WALLIS: And that is quite different

8 MR. AGGARWAL: May I suggest that you
9 hold that thought and let's proceed, and we will
10 give you the imperfect examples to make a point, and
11 tell you what that all means.

12 CHAIRMAN BONACA: Now, is this
13 consistent with the move towards risk-informed
14 regulations? Probably not.

15 MR. AGGARWAL: Not really. What we are
16 going to talk about is the PRA in a minute. Also, I
17 would like to point out that the single failure
18 could occur prior to or at any time, during or the
19 DBE for which the safety system is required to
20 function.

21 It is a given, but keep these two ideas
22 in mind as we progress. Now, I --

23 DR. APOSTOLAKIS: Now, if I said that
24 the single failure criteria means a specific
25 implementation of the concept of defense in depth, I

NEAL R. GROSS

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

1 would be right, right?

2 MR. AGGARWAL: Yes.

3 DR. APOSTOLAKIS: It just makes that
4 concept specific and implementable in a particular
5 case.

6 MR. AGGARWAL: That's correct.

7 DR. APOSTOLAKIS: All right.

8 DR. SHACK: And this only holds true, of
9 course, during design basis events.

10 DR. APOSTOLAKIS: True. True.

11 DR. ROSEN: Well, the whole idea of risk
12 informing the regulations is that we know serious
13 events don't have just a single failure. There is
14 almost never a significant event with just one thing
15 happening.

16 DR. SHACK: Well, you design it with
17 just a single failure event, period.

18 DR. ROSEN: All serious events, not just
19 in the nuclear industry, but in all industries, are
20 combinations of multiple issues.

21 MR. AGGARWAL: Well, if I may proceed,
22 let me give you the feedback background under that
23 guide. The issue that (inaudible) 11-18 for public
24 comments.

25 DR. ROSEN: Well, excuse me, but I may

1 have missed this. Why are you doing this?

2 MR. AGGARWAL: Why are we doing it?

3 This is the commission policy to look at the IEEE on
4 a national consensus standard on single failure
5 criteria, whether they meet our regulations or not.
6 If they do, we would like to introduce them in a reg
7 guide or regulation.

8 DR. ROSEN: This is a national standard
9 on single failure criteria

10 MR. AGGARWAL: Yes, sir. What you have
11 is a national consensus standard.

12 DR. ROSEN: But who issued it?

13 MR. AGGARWAL: IEEE.

14 DR. APOSTOLAKIS: It applies only to
15 nuclear facilities?

16 MR. AGGARWAL: That's right.

17 DR. APOSTOLAKIS: So why should IEEE
18 care?

19 MR. AGGARWAL: Well, if you would like
20 to circulate that standard among the members.

21 DR. APOSTOLAKIS: Why would IEEE care
22 about nuclear facilities?

23 MR. AGGARWAL: Sir, George, IEEE assigns
24 the maximum number of standards for operations in
25 nuclear power plants.

NEAL R. GROSS

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

1 DR. APOSTOLAKIS: Well, I can see them
2 publishing standards for instrumentation and
3 control, and things --

4 DR. SHACK: This is single failure for
5 instrumentation control systems.

6 MR. AGGARWAL: Power, and electrical,
7 and --

8 DR. APOSTOLAKIS: Oh, it is not general?

9 MR. AGGARWAL: No, this is what my first
10 opening line was, that the (inaudible) control
11 systems.

12 DR. APOSTOLAKIS: I think though the --

13 CHAIRMAN BONACA: The question I think
14 is that this kind of concept somewhat, which I think
15 is very appropriate for a component or system, et
16 cetera, is really a casualty analysis to determine
17 how it is capable of performing its function with a
18 failure in it, was really translated later on in the
19 accident analysis it seems to me.

20 When instead you have a much more
21 complex grouping of systems, et cetera, and you
22 should consider possible multiple offenders, I
23 think.

24 DR. APOSTOLAKIS: Well, this was
25 actually a very good when it was proposed.

1 CHAIRMAN BONACA: Well, sure.

2 DR. APOSTOLAKIS: But it really makes
3 sure that you don't have single element minimal
4 concepts. That is really what it does.

5 MR. AGGARWAL: Exactly.

6 MR. LOESER: And in this case the
7 original document that was endorsed was dated 1972.
8 A lot has happened since then, and --

9 DR. APOSTOLAKIS: The reactor safety
10 study, for example.

11 MR. LOESER: And in this case there have
12 been several other versions that have not been
13 endorsed. I am not sure why. But we decided that
14 it was time to endorse the latest one, the 2000, and
15 that is what this draft guide is for, is to help
16 update Reg. Guide 153 to a remedial standard.

17 DR. POWERS: Let me ask, and I may be
18 asking this question out of turn here, but I will
19 ask it anyway. When you think about modern
20 electrical systems, and you say the failure is when
21 there is a termination of the ability to perform its
22 intended function.

23 And I think about software controlled
24 digital systems with design requirements embedded in
25 them that may in fact be flawed. So the system does

NEAL R. GROSS

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

1 not perform the function that one group of people
2 intended it to do, but the other group of people
3 definitely didn't address that because they didn't
4 put the requirements on the software to address that
5 particular set of circumstances. Have we had a
6 single failure?

7 MR. LOESER: Yes, and that's why the
8 branch technical position 19 requires a diverse
9 method not subject to the same single failure to
10 accomplish the same basic function.

11 That's why if you have all of the
12 software and all four channels using identical
13 software, they is supposed to be some alternative
14 way in case that software fails to perform its
15 function, whether by specification error, or coding
16 error, or just something else.

17 If there is a common failure of all the
18 systems using that software the plant still has to
19 be able to survive.

20 DR. POWERS: That is what we have done
21 on safety. What I am really asking is that with
22 regard to the standard have we had a single failure?

23 MR. ZAPRAZNY: Yes. Design error can be
24 a single failure.

25 DR. POWERS: And so the fact that these

1 guys developed a piece of electrical equipment, and
2 it meets all of their requirements, but it just does
3 not happen to meet what the systems requirements
4 are. There has been a failure, and their failure.

5 DR. APOSTOLAKIS: A design error can be
6 a single failure as long as it affects one
7 component. I don't think you are dealing with
8 common cause failure.

9 MR. ZAPRAZNY: It is dealing with common
10 cause failure, yes, and that is addressed in the
11 standard.

12 MR. AGGARWAL: And then I also might
13 point out that that there is this IEEE 7.432, which
14 addresses the basic issues raised.

15 DR. POWERS: I know it is, and --

16 MR. AGGARWAL: And which we have
17 endorsed.

18 DR. POWERS: And you brought that before
19 us, and we spent hours trying to understand
20 everything there.

21 MR. AGGARWAL: Right.

22 DR. POWERS: I was just looking at the
23 definition of your standard and trying to think
24 about what was missing, and what you brought up, I
25 think I understood. But it is a question with

NEAL R. GROSS

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

1 respect to this standard itself, and whether that
2 was recognized as a failure, because I would not
3 have.

4 They did, but I would not have if I were
5 kind, but that's okay. That's okay.

6 DR. APOSTOLAKIS: You will talk about
7 common cause failures later?

8 MR. AGGARWAL: Yes.

9 DR. APOSTOLAKIS: Okay.

10 MR. AGGARWAL: I did say earlier that we
11 received four comments letters, and as a result of
12 those comments letters, we made a few minor changes
13 in the (inaudible) section.

14 I might point out that comment letters
15 may be found to be long, several pages, but what is
16 contained on those comment letters is noting new.
17 One of the lawyer firms sent this letter every time
18 he devised an electrical regulation or reg guide,
19 bringing up fundamental issues which the Commission
20 had addressed before, in terms of the rule making
21 when their endorsement of IEEE Standard 603, and
22 more specifically 10 CFR 50 (a) (h) subparagraphs.

23 So we met with CRGR to discuss this reg
24 guide and seek their endorsement, and it might also
25 be noted that when we issued the draft reg guide, in

NEAL R. GROSS

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

1 the implementation section, we are given the option
2 that you can use the old one and be subject to
3 review by the staff on a case-by-case basis, or you
4 can use the civilian.

5 This language we have used at the
6 insistence of CRGR, and brought it (inaudible) in
7 the industry, because the project changed, and the
8 change was not acceptable to the public.

9 This (inaudible) something be done in
10 this language, and they didn't like it, okay? In
11 other to resolve this, if you will turn over to the
12 next page, the final reg guide.

13 This is the language that we have been
14 using in all reg guides over the last 10 years, and
15 so all we did was bring it to the same language
16 which is accepted by the industry and in our opinion
17 and OGC's opinion it not clear.

18 The bottom line is that backfitting is
19 not intended. Now in doing so, and the industry
20 raises the issue of safety systems, protection
21 system, and what not, CRGR asked us in the Section
22 A, and this is a reg guide, dated August 25th, 2003,
23 and copies of which have been provided to the
24 committee.

25 And this is under Section A, which we

NEAL R. GROSS

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

1 expanded to clarify what a safety function means,
2 and what a protection system means, and all this
3 information is nothing new. It was already there
4 when we were doing the rule making.

5 So it is simply that we are reproducing
6 it here, and in the instrumentation section, we made
7 it clear that no backfitting is intended, and this
8 will be used for the operating plants on a voluntary
9 basis if there are any modifications proposed by the
10 licensee,

11 DR. LEITCH: What does the word evaluate
12 mean? In other words, if a license voluntarily
13 proposes modifications to a safety system that do
14 not comply, then that is a cause for a rejection of
15 that modification?

16 MR. AGGARWAL: Technically, this is one
17 matter that the staff will accept without question.
18 The licensee is always free to come up with an
19 orderly matter of accomplishing it.

20 And naturally that will be evaluated by
21 this staff and that is all that it means.

22 MR. LOESER: In this particular case, if
23 they had previously committed, for example, to the
24 1972 version --

25 MR. AGGARWAL: Right.

NEAL R. GROSS

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

1 DR. LEITCH: -- and their new
2 modification met the 1972 version, but did not meet
3 the 2002 version that's okay?

4 DR. LEITCH: That's okay. Okay.

5 MR. LOESER: There is not a requirement
6 for them to meet this new one, because there is no
7 backfit required as long as they meet the
8 commitments that they made at the time of their
9 license.

10 DR. LEITCH: Okay. And obviously an
11 encouragement to do so, but not a requirement to do
12 so.

13 MR. LOESER: That's exactly correct.

14 DR. LEITCH: I understand. Thank you.

15 MR. AGGARWAL: At this time I would like
16 to raise or discuss the issues of the significant
17 technical changes between 1972 and what we are
18 endorsing now.

19 The first item is that in the current
20 version which you have before you, we have included
21 a requirement for a single failure analysis in
22 design using digital computers.

23 And that brings you to the IEEE Standard
24 603, and 7-4.3.2. Incidentally, I might point out
25 to the committee that if the standard had been

NEAL R. GROSS

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

1 revised and approved by the IEEE standard vote
2 yesterday, and we would have Standard 7-4.3.2, which
3 is still a much more improved standard for guidance
4 in the digital computers.

5 And it is the staff's intention to
6 endorse that standard in the near future, and so we
7 will be back to you again explaining to you how we
8 are going to meet all these requirements in terms of
9 digital computers.

10 DR. LEITCH: Let me ask another question
11 and perhaps that I should have asked earlier. Those
12 definitions that you referred to right at the
13 beginning of your talk, are they different in the
14 new standard versus the 1973 standard, or are they
15 still the same old definition?

16 MR. AGGARWAL: They are different. They
17 are much more improved based on our experience, and
18 clarity. If you would like to hear, we can tell
19 you exactly what changed, but it includes improved
20 language just for clarity.

21 And even in the reg guide, I had made
22 this point very clear what that really means,
23 because I know often that the term single failure is
24 misunderstood, and so I thought that this is the
25 time that we put that to bed, and this is exactly --

NEAL R. GROSS

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

1 yes, sir?

2 DR. APOSTOLAKIS: I guess I am still
3 struggling to understand what the single failure is.
4 The safety systems you say here will be capable of
5 performing the required safety functions. Is a
6 single failure an actual failure, or could it be a
7 cause for failure of 3 or 4 different systems?

8 MR. AGGARWAL: It could be either.

9 DR. APOSTOLAKIS: It could be a cause.

10 MR. AGGARWAL: Right.

11 MR. LOESER: Well, in this case, when
12 you consider a single failure, you have to consider
13 not only the failure itself, but all the subsequent
14 failures that that causes.

15 For example, a software failure could
16 cause more than one component to fail, because there
17 is more than one component using that software.

18 DR. APOSTOLAKIS: Right.

19 MR. LOESER: So you have to use sort of
20 a trickle down effect. If you have a power spike of
21 some sort and that equipment that is not fused,
22 everything that power spike will blow out is part of
23 that single failure.

24 DR. APOSTOLAKIS: So you are moving now
25 towards PRA, and that is really what you are doing.

NEAL R. GROSS

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

1 MR. LOESER: Well --

2 DR. APOSTOLAKIS: You are considering
3 the consequences of a failure.

4 MR. LOESER: We are not doing this on a
5 -- well, it is a cause and effect, and not only the
6 failure itself, but all subsequent failures that
7 that failure causes are all part of the same single
8 failure.

9 DR. ROSEN: I would say it is more like
10 failure modes and effects.

11 MR. LOESER: That is actually correct.

12 MR. AGGARWAL: You're right.

13 DR. APOSTOLAKIS: Yes, but the initiator
14 here must be a failure itself, and not a cause. In
15 other words, it can not be human error of omission
16 or commission.

17 It has to be an actual failure. As you
18 said, you know, power fails, and then it
19 propropagates. But it cannot be a cause that is not a
20 failure by itself. That is the way that I
21 understand it.

22 MR. ZAPRAZNY: If you have a circuit
23 breaker fail on a load center --

24 DR. APOSTOLAKIS: Well, that is a
25 failure.

1 MR. ZAPRAZNY: But your failure results
2 in loss of all the --

3 DR. APOSTOLAKIS: Fine, fine, I
4 understand that.

5 DR. ROSEN: And then later on the
6 sequence, if there is an operator action required,
7 and the operator fails to do it, that is not one
8 failure. That is two failures.

9 DR. APOSTOLAKIS: Right. And the other
10 question is how about passive failures? I mean,
11 does that make sense in this context?

12 MR. AGGARWAL: It does, and I intend to
13 touch on that area.

14 DR. APOSTOLAKIS: So if I have a fire
15 that just deteriorates and all of a sudden I have a
16 hot short, that is a failure?

17 MR. AGGARWAL: Yes.

18 MR. LOESER: A failure to do something
19 is not considered any differently than a failure to
20 not do something. So a failure to trip or a failure
21 for a component to react because it is burned out,
22 or because a wire worked its way loose or something,
23 a failure to act in some manner is still a failure.

24 But I think that there is an important
25 difference between electrical and mechanical

NEAL R. GROSS

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

1 systems. In the mechanical systems, you don't
2 consider a pipe failure as a single failure. I
3 think there is a fundamental difference here.

4 DR. ROSEN: Well, that is an initiating
5 event, and we consider the pipe failure the
6 initiating event, and then we test the responses for
7 the single failure criteria.

8 MR. AGGARWAL: Right.

9 DR. APOSTOLAKIS: So that is a design
10 basis failure?

11 MR. ZAPRAZNY: Once again, a pipe
12 failure is a passive failure which is a single
13 failure.

14 DR. APOSTOLAKIS: No, that is --

15 DR. ROSEN: That is the initiating
16 event.

17 DR. APOSTOLAKIS: -- the initiating. It
18 is a DBE, but it is not -- because here you said
19 even with a DBE, I don't want a single failure to
20 disable the system.

21 MR. LOESER: I think you would have to
22 differentiate which pipe. If you are talking about
23 a pipe that causes the event, but if there is some
24 other valve that is now supposed to open, or a pipe
25 that is supposed to transmit water to alleviate this

NEAL R. GROSS

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

1 situation to mitigate the accident, then that
2 failure would be the single failure.

3 DR. APOSTOLAKIS: But that is the
4 system.

5 CHAIRMAN BONACA: It is the system, and
6 so you are not supposed to assume two pipe failures.

7 MR. LOESER: That's correct.

8 DR. APOSTOLAKIS: In other words, if I
9 have an initiating event that comes from a pipe
10 failure, a single failure cannot be another pipe
11 failure.

12 CHAIRMAN BONACA: Or any other component
13 that --

14 DR. APOSTOLAKIS: Is that consistent
15 with -- would a system failure be another passive
16 failure?

17 CHAIRMAN BONACA: No.

18 MR. LOESER: Wait a second. It could.
19 I think there is a difference. If you had an
20 initiating event -- for example, a computer in the
21 feedwater system failing to do whatever it is
22 supposed to do in cutting off feedwater; another
23 electrical failure in a digital system, or in a
24 valve, or anything else, would be a single failure
25 even if the failure is similar to a software .

NEAL R. GROSS

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

1 failure.

2 It is not like the -- I mean, the single
3 failure could be very similar to the one that
4 initiated the event.

5 DR. APOSTOLAKIS: Yes, in that sense
6 they are different from mechanical systems.

7 MR. AGGARWAL: I might bring to the
8 attention of the committee that this particular
9 slide is addressing the issue of shared system, and
10 what I intend to bring to your attention that IEEE
11 standards describe the manner in which single
12 failure criteria should be applied to shared
13 systems.

14 The intent is neither to endorse or
15 (inaudible) the hearing between the system, the
16 standard for minimum requirements to ensure that
17 shared systems are analyzed as adversely as possible
18 to ensure that the fact of component failures as
19 there was no sharing.

20 That is a very simple thing, that you
21 can share systems, but you still have to have
22 (inaudible). So this is a new addition to the IEEE
23 standard 379.

24 DR. APOSTOLAKIS: Is it shared systems
25 or shared components?

1 MR. AGGARWAL: Shared systems. But
2 shared components are a part of the system.

3 DR. APOSTOLAKIS: Give me an example of
4 a shared system.

5 MR. AGGARWAL: You might have the same
6 diesel which you might be sharing between the two
7 units.

8 DR. ROSEN: A start-up boiler at a plant
9 that has two units, and that would share the piping
10 and the boiler.

11 MR. AGGARWAL: In some old plants the
12 D.C. power is shared, and I am in 372 in terms of
13 control So essentially as I was speaking to you
14 about the shared system, and these are the two basic
15 criteria which are in this standard, that the safety
16 system of each unit shall be capable of performing
17 their required safety function, and with a single
18 failure initiative concurrently in each unit within
19 the system that are not shared.

20 Number 2, for reasons that will be
21 included in the design to ensure that a single
22 failure within one unit will not adversely affect
23 the other unit, thereby preventing the shared system
24 from performing the required safety function.

25 DR. APOSTOLAKIS: So if I have two

1 units, what you are saying is that I should be able
2 to survive a single failure in one and a single
3 failure in the other; is that what this says?

4 MR. AGGARWAL: Yes.

5 DR. APOSTOLAKIS: It says that in each
6 unit you should be able to handle a single failure.
7 So I an have one here and one there, and I would
8 still be okay?

9 MR. AGGARWAL: Right.

10 DR. APOSTOLAKIS: Well, why did you have
11 to do this? I mean, I don't understand why. Wasn't
12 that embedded in the previous definition?

13 MR. AGGARWAL: Well, there were concerns
14 over how we deal with the shared system, and the
15 IEEE made it clear that some guidance would be
16 provided in the failure.

17 DR. APOSTOLAKIS: Now the second bullet
18 really -- and in the first -- are redundant aren't
19 they?

20 MR. AGGARWAL: In a way.

21 DR. APOSTOLAKIS: So there is an
22 implementation of a single failure criterion on this
23 transparency.

24 MR. AGGARWAL: That's correct.

25 DR. APOSTOLAKIS: You don't understand

1 the first, but they give you the second?

2 MR. LOESER: There is a number of cases
3 where things were understood to be in the original
4 document. Everybody knew this is what was going on,
5 but it was not spelled out. So this standard tried
6 to spell out a number of the items, and this is one
7 of them.

8 Like you said, everybody understood
9 this, but it didn't say it very specifically. So
10 that is one of the items that we tried to take care
11 of.

12 DR. APOSTOLAKIS: Probably the second
13 bullet is more appropriate actually.

14 MR. AGGARWAL: And also you should know,
15 and I am sure that you are aware of, that in the
16 nuclear industry it is a very aging group, and newer
17 people are coming in, and they have no idea how the
18 systems work.

19 So this is an other training tool to
20 them to make it explicitly clear what the standards
21 were meant. Now I will turn my attention to the
22 analysis.

23 DR. APOSTOLAKIS: I think the first
24 bullet in fact is vulnerable to criticism because of
25 that word concurrently. I think the second bullet

NEAL R. GROSS

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

1 is more appropriately worthy. It says that if you
2 have a single failure in one unit, it should not
3 prorogate to the other, and that's fine.

4 But to say to consider two single
5 failures concurrently is against the philosophy of
6 single failure criteria isn't it?

7 DR. ROSEN: No, that is two different
8 units.

9 DR. APOSTOLAKIS: Yes.

10 MR. AGGARWAL: All right. We are going
11 to turn over to the analysis which is needed to be
12 done, and there are several stats, and that might
13 answer some of the questions which have been raised
14 recently.

15 The first criteria is that a safety
16 function for which the analysis is to be performed
17 shall be determined, and let me give you the
18 examples. Like reduced power, and isolate
19 containment, and cool the core.

20 The second criteria is that protective
21 action at the system level that are available for
22 safety functions shall be determined. Let me again
23 give you a few examples. For example, the rapid
24 (inaudible) and not the control rods, and building
25 of the containment isolation was safety injections,

NEAL R. GROSS

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

1 and poor spray.

2 These are the types of examples of that
3 protection. The next criteria is that safety group
4 that will sufficiently satisfy the required safety
5 functions shall be determined. Again, let me take a
6 few examples.

7 One example that comes to mind is that
8 either a two (inaudible) system, or one (inaudible)
9 spray and two LPSI, lower pressure coolant injection
10 subsystem, would we advocate to cool the core.

11 The next criteria is the independence of
12 the safety group that will be established shall be
13 verified. And again just to expand on that, this
14 independence should be verified.

15 And how would you verify that? By
16 observing that there are at least two safety groups
17 that have no shared equipment. For example, relays,
18 switch gear, buses, power sources, and even the
19 locations.

20 The next item here is for systems or
21 parts, where independence cannot be established, a
22 systematic investigation of potential failures shall
23 be conducted to assure that single failure criteria
24 is not valid.

25 Again, let me give you a few examples.

1 Failures include short-circuits, open voltage,
2 grounds, low AC and DC voltage, and these are all
3 examples that fall into this category.

4 DR. LEITCH: But it seems to me that it
5 depends greatly on how one defines the safety
6 function in your previous slide.

7 MR. AGGARWAL: That is correct.

8 DR. LEITCH: And, for example, to go
9 back again to this example, if the safety function
10 is to inject water at high pressure, the BWR would
11 fail if you define the function as to cool the core
12 and it passes.

13 MR. LOESER: In this particular case,
14 you are defining the function and then saying that
15 function fails. That is not really a -- you are
16 saying the function is to inject water at high
17 pressure, and then you are saying the system injects
18 water at high pressure and fails, this is -- you can
19 do that to any degree.

20 With any single component failure the
21 system that injects high water or high pressure at
22 water -- water at high pressure -- I am getting a
23 little tongue-tied -- will not fail.

24 That is, you can lose any particular
25 valve, and you can lose any particular pipe, and you

1 can lose any particular sensor that tells it to
2 inject the water, and it will still do that.

3 However, then if you want to failure the
4 entire system -- that is, HPSI, you have to now take
5 your function to the next higher level, and that is
6 to say to adequately cool the core.

7 You can't define your function and then
8 define the failure as that function at the same time
9 and have a valid analysis.

10 DR. LEITCH: Well, if you had redundant
11 HPSI systems, you could, right?

12 DR. LEITCH: Well, it would define the
13 function of injecting water, you would have two of
14 them, and you would say, okay, I define my failure
15 as not being able to inject water, regardless of how
16 many.

17 CHAIRMAN BONACA: That would restrict
18 really your designing ability. I mean, you can
19 either provide the function by having a redundant
20 high pressure planes, or you may have provided the
21 function of cooling a high pressure at the lowest
22 level still. So one train of high pressure and one
23 train of --

24 DR. APOSTOLAKIS: But Graham's point is
25 very well taken. It depends on what you call

NEAL R. GROSS

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

1 function.

2 MR. LOESER: Yes.

3 CHAIRMAN BONACA: Oh, yes.

4 MR. LOESER: And that defines the
5 function, because no matter what you are defining,
6 you could always say, okay, I lose that, and what is
7 next.

8 DR. APOSTOLAKIS: I have a question for
9 Dr. Powers. In your infamous memo, or taped report,
10 or whatever it was regarding the (inaudible) you had
11 in big boldface letters, this design phase, and the
12 defense in depth I think you said, or single failure
13 criteria of the agency, isn't this really what you
14 had in mind there?

15 You said if the primary way of removing
16 heat failed, there would have no alternate way of
17 doing it as I recall.

18 DR. POWERS: I think in fact I had them
19 failing on a couple of bases, and one of them is
20 that they lost their final heat sync and they had no
21 way to get to the heat sync.

22 DR. APOSTOLAKIS: All right.

23 DR. POWERS: And the second one is if
24 they SCRAMed the reactor, they had to use the safety
25 systems to shut it down, because just using the

1 control rods to cool it down, because the
2 temperature coefficient and reactivity it came back
3 alive, and so you had to put in the SCRAM rods in
4 order to shut it down.

5 So if your SCRAM rods failed, you can't
6 shut the reactor down. In other words, if you have
7 a single failure and your SCRAM is (inaudible), you
8 can't shut the reactor down and that is a violation
9 of the single failure criterion.

10 DR. APOSTOLAKIS: Well, it is a
11 violation of the system level, the fire level,
12 because you are assuming that you are losing the
13 whole SCRAM system, independently of whether you are
14 losing it due to a single failure or some other
15 failure, it is the function level that we are
16 talking about.

17 DR. POWERS: Well, clearly in my
18 memorandum, I was thinking of the function level,
19 but in fact that particular SCRAM system can be lost
20 by failure of a single digit component.

21 DR. APOSTOLAKIS: I see. So the heat
22 sync is what? You don't need an alternate heat
23 sync. There is one heat sync, but getting there --

24 DR. POWERS: You have to be able to get
25 there.

NEAL R. GROSS

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

1 CHAIRMAN BONACA: The point that I was
2 making before was that in the function of the
3 accident analysis, I don't think the regulation is
4 prescribed that you must have two trains of high
5 pressure, two trains of low pressure, and especially
6 for boilers.

7 The old boilers used to have many
8 isometric means of providing redundant functions.
9 So you could use high pressure injection and in
10 compliance with only one train.

11 But then you have other means through
12 the installation condenser, and to provide a
13 function of cooling during a LOCA, and what you have
14 to demonstrate is that either way we will take you
15 to shutdown, and there were different ways to get
16 there.

17 So I don't think in defining the
18 function of the regulation that it is prescriptive
19 of high pressure injection, and you have to have two
20 trains or whatever. That is one vital design, but
21 it was left free to perform the function, which is
22 the one of cooling, at high pressure, mid-pressure,
23 and low -pressure until you get to shutdown.

24 DR. LEITCH: But if we are starting with
25 a blank piece of paper to design an advanced reactor

NEAL R. GROSS

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

1 wouldn't that redundancy be required at the system
2 level?

3 I mean, what I am trying to say is that
4 say we design, and you are starting with a clean
5 piece of paper to design a BWR today, would these
6 regulations require that you have two HPSI systems?

7 MR. LOESER: I don't think so. I would
8 think that it would define the function and what the
9 licensing comes in, but once again we are probably
10 not prescriptive enough.

11 We would want to know that if you lost
12 that system that there would be no consequent to the
13 health of the public or the safety. That is, you
14 have some other way of cooling off the core before
15 there is any problem.

16 And if that way was to depressurize and
17 then use low, I would suspect that that would be
18 acceptable. However, I might point out that I am
19 out in the accident analysis branch, or the reactor
20 systems branch.

21 DR. LEITCH: I understand that.

22 MR. LOESER: So I may be making a bad
23 supposition.

24 CHAIRMAN BONACA: That is a good
25 question. There were old boilers at the Vermont

1 Yankee, for example, that had in fact -- they were
2 isometric in that sense, and had redundant systems.

3 But they had multiple systems, and
4 Vermont Yankee, for example, had only one high
5 pressure injection train. Then you have the
6 isolation condenser, and you have other means of
7 system safety failure, and so you have in an
8 isometric plant, but still it was not licensed. But
9 today I don't know if you would --

10 DR. ROSEN: I don't think there is
11 anything that would mitigate against it, and in fact
12 those older plants having different means of getting
13 the same function or more armor against a common
14 mode failure.

15 CHAIRMAN BONACA: They are very, very --
16 in fact, the core damage frequency for those plants
17 is very low.

18 DR. APOSTOLAKIS: Even if you have
19 redundant ways, that is where the mechanical systems
20 differ from electrical systems. And in a lot of
21 what the old plants, there is a single suction line
22 for both trains from the RWST, and so you have the
23 design basis event somewhere else, and it is a LOCA.

24 Now you have to cool the core, but that
25 single failure doesn't count as a single failure.

NEAL R. GROSS

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

1 CHAIRMAN BONACA: But you would not
2 design it today that way.

3 DR. APOSTOLAKIS: You would not.

4 CHAIRMAN BONACA: And typically the
5 (inaudible) because some of the earlier plants had
6 it that way.

7 DR. ROSEN: You would not do it not
8 because it is not strictly allowed by the
9 regulation. You would just do it because it is a
10 better practice.

11 CHAIRMAN BONACA: A good practice.

12 DR. APOSTOLAKIS: Yes.

13 MR. AGGARWAL: Let me conclude with
14 regard to the analysis and further observations.
15 Electrical, mechanical, and system logic failures
16 shall be considered in a single failure analysis.

17 A given component can have different
18 failure modes, and all analyses will be made for all
19 or each mode the failures. The location of safety
20 equipment shall be also analyzed to determine the
21 effect of common cause failures.

22 I am going to turn to the PRA now. The
23 IEEE or the industry has concluded that PRA analysis
24 is no substitute for a single failure analysis.

25 DR. ROSEN: Nor is a single failure

NEAL R. GROSS

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

1 analysis a substitute for a PRA.

2 MR. AGGARWAL: So conversely that is
3 very well said. However, I would like to add
4 something. A failure can be excluded for a single
5 failure analysis based on PRA operating experience.

6 DR. APOSTOLAKIS: In other words, I can
7 argue that -- well, first, I have a single failure
8 someplace, and I fail the criteria. But then I can
9 come back and say, look, based on this, and this,
10 and this, and that, and that, and that analysis, the
11 reliability of this particular piece of equipment is
12 so high that you should exclude it. I mean, the
13 failure cannot happen, and that is what you say.

14 MR. AGGARWAL: And that would apply
15 here.

16 DR. APOSTOLAKIS: Is that a new thing, a
17 new idea?

18 MR. LOESER: No, no. What about the
19 reactor vessel?

20 MR. LOESER: It is not a new idea, but
21 one that has been spelled out clearly.

22 MR. AGGARWAL: Clearly and explicitly.

23 MR. LOESER: It is one of those things
24 that we always knew this.

25 DR. ROSEN: We never took the failure of

1 a reactor vessel.

2 DR. APOSTOLAKIS: Well, it allows you to
3 have a common --

4 DR. ROSEN: We argued that the reactor
5 vessel is not going to fail.

6 DR. APOSTOLAKIS: Well, the reactor
7 vessel is a different beast, but the suction lines,
8 that is a basis on whether you allow it.

9 MR. AGGARWAL: Another example that
10 comes to my mind is that we essentially are
11 considering the passive failure, and you take a
12 motor controlled sample (inaudible), and you take it
13 granted that it will not fail, and that is based on
14 your analysis, judgement, PRA, or whatever it is.

15 And you don't have to conclude in your
16 analysis that let's fail the whole thing.

17 DR. APOSTOLAKIS: Wouldn't the more
18 accurate expression be passive component failure.
19 The failure itself cannot be passive.

20 MR. AGGARWAL: Okay. You are right.

21 DR. APOSTOLAKIS: It is like expert
22 elicitation.

23 MR. AGGARWAL: You're right.

24 DR. APOSTOLAKIS: It is an expert
25 opinion elicitation, right?

1 MR. AGGARWAL: The last significant
2 change involves the sensing lines, and now the
3 standard explicitly states that the lines connecting
4 sensors to the proper system shall be included, and
5 let me again give an example.

6 Equalizing walls, chambers, and
7 isolation walls. In conclusion --

8 DR. LEITCH: All the way back to the
9 penetrations to the vessel, right?

10 MR. AGGARWAL: What about it?

11 DR. LEITCH: I mean, you have to have
12 redundant penetrations to the vessel.

13 MR. AGGARWAL: Correct.

14 DR. LEITCH: And not just coming out of
15 the vessel and then (inaudible) redundant valves.

16 MR. LOESER: And this is another one of
17 those cases where everybody knew this was meant all
18 the while, but it was never spelled out. So it was
19 just spelled out.

20 MR. AGGARWAL: In conclusion, it is my
21 submission to the committee that IEEE standards in
22 question is a much improved standard over the number
23 of years, and the staff is working with the IEEE
24 hand-in-hand.

25 In the last reg guide with the many

1 exceptions to the IEEE standard, and looking over a
2 number of years, although those sections have been
3 incorporated or resolved, it is the opinion of the
4 staff that this standard, if it satisfies so that
5 the requirements are met, it will meet the
6 commission requirements on the part of single
7 failure.

8 And it is my submission to you that the
9 committee concur with our findings, and permit us to
10 publish this guide as a final guide. Thank you. I
11 would also like to thank Dave, who took the time to
12 come from Susquehanna River to join us today, and on
13 behalf of the NRC, I would like to thank him.

14 MR. CARUSO: Excuse me, Satish.

15 MR. AGGARWAL: Yes.

16 MR. CARUSO: I was wondering if you
17 could please -- in my review of the reg guide, I saw
18 that there is additional guidance with regard to
19 single failure analysis in the designs that used
20 digital computers.

21 And that this guidance is provided in
22 the common cause failure section and refers the
23 reader to the IEEE standard 7-4.3.2-1993.

24 MR. AGGARWAL: Right.

25 MR. CARUSO: And it discusses common

1 cause failures, but yet design deficiencies are
2 specifically exempted from the standard. Could you
3 please elaborate on why those were exempted from the
4 standard?

5 MR. AGGARWAL: I really don't understand
6 the question. Do you, Dave?

7 MR. ZAPRAZNY: Could you repeat that
8 again?

9 MR. CARUSO: When I looked at the
10 standard --

11 MR. AGGARWAL: This is the standard that
12 we are talking about now, 379, or 7-4.3.2?

13 MR. CARUSO: Well, 379, and it refers or
14 it says that additional guidance was added to
15 address single failure analysis in designs that used
16 digital computers, and that this guidance is
17 provided in the common cause failure section and
18 refers the reader to IEEE Standard 7-4.3.2-1993.

19 And it identifies some important common
20 cause failure mechanisms for digital computers, and
21 that it would be a software flaw, which can be
22 considered a design deficiency. Yet, design
23 deficiencies were specifically exempted from the
24 standard.

25 MR. AGGARWAL: Ralph, could you tell us

1 the section number also? Are we on 5.5?

2 MR. CARUSO: This was based on 1.53 in
3 the reg guide, I guess.

4 MR. AGGARWAL: Okay. And where are you
5 reading it from?

6 MR. CARUSO: This was --

7 DR. ROSEN: Excuse me. Cliff Douth, do
8 you remember the design deficiency section?

9 MR. DOUTH: I think --

10 MR. AGGARWAL: Cliff, could you please
11 move to the mike, please?

12 DR. ROSEN: Thank you.

13 MR. DOUTH: Are you talking about the
14 next to last paragraph on page 5?

15 MR. CARUSO: Yes.

16 MR. DOUTH: I think what he is asking is
17 on your single failure criteria, and you go to
18 common cause, common cause has some exceptions for
19 the single failure criteria, based on -- you know,
20 you have design issues which are exempted because
21 you are saying that surveillance, or quality control
22 programs, or whatever, will take care of that.

23 But in digital systems, it references
24 you back to 7.4.3.2, because that common cause there
25 is a design.

1 The standard itself exempts some common
2 cause based on I think one's design, and the
3 reasoning being that if you go back over and say you
4 are going to take credit for either surveillance or
5 quality control programs, but in software the design
6 flaw is common cause. I know the standard
7 references you back to 7.4.3.2.

8 MR. LOESER: Let me see if I understand
9 what you are saying. You are objecting because this
10 particular paragraph has on the third line, it says
11 things that are exempted are design deficiencies.

12 But in fact if you take into account
13 7.4.3.2, which talks about V&V, for example, on the
14 design and on the specifications and all of this,
15 where you ensure that there are no design
16 deficiencies, or at least to the probability of a
17 design deficiency, is sufficiently small that you
18 are not capable of finding it anymore, despite your
19 best efforts.

20 MR. DOUTT: Yes, I think the standard
21 actually draws you off, because common cause failure
22 in software is unique, and so it takes you to
23 7.4.3.2 to resolve that.

24 MR. AGGARWAL: Exactly, and that is the
25 subject matter of the IEEE Standard 7.4.3.2.

1 MR. DOUTT: Right.

2 MR. AGGARWAL: And as I submitted to the
3 committee before, that the latest (inaudible) IEEE
4 standard yesterday, and the staff plans to endorse
5 that, and we will be back to you, and provide
6 information on how single failure will apply to
7 digital computers.

8 MR. LOESER: In this particular case the
9 last paragraph of Section 5.5 happens to be on page
10 6, and it says guidance on using diversity to
11 address common cause failures in digital computer
12 systems as provided by IEEE Standard 7.4.3.2-1993.

13 And that in fact does address design
14 errors. So if you think about it, that last sentence
15 is sort of an exception to the fact that it talks
16 about design deficiencies being exempted from common
17 cause failure. Does that answer your question?

18 MR. CARUSO: Yes, and it seems like
19 there was -- and maybe I am missing something, but
20 it appears that it is going to be addressed --

21 MR. LOESER: Well, design deficiencies
22 are addressed in the existing version of 7.4.3.2.

23 MR. CARUSO: Yes, that's correct.

24 MR. LOESER: Design deficiencies are
25 addressed in the existing version of 7.4.3.2.

1 MR. CARUSO: Yes.

2 MR. LOESER: And the fact that there is
3 a new one coming out doesn't really change that.

4 MR. AGGARWAL: But he is talking about
5 the reg guide, and what we are saying is that the
6 reg guide will endorse the standard will be
7 forthcoming, yes.

8 MR. LOESER: But, Satish, that has
9 nothing to do with what we are talking about. The
10 fact that we are planning to endorse a new version
11 of 7.4.3.2 doesn't matter if the existing version
12 takes care of this version.

13 MR. CARUSO: I think the reference for
14 7.4.3.2 was intended to cover common cause software
15 failure in 7.4.3.2 right now, and the new standard
16 will just be whatever enhancements there are.

17 MR. AGGARWAL: That's right.

18 MR. LOESER: So what is the question?

19 MR. CARUSO: That the design
20 deficiencies are considered as a common cause
21 failure.

22 MR. LOESER: In digital software, yes.
23 That's why we review the design.

24 MR. CARUSO: Very good.

25 MR. AGGARWAL: This will conclude our

1 presentation.

2 DR. SHACK: Any further questions from
3 the committee? If not, thank you for a detailed
4 presentation, Satish.

5 MR. AGGARWAL: Thank you.

6 CHAIRMAN BONACA: I think we can go off
7 the record now. We do not have to record the
8 meeting anymore.

9 (Whereupon, at 9:31 a.m., the meeting
10 was concluded.)

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

CERTIFICATE

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

Name of Proceeding: Advisory Committee on
Reactor Safeguards
505th Meeting

Docket Number: n/a

Location: Rockville, MD

were held as herein appears, and that this is the
original transcript thereof for the file of the United
States Nuclear Regulatory Commission taken by me and,
thereafter reduced to typewriting by me or under the
direction of the court reporting company, and that the
transcript is a true and accurate record of the
foregoing proceedings.



Eric Hendrixson
Official Reporter
Neal R. Gross & Co., Inc.

Regulatory Guide 1.53 Rev 1 Single Failure Criterion

Presentation to
Advisory Committee on Reactor Safeguards
September 12, 2003



Satish Aggarwal
Office of Nuclear Regulatory Research
301-415-6005

Single Failure Criterion

- Draft RG DG-1118 was issued in 2002 for public comment.
- Received 4 comment letters.
- Made few minor changes in the implementation section:
 - Backfitting is not intended for current operating nuclear power plants

Single Failure Criterion

- Draft DG-1118:

Licensees of Operating Nuclear Power Plants will have the option to use for safety system modifications.

1. The June 1973 issue of RG 1.53 and be subjected by the staff on a case-by-case basis; or
2. This revision 1

Single Failure Criterion

- Final RG:

It will also be used to evaluate the submittals from the operating reactor licensees who voluntarily propose to initiate safety system (or protection system) modifications, if there is a clear nexus between the proposed modifications and this guidance for applying single failure criterion.

Single Failure Criterion

- What is a “Single Failure?”

The safety systems shall perform all required safety functions for a DBE in the presence of:

- Any single detectable failure within the safety systems.
- All failures caused by the single failure.
- All failures that cause or are caused by the DBE requiring the safety function.

Single Failure Criterion

- **Single Failure:**
 - The single failure could occur prior to, or at any time during, the DBE for which the safety system is required to function.

Single Failure Criterion

- Single-Failure analysis in designs using digital computers:

Reference to another IEEE Std was added (IEEE Std 7-4.3.2 – 1993).

Single Failure Criterion

- Shared Systems:

Single-Failure Criterion is:

- The safety systems of all units be capable of performing their required safety functions with a single failure assumed within the shared systems or within the auxiliary supporting features or other systems with which the shared systems interface.

Single Failure Criterion

- The safety systems of each unit shall be capable of performing their required safety functions, with a single failure initiated concurrently in each unit within the systems that are not shared.
- Provisions shall be included in the design to ensure that single failures within one unit will not adversely affect (propagate to) the other unit, thereby preventing the shared systems from performing the required safety functions.

Single Failure Criterion

Design Analysis for Single Failure

Procedure:

For each design basis event, the following steps shall apply:

- The safety function for which the analysis is to be performed shall be determined.
- The protective actions at the system level that are available to accomplish the safety function shall be determined.

Single Failure Criterion

- The safety groups that will sufficiently satisfy the required safety functions shall be determined.
- The independence of the safety groups that were established above shall be verified.
- For systems or parts where independence cannot be established, a systematic investigation of potential failures shall be conducted to assure that the single-failure criterion is not violated.

Single Failure Criterion

- Probabilistic Assessment
 - A probabilistic assessment shall not be used in lieu of the single failure analysis.
 - A failure can be excluded from the Single-Failure Analysis based on:
 - Reliability Analysis
 - Probability Assessment
 - Operational Experience
 - Engineering Judgement
 - Any Combination

Single Failure Criterion

- Sensing Lines

Lines connecting sensors to the process systems shall be included in the Single-Failure Analysis.