

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: Wednesday, September 7, 2011

Work Order No.: NRC-1107

Pages 1-184

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

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

OPEN SESSION

+ + + + +

WEDNESDAY

SEPTEMBER 7, 2011

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Chairman
DENNIS C. BLEY, Member
JOHN D. SIEBER, Member
JOHN W. STETKAR, Member

ACRS CONSULTANTS PRESENT:

MYRON HECHT

NRC STAFF PRESENT:

CHRISTINA ANTONESCU, Designated Federal Official
EUGENE EAGLE, NRO/DE/ICE2
IAN JUNG, NRO/DE/ICE2
JOHN LAI, ACRS Staff
RICHARD STATTEL, NRR/DE/EICB
RUSS SYDNOR, RES/DE/DICB

ALSO PRESENT:

BOB HIRMANPOUR, NuStart*
GEORGE STRAMBACK, Westinghouse*

*Participating via telephone

C-O-N-T-E-N-T-S

Call to Order and Opening Remarks Charlie Brown Chairman	4
Introductory Remarks Ian Jung Branch Chief Instrumentation Control Engineering Branch NRO	6
Review of SRP BTP 7-19, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based I&C Systems, Revision 6 Gene Eagle NRO/DE/ICE2 Richard Stattel NRR/DE/EICB	8
Review of Open Items	170

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

8:30 a.m.

CHAIRMAN BROWN: (presiding) The meeting will now come to order.

This is a meeting of the Digital I&C or Instrumentation and Controls Systems Subcommittee.

I am Charles Brown, Chairman of the Subcommittee.

ACRS members in attendance are Dennis Bley, Jack Sieber, John Stetkar. Myron Hecht, a consultant, is also attending as a consultant for the Subcommittee.

Christina Antonescu of the ACRS staff is the Designated Federal Official. She is not here right now, and she is being amply substituted for by Mr. Lai, who will make sure that I don't do anything out of order here relative to the rules and regulations.

During this meeting, the staff will discuss Revision 6 to Branch Technical Position BTP 7-19, "Guidance for the Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems". The NRC is in the process of issuing Rev. 6 to BTP 7-19, which is part of the Standard Review Plan, Chapter 7, that will

NEAL R. GROSS

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

(202) 234-4433

(202) 234-4433

1 incorporate the guidance from the Interim Staff
2 Guidance ISG-02, Revision 2, "Diversity and Defense-
3 in-Depth," which was issued in June of 2009.

4 The Subcommittee will gather information,
5 analyze relevant issues and facts, and formulate
6 proposed positions and actions as appropriate for
7 deliberation by the full Committee.

8 The rules for participation in today's
9 meeting have been announced as part of the notice of
10 this meeting previously published in The Federal
11 Register on August 23rd, 2011.

12 We have received no written comments or
13 requests for time to make oral statements from members
14 of the public regarding today's meeting.

15 Also, we have Bob Hirmanpour, NuStart, and
16 George Stramback, Westinghouse Electric Company, on
17 the bridge phone line listening to the discussions.

18 Is there anybody else on the phone line
19 right now? If you would, please identify yourself.

20 (No response.)

21 Okay. To avoid interruption of the
22 meeting, the phone line will be placed on a listen-in-
23 mode-only during the discussions, presentations, and
24 Committee discussions.

25 A transcript of the meeting is being kept

NEAL R. GROSS

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

1 and will be made available, as stated in The Federal
2 Register notice. Therefore, we request that
3 participants in this meeting use the microphones
4 located throughout the meeting room when addressing
5 the Subcommittee. The participants should identify
6 themselves and speak with sufficient clarity and
7 volume so that they may be readily heard.

8 We will now proceed with the meeting.
9 Okay, Ian is here.

10 Excuse me. Our Designated Federal
11 Representative, Christina Antonescu, has now arrived.
12 So, she will be taking charge of that aspect of the
13 meeting.

14 I will now call upon Mr. Ian Jung, Branch
15 Chief of the Instrumentation Control Engineering
16 Branch of NRO, to provide some introductory remarks.

17 MR. JUNG: Thanks, Charlie.

18 Good morning, members.

19 The purpose of today's presentation is to
20 get the Members' endorsement of the Revision 6. It is
21 about to be issued. This is the last step of the
22 revision to BTP 7-19.

23 And briefly, just Revision 6 versus
24 Revision 5. Revision 5 itself was a viable Staff
25 Guidance. In the 2006 timeframe, the industry came

NEAL R. GROSS

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

1 and asked for additional clarifications on seven
2 problem statements. And those problem statements were
3 addressed through Working Groups and significant
4 interactions with industry. Those problem statements,
5 the staff made in some cases very strong the guidance,
6 not just to go with the industry's position.

7 But, fundamentally, the agency policy laid
8 out in the SRM to the 93-087, those four-point
9 positions, we call it, have not been changed. It has
10 been elaborated with additional guidance.

11 So, the main purpose of the Revision 6
12 that we are about to issue is to incorporate those
13 issues that have come up through the ISG, through the
14 development process. So, that is the background.

15 With that, today we have two presenters,
16 Richard Stattel from the Office of Nuclear Reactor
17 Regulation and Eugene Eagle from the Office of New
18 Reactors. They were two of the key TWG2 members. And
19 Mike Waterman, who was the technical lead, could not
20 attend this due to his personal leave.

21 And alongside with me is Russ Sydnor, who
22 is the Branch Chief of the INC in the Office of
23 Regulatory Research. We will be on the sidelines to
24 support any issues that may come up.

25 And with that, I will turn it over to Gene

NEAL R. GROSS

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

1 Eagle.

2 MR. EAGLE: Slide 3 today presents our
3 agenda. We have 10 items listed here. However, most
4 of our concentration will be on the stakeholder
5 concerns that came out of ISG-02, the seven problem
6 statements, with some other items.

7 First, we would like to review the general
8 basis and purpose of BTP 7-19, Revision 6. BTP 7-19
9 applies to software common cause failure, and will
10 simply be referred to as common cause failure or CCF
11 in this presentation.

12 Despite the use of quality software,
13 development techniques, and extensive testing, digital
14 systems generally cannot be proven to be error-free.
15 Software-based digital systems are considered
16 susceptible to the same error appearing in identical
17 copies of the software-based logic and architecture
18 that are present in redundant divisions of the safety-
19 related systems. Therefore, software-based or
20 software-logic-based digital system development errors
21 are a credible source for common cause failure. In
22 BTP 7-19, software includes firmware and logic
23 developed from software-based development systems.

24 In summary, while the NRC staff considers
25 software common cause failure in digital systems to be

NEAL R. GROSS

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

1 beyond-design-basis, nuclear power plants should be
2 protected against the effects of anticipated
3 operational occurrences and postulated accidents with
4 a concurrent common cause failure in the digital
5 protection system.

6 CHAIRMAN BROWN: Before you leave that
7 slide, since I am new to that particular point --

8 MR. EAGLE: Yes.

9 CHAIRMAN BROWN: -- when did this become,
10 in other words, CCF not being beyond-design-basis?
11 When did that actually get stated or determined to be
12 a policy?

13 MR. JUNG: Yes, Charlie, that was
14 discussed during the 93-097 (sic) SECY paper to the
15 Commission.

16 CHAIRMAN BROWN: 087?

17 MR. JUNG: Right.

18 CHAIRMAN BROWN: Yes, I read that. And
19 that's the specific point? I noticed that it didn't
20 state it exactly in that form, if I remember
21 correctly. I have to go back and read it again. But
22 that is the initial point, and that has been carried
23 forward?

24 MR. JUNG: Yes, that has been the initial
25 point. Because of that interpretation, the Commission

NEAL R. GROSS

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

1 specifically struck out originally the diverse backup
2 system to be safety-related systems. The Commission
3 specifically struck it out and said you can use non-
4 safety-related with realistic assumptions. So, that
5 is the corresponding part --

6 CHAIRMAN BROWN: Okay. So, that was the
7 part where they approved part of the staff
8 recommendations --

9 MR. JUNG: Right.

10 CHAIRMAN BROWN: -- initially in the SECY
11 paper, and then they did not elucidate what they
12 didn't approve in the SRM, if I remember correctly.
13 So, I was trying to figure out which was which in
14 there. Okay.

15 MR. EAGLE: Right.

16 MR. JUNG: Technically speaking, the
17 reasoning behind this, even in the GDC, the
18 introduction section of the GDC, it talks about
19 certain failures related to design errors. Those are
20 considered to be beyond-the-design requirements.
21 Those are typically handled by quality and reliability
22 elements.

23 And then, industry standards sort of
24 refers to generally the design errors are something
25 that is built into the quality, not as a fundamental

NEAL R. GROSS

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

1 design basis.

2 So, those are some general alignments on
3 that argument.

4 CHAIRMAN BROWN: Okay. All right, go
5 ahead.

6 Thank you.

7 MR. EAGLE: Slide 6 outlines the purpose
8 of BTP 7-19 as presented in Revision 6.

9 I might only just point out one specific
10 item here. The third bullet, ensure conformance with
11 NRC position on D3, is one of the key areas. Almost
12 everything revolves around that.

13 As far as the background to BTP 7-19, in
14 March 2007, BTP 7-19 Revision 5, the previous --

15 CHAIRMAN BROWN: Before you go on, if I
16 can backtrack? You don't have to go back on the
17 slide.

18 The issue of diversity --

19 MR. EAGLE: Yes.

20 CHAIRMAN BROWN: Did that first start,
21 come into play -- again, I am trying to get a little
22 history lesson here -- relative to the digital I&C
23 systems as opposed to diversity as being a part of the
24 original analog designs? I know in my program I
25 didn't deal with diversity relative to the analog

NEAL R. GROSS

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

1 designs. That's just the way it was.

2 MR. STATTEL: I mean I wasn't at the NRC
3 at that time, but there was a lot of --

4 CHAIRMAN BROWN: Pardon?

5 MR. STATTEL: I was not at the NRC at that
6 time.

7 CHAIRMAN BROWN: Oh, okay.

8 MR. STATTEL: However, there were several
9 digital systems that were being installed in various
10 plants. For instance, the Eagle21 system was being
11 put in at, I believe, Diablo Canyon and a couple --

12 CHAIRMAN BROWN: It was in the eighties,
13 wasn't it, or something, late eighties?

14 MR. STATTEL: Yes. Yes, it was kind of
15 early on. And the staff, during those reviews, the
16 early reviews, was concerned about the potential,
17 because it was very obvious in those designs that they
18 were duplicating the code from one division to
19 another. And the concern was that those errors would
20 be also duplicated, and they created a commonality, a
21 common point of failure, for those systems that did
22 not exist in the analog system. It was not as much of
23 a concern in the analog systems that they were
24 replacing.

25 CHAIRMAN BROWN: Okay. I am just trying

NEAL R. GROSS

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

1 to get --

2 MEMBER STETKAR: As someone who was
3 around, not at NRC, back in the gory days, there were
4 notions of diversity for analog, but they were done on
5 an ad hoc kind of reactionary basis. For example,
6 ATWS --

7 CHAIRMAN BROWN: Yes, okay.

8 MEMBER STETKAR: -- there were redundant
9 sensors. There were redundant trip signals. There
10 were redundant actuation devices for failure to scram
11 in response to events that happened. But there wasn't
12 a comprehensive program for installing diversity of
13 protection or actuation signals in the analog world.

14 When events happened, somebody dreamed up
15 a diverse way, and people installed it.

16 CHAIRMAN BROWN: Yes.

17 MR. EAGLE: Charlie, he is talking about
18 redundancy versus diversity. When you had a lot of
19 the individual items like the silos for the analog
20 systems, there you had redundancy. But when you
21 started getting the same kind of software being
22 duplicated, then you started being more concerned
23 about diversity.

24 CHAIRMAN BROWN: No, I understand that
25 problem exactly.

NEAL R. GROSS

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

1 MR. EAGLE: Okay. Yes.

2 CHAIRMAN BROWN: That part I got. I just
3 was trying to get to see how far back, since I wasn't
4 part of the NRC programs, how far back into the analog
5 world the thought process --

6 MR. STATTEL: There were a lot of parallel
7 concerns in the analog world because, obviously, the
8 schematics and the designs were also being duplicated
9 across divisions. However, it is kind of a timing
10 issue because it was evident with these digital
11 systems that the point that these design errors would
12 present themselves would be identical in all four
13 channels. Whereas, if you have an analog component,
14 a transistor or a resistor, the likelihood or the
15 credibility of a simultaneous failure in multiple
16 channels was very low.

17 MEMBER STETKAR: Nobody ever saw any
18 common cause relay failures, I guess.

19 (Laughter.)

20 MR. STATTEL: Well, right.

21 CHAIRMAN BROWN: Oh, no, I'm very familiar
22 with some common cause relay failures.

23 MEMBER STETKAR: Like the whole plant?

24 CHAIRMAN BROWN: Like the whole system.

25 (Laughter.)

NEAL R. GROSS

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

1 MR. JUNG: Allow me just to -- I agree
2 with John regarding the ad hoc nature of how the
3 agency dealt with the common cause failure of software
4 prior to the ABWR Design Certification. There was a
5 first new reactor application for design certification
6 that came. That really times-up really well with the
7 93-087 SECY paper.

8 So, the SECY paper that went on to the
9 Commission is a combination of the experience and
10 increased use of digital technology and concerns
11 especially with the complexity that has come along
12 that really resulted in ABWR, at the same time
13 development of the 93-087, which eventually led to an
14 issuance of BTP 7-19 in 1997.

15 CHAIRMAN BROWN: Okay. Thank you.

16 MR. EAGLE: As far as the background for
17 BTP 7-19, in March 2007, Revision 5 was issued in
18 anticipation of the new reactor applications.
19 However, in November of 2006, industry representatives
20 in a public meeting claimed to the Commission that
21 there was still confusion or insufficient guidance in
22 digital I&C areas and the need existed for additional
23 guidance for licensing certainty.

24 In early 2007, a Steering Committee was
25 formed and a Project Plan was developed. Seven Task

NEAL R. GROSS

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

1 Working Groups were formed.

2 Task Working Group No. 2 that we
3 participated in was formed concerning D3, that is,
4 defense-in-depth and diversity. And it was formed
5 with members from NRR, Research, and the Office of New
6 Reactors.

7 There was significant stakeholder
8 involvement throughout the process with public
9 meetings and review of different versions of the
10 document as it was developed. And also, White Papers
11 came in from industry providing input on the
12 development of this document.

13 The initial issue of Interim Staff
14 Guidance for D3 was in September of 2007. Now the
15 Interim Staff Guidance was the technique or method
16 that was used to quickly get out information in
17 dealing with such areas as the digital I&C and other
18 areas. This issue was Revision 1, and it addressed
19 the seven problem statements that had been submitted
20 by industry.

21 The ACRS at that time reviewed the draft
22 of Revision 1 and provided three observations.

23 First, they observed that it would be very
24 helpful for licensing and licensing review.

25 The staff should determine the conditions

1 under which an operator manual action can be credited
2 as a diverse protective function.

3 And third, the issue of spurious actuation
4 needed to be examined further.

5 MR. STATTEL: I'll just add, since that
6 time, the staff at NRR has used ISG-02 extensively
7 during our reviews of the Oconee digital upgrade as
8 well as the Wolf Creek upgrade.

9 MR. EAGLE: Revision 2, which is still
10 currently active, was issued in June 2009, and this
11 edition had many clarifications and editorial changes,
12 but its basic thing was to answer the seven questions
13 and, also, to deal with the ACRS Letter of
14 Recommendations.

15 They clarified the option for manual
16 operator action as a diverse protective action. Now
17 this was based on being able to justify this with the
18 human factors analysis methods found in ISG-05.

19 BTP 7-19 Revision 6 came about by
20 incorporating the ISG-02 Revision 2 items,
21 particularly the seven questions.

22 Go back just one moment.

23 Originally, there was a 30-minute hard
24 limit that manual operator action could only be used
25 if not required for at least 30 minutes. This was in

NEAL R. GROSS

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

1 line with the guidance or regulations from other
2 countries that were major generators of electrical
3 power for nuclear power plants, as learned in a major
4 international meeting in this very room.

5 CHAIRMAN BROWN: Did you mean to phrase
6 that the way you --

7 MR. EAGLE: What?

8 CHAIRMAN BROWN: Say that 30-minute thing
9 again.

10 MR. EAGLE: Originally, there was a 30-
11 minute, I call it hard limit.

12 CHAIRMAN BROWN: Yes, I understand the 30-
13 minute, but it was the way you phrased it.

14 MR. EAGLE: Okay.

15 CHAIRMAN BROWN: And I just wasn't quite
16 sure --

17 MR. EAGLE: Sometimes it is phrased saying
18 that anything less than 30 minutes has to be
19 automated.

20 CHAIRMAN BROWN: You had to have at least
21 30 minutes in order to credit operator action.

22 MR. EAGLE: Yes, right.

23 CHAIRMAN BROWN: Okay. Okay. I didn't
24 get that out of the way you phrased it.

25 MR. EAGLE: Yes, it can only be used, the

NEAL R. GROSS

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

1 manual operator action could only be used if not
2 required for at least 30 minutes.

3 CHAIRMAN BROWN: Okay.

4 MR. STATTEL: Now there are many plants
5 out there that do rely on manual actions that are less
6 than 30 minutes, but they have to provide
7 justification for that.

8 MEMBER STETKAR: You are going to discuss
9 this a little bit more?

10 MR. STATTEL: We'll cover that, yes.

11 MR. EAGLE: Right. That is going to be a
12 major area that we will discuss.

13 MEMBER STETKAR: Because this whole issue
14 needs a little more clarification on its background.

15 MR. STATTEL: Okay. We understand that.

16 MR. JUNG: Just clarification, I mean,
17 even though it is a very hard limit, at the time the
18 industry wanted what is a go and no-go on that aspect,
19 but we are still dealing in a guidance space, right?
20 So, any deviation from that, the applicant has to
21 demonstrate why the alternative was justified.

22 So, we are still in the guidelines. When
23 we say "hard limit", that didn't mean we have any
24 legal basis to say, no, you don't meet the guidance.
25 If they don't meet the regulation or policy, we have

NEAL R. GROSS

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

1 a strong basis.

2 So, I just want to highlight that we are
3 still in the guidance space.

4 MR. STATTEL: Well, right, and that was
5 one of the points, major points, of discussion at the
6 Working Group because the industry correctly pointed
7 out that there are many manual actions that are
8 already credited in accident analysis that are less
9 than 30 minutes. And therefore, having a perceived
10 limit --

11 CHAIRMAN BROWN: That require action in
12 less than 30 minutes in order to be effective.

13 MR. STATTEL: Exactly. Exactly. So, in
14 lieu of setting a time, a particular timeframe, it was
15 proposed an HFE process, evaluation process -- and we
16 will get into it in the later slides -- where we would
17 make a determination for what time is needed to
18 perform that action and, also, assess the operator's
19 ability to perform that action within that amount of
20 time within reasonable assurance.

21 MR. EAGLE: By the way, we are still in
22 the background. This is just setting it up. There
23 will be more details about it.

24 Again, remember, when we were talking
25 about the operator action, we are talking about

NEAL R. GROSS

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

1 operator action as a diverse means.

2 Industry represented strong dissent to not
3 having an option to use manual operator action as a
4 diverse means for actions required in less than 30
5 minutes. And the ACRS at the time agreed that it
6 should be considered.

7 DR. HECHT: Didn't EPRI issue a report in
8 that regard?

9 MR. EAGLE: They did put in a White Paper.
10 During this whole period, the industry, in general,
11 wanted to see an option for less than 30 minutes. So,
12 the result was, of course, ISG-02, Rev. 2.

13 DR. HECHT: Yes. I recall that they were
14 making the case that using a risk-based analysis, they
15 argued that it was actually more risky in some cases
16 to require automated actions.

17 MR. EAGLE: Yes, and we addressed that,
18 some of the issues involved. Okay?

19 MR. JUNG: Just to Myron, the industry
20 provided several White Papers on the whole subject of
21 diversity and defense-in-depth. One of them is a risk
22 argument that ISG-03 specifically addressed on how to
23 use risk argument for digital systems, which generally
24 the staff indicated there are limitations using risk-
25 based argument for not providing diverse means because

NEAL R. GROSS

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

1 of various concerns, including the quality of PRA.
2 Digital system PRA is still going through a lot of
3 research, all this research.

4 And one of the other elements was operator
5 action. Another White Paper was about defensive
6 design attributes, sort of preventive measures within
7 the safety system that could provide, you know, so
8 that they don't have diversity because we have this
9 set of design attributes.

10 So, I am just saying these things because
11 there are a lot of the industry White Papers that came
12 out. We had a lot of interactions. One of them was
13 they strongly pushed for the use of operator action as
14 a diverse means.

15 One of the arguments they made was, if we
16 put in a complex diverse backup system, that diverse
17 backup system can also, you could use purist actuation
18 of the plant. It is that particular increase in
19 potential risk would be actually potentially more than
20 the safety benefit of that system, then, as a diverse
21 means.

22 Generally, the staff did not buy that
23 argument because a diverse system should be developed
24 in a quality manner that does not have any significant
25 concern over --

NEAL R. GROSS

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

1 DR. HECHT: Okay. Thank you.

2 MR. JUNG: You will see, actually, a slide
3 on that topic.

4 MR. EAGLE: There's another thing about
5 risk. You know, you can have very low risk, but if
6 you have high consequences, you have to be very
7 careful. And we saw that in the oil spill. There has
8 never been an oil spill problem like that in 60 years,
9 and yet, we saw it. We saw the tremendous effects of
10 something that was supposed to be a low-risk thing in
11 that oil spill in the Gulf recently.

12 Okay. As a result of several public
13 comments on the phrasing of four points, the staff
14 decided to quote the NRC Four-Point Policy on D3
15 directly, as seen in slides 11 and 12. And that is
16 that the key of points 1 and 2 is the fact that there
17 will be an assessment and an analysis of a digital I&C
18 system. And if the analysis determines that there is
19 a potential for common cause failure, then point 3
20 points out that we need to have a diverse means to
21 take care of it.

22 The mention of the safety computer in
23 these points clearly indicates that the focus on
24 postulated common cause failure is the effect on the
25 automated protection system. And we talked a few

NEAL R. GROSS

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

1 minutes ago about things, that there were manual
2 actions that were taken in less than 30 minutes. For
3 instance, in those types of actions, if you are
4 already doing something manually, it is expected that
5 it would still possibly be manual, even in the light
6 of a common cause failure.

7 What we are talking about is we are
8 looking at mainly here, the main purpose here is the
9 automated protection system undergoing a common cause
10 failure. However, the staff interprets that, if the
11 manual initiation methods of the reactor protection
12 system are subject to postulated common cause failure,
13 then point 3 also directs that a diverse manual system
14 is needed.

15 CHAIRMAN BROWN: Question?

16 MR. EAGLE: Yes.

17 CHAIRMAN BROWN: Well, actually, a point
18 of understanding again.

19 MR. EAGLE: Yes.

20 CHAIRMAN BROWN: We have automated
21 protection systems.

22 MR. EAGLE: Right.

23 CHAIRMAN BROWN: Based on past meetings
24 and past reviews, all of those automated systems have
25 a built-in ability to initiate those manually.

NEAL R. GROSS

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

1 MR. EAGLE: Yes.

2 CHAIRMAN BROWN: Forget common cause
3 failure, forget this, forget whatever it is. I mean,
4 you can go hit a switch, and it may process through
5 all of the computer systems.

6 MR. EAGLE: Right.

7 CHAIRMAN BROWN: And that's allowed.

8 MR. EAGLE: That's allowed.

9 CHAIRMAN BROWN: But, then, diverse
10 means -- so, I am trying to separate the points here.
11 Manual has a lot of different connotations.

12 MR. EAGLE: Right.

13 CHAIRMAN BROWN: There's manual operation
14 where you just go right through the normal channels.

15 MR. EAGLE: Right.

16 CHAIRMAN BROWN: There is manual operation
17 which bypasses all of those and goes directly to
18 components or, excuse me, downstream of the computer-
19 based systems, which is not necessarily diverse yet.
20 But, then, there is your diverse system that gets
21 talked about also.

22 MR. EAGLE: Yes, we are going to be
23 getting into that, Charlie.

24 CHAIRMAN BROWN: Okay. All right.

25 MR. STATTEL: Very simply, there are two

NEAL R. GROSS

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

1 distinct requirements regarding manual operations.

2 MR. EAGLE: Yes, we are going to be
3 getting to that. Do you want to wait until we get to
4 that point?

5 CHAIRMAN BROWN: That's okay.

6 MR. STATTEL: I just want to make a point
7 here.

8 CHAIRMAN BROWN: Okay.

9 MR. STATTEL: There are two distinct
10 requirements. Now, within the guidance, we don't
11 really direct how those points, those requirements are
12 met. However, we do look at them. Basically, we are
13 looking at them from two different angles, right?

14 Now whether the manual operator action
15 requirement is met with a single system or with a
16 separate system, that is really design-specific, and
17 we will talk about some of the specific designs that
18 we have seen.

19 In some cases, it works. In other cases,
20 they really require a separate system.

21 CHAIRMAN BROWN: Does 603 have a specific
22 manual operation? I thought it had a separate manual
23 operation.

24 MR. STATTEL: It does.

25 CHAIRMAN BROWN: But that doesn't dictate

NEAL R. GROSS

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

1 how --

2 MR. STATTEL: It is more in line with, it
3 basically requires that the operator have a means of
4 manually initiating. And that means it has to be at
5 a system- or division-level, right?

6 CHAIRMAN BROWN: Yes.

7 MR. STATTEL: So, we are not expecting the
8 operator to go around to individual pumps and valves
9 in order to initiate a safety --

10 CHAIRMAN BROWN: Or trip the breakers --

11 MR. STATTEL: Right.

12 CHAIRMAN BROWN: -- to the control rod
13 drive mechanism?

14 MR. STATTEL: The real spin on the 603
15 requirement is that he has a very simple, concise
16 action that he can take to initiate that safety
17 function.

18 CHAIRMAN BROWN: And that is what I was
19 talking about relative to --

20 MR. STATTEL: That is one requirement,
21 right.

22 CHAIRMAN BROWN: Yes, and that is a 603,
23 that's a rule?

24 MR. STATTEL: Yes, it is.

25 CHAIRMAN BROWN: Okay. I'm trying to

NEAL R. GROSS

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

1 break this in my brain into stuff that is required by
2 rule and those now that get flipped over into the
3 guidance part of this.

4 MR. STATTEL: Right.

5 CHAIRMAN BROWN: Because it kind of gets
6 mushed-up in the discussion. I am not complaining,
7 okay? It is just a lack of understanding on my part.
8 Just to make sure I understand it.

9 MR. STATTEL: What we have seen in the
10 designs, there are some designs that can meet the
11 requirements of that rule base -- you're correct, it
12 is ruled by reference to 603 -- but do not meet the
13 guidance that we are proposing for diversity, for
14 diverse actions.

15 CHAIRMAN BROWN: Yes, I understand. Okay.

16 MR. STATTEL: So, it is two different --

17 CHAIRMAN BROWN: Okay.

18 MR. EAGLE: And we'll be coming to that.

19 CHAIRMAN BROWN: All right. I'll let you
20 go on.

21 MR. EAGLE: Okay.

22 CHAIRMAN BROWN: I just wanted to make
23 sure I got that thought on, so that it gets addressed.

24 MR. EAGLE: Okay. As I said, the staff
25 decided that they would quote because there were

NEAL R. GROSS

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

1 different comments involving the way the BTP Rev. 5
2 had handled presenting the four points. They decided
3 to quote those four points exactly and then provide
4 certain interpretations or comments concerning it.

5 For instance, the idea or the term "best
6 estimates" used in the four points, we felt that the
7 term "realistic assumptions" was a better way of
8 describing it. And this was defined as normal plant
9 conditions corresponding to the event. As you can
10 see, it was various types of components there or
11 parameters.

12 DR. HECHT: Can I just ask a question?

13 MR. EAGLE: Yes.

14 DR. HECHT: The use of realistic
15 assumptions, and I guess the original SECY language
16 was "best estimate methods". It wasn't clear to me
17 what chain of logic led "best estimate methods" into
18 "realistic assumptions".

19 MR. EAGLE: Do you want to answer that?

20 MR. STATTEL: Well, the alternative, for
21 instance, when you are dealing with a safety analysis
22 or within-design-basis accidents, it would be to
23 assume worst-case scenarios, right? So, the action is
24 initiated from the worst-case power level which would
25 challenge the integrity of the plant, right? Worst-

NEAL R. GROSS

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

1 case temperatures, worst-case pressures, worst-case
2 flows, right?

3 So, what this does, it recognizes the fact
4 that this is not within design basis. So, we are
5 talking about a common cause failure that defeats the
6 safety functions coincident with one of the design-
7 basis accidents or some AOO events, right?

8 So, basically, this is a little less
9 stringent, less restrictive in that we assume the
10 initiating point. When the licensee performs these
11 analyses, they are assuming just normal operating
12 power levels, temperatures, you know, the parameters,
13 right?

14 DR. HECHT: Well, I understand that, but
15 best estimates methods, to my mind, when I first read
16 that, said, well, use a complex computer code rather
17 than a simple approximation. That was my first
18 meaning of it.

19 MR. JUNG: Myron, let me take a crack at
20 it.

21 DR. HECHT: Yes.

22 MR. JUNG: The reason that the industry,
23 and even among the staff members, the expression "best
24 estimate" is not well-defined.

25 DR. HECHT: Okay.

1 MR. JUNG: That was the genesis of that.

2 DR. HECHT: Right.

3 MR. JUNG: The realistic assumption is
4 based on actually Chapter 15. Actually, Chapter 15,
5 there has been the methods that -- there are two. One
6 of the codes they are running, actually, they dealt
7 with the realistic assumptions for some of the code.

8 So, I mean, I don't think the staff is
9 looking for best estimate as a sort of simplistic
10 analysis. What we are looking for is still very
11 complex analysis, that they still have to run the
12 codes and Chapter 15 analysis codes, but the
13 assumptions built into Chapter 15, design-basis
14 assumptions have built in a lot of the additional
15 margins, sometimes very conservative.

16 And "realistic assumptions" is a known
17 term that Chapter 15 understands it. Recent
18 experience with the USAPWR design, actually, they
19 provided the code runs using realistic assumptions.
20 And Chapter 15 folks looked at it. We are still going
21 through the reviews. But the intention was to reduce
22 -- because of the beyond design basis, they don't have
23 to have beyond reasonable extra margin to the
24 assumptions, according to the codes.

25 So, that is the one option. If somebody

NEAL R. GROSS

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

1 chooses to use Chapter 15 as it is, as a conservative
2 case, we would have been just fine as well.

3 DR. HECHT: Thank you.

4 MR. JUNG: So, the bottom line is that the
5 language itself "best estimate" could mean to somebody
6 some different meaning. So, we wanted to be more
7 aligned with the Chapter 15 aspects, that we are more
8 aligned with what has been known before. So, this
9 topic, we work with the Chapter 15 folks.

10 MEMBER STETKAR: Richard or Eugene, either
11 one, or anybody, as I read through this, and I read
12 through the stakeholder comments and the resolution of
13 the comments, there was some discussion about point 2,
14 about clarification of realistic assumptions, best
15 estimate methods. As I read the discourse, it was
16 all, I think, in the context of events that occurred
17 during plant power operation.

18 The question I have is, how does the staff
19 review the design of a digital protection system for
20 events that can occur during shutdown? Because a lot
21 of these protection systems now there are tech specs
22 that require protection against loss of inventory,
23 against boron dilution, against other reactivity
24 excursions, against cold over-pressure transients and
25 pressurized water reactors.

NEAL R. GROSS

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

1 So, there is a litany of events that can
2 occur during shutdown modes, zero power, mode 5, that
3 could introduce the potential for common cause
4 failures in the protection system, because different
5 parts of the logic are challenged. There are
6 different input sensors. There are different
7 algorithms that look at the conditions to initiate
8 those protective functions.

9 How does this guidance provide staff
10 review for those conditions? Because a lot of those
11 accidents are not necessarily treated in the standard
12 Chapter 15 at-power, stylized, design-basis accident
13 analysis.

14 MR. STATTEL: I don't know that this
15 guidance really directs which accidents would be
16 analyzed.

17 MEMBER STETKAR: Well, except it says,
18 there are references to power operation accidents in
19 Chapter 15 of the FSAR, for example, which is pretty
20 clear guidance to me.

21 MR. STATTEL: Okay.

22 MEMBER STETKAR: If I were a reviewer and
23 if I were an applicant, I would say, well, we don't
24 have to address those things because the guidance
25 points me strictly to power operation and strictly to

NEAL R. GROSS

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

1 the Chapter 15 accident analysis.

2 MR. EAGLE: Okay. Notice that, in fact,
3 this was done partly in answer to that public comment,
4 where they said they were concerned about the way we
5 had expressed it, that it was aiming only at power
6 operation. So, notice the phrasing was placed in here
7 "corresponding to the event". In other words, the
8 normal plant conditions corresponding to the event,
9 power levels, anything else.

10 So, that could be at a much lower power.
11 In fact, you may have a different, more difficult
12 situation maybe at a lower power for a certain type of
13 event.

14 MEMBER STETKAR: I'm talking about zero
15 power.

16 MR. EAGLE: Okay. It doesn't matter. We
17 said corresponding to the event.

18 MEMBER STETKAR: Is that the
19 interpretation? Is that the staff's interpretation?

20 MR. EAGLE: That was the interpretation,
21 that we put it in --

22 MEMBER STETKAR: Okay. That doesn't come
23 across very clearly. The reason I asked the question
24 is I got a bit of a nuance of that in some of the
25 discussion of the public comments.

NEAL R. GROSS

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

1 MR. EAGLE: Right. That was we reason we
2 put it in that way.

3 MEMBER STETKAR: But in the guidance, it
4 really is not all that clear that the intent is to
5 also look at non-power events.

6 CHAIRMAN BROWN: A point to that, when you
7 talk about corresponding to the event, it would be
8 like, instead of the event, corresponding to the plant
9 conditions at which the plant is or is existing.

10 MR. EAGLE: Right.

11 MR. STATTEL: Oftentimes, the analyses are
12 performed kind of with a different view because a
13 particular system or a particular part of a system is
14 what is being upgraded.

15 So, the way I have seen these analyses
16 come in for staff review is, basically, they present
17 us with tables. These are the AOOs, and these are the
18 events for which this portion of the system, its
19 safety function is being credited. Right?

20 MEMBER STETKAR: I understand that. It
21 says "NRR" on your thing.

22 MR. STATTEL: Yes.

23 MEMBER STETKAR: I look over to NRO
24 because I see integrated systems coming in --

25 MR. STATTEL: Right.

NEAL R. GROSS

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

1 MEMBER STETKAR: -- for review, and they
2 have integrated functions that look at inventory
3 control. They look at pressure. They look at
4 temperature.

5 And those systems know whether you are at
6 power. They know power levels. They know whether you
7 are shut down. They invoke certain algorithms when
8 you are shut down. They invoke different algorithms
9 when you are at power.

10 And simply, when those systems are
11 presented to NRO for review, they say, "Here, verily,
12 is my digital protection system. Please review it and
13 give us a design certification." They don't
14 differentiate about a list of tables with specific
15 functions.

16 MR. STATTEL: I guess we are not dealing
17 with the integrated aspects when we are looking at the
18 upgrades.

19 MEMBER STETKAR: Yes. Well, but there may
20 be elements of some of those. Have you asked anybody
21 whether while they are upgrading the system maybe they
22 put some things in there also to protect against
23 shutdown events?

24 MR. STATTEL: Normally, they are not
25 looking for changing or modifying the safety

NEAL R. GROSS

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

1 functionality of the system. It usually is the one-
2 for-one replacement.

3 So, it is very evident to us that all of
4 the accidents and AOOs for which the safety functions
5 are being credited are included in that list. It is
6 fairly evident.

7 MEMBER STETKAR: Okay.

8 MR. STATTEL: We have never had any
9 questions over omissions from the list.

10 MEMBER STETKAR: No, I'm not talking about
11 omissions. I am talking about extra things that they
12 put in there to protect against things at shutdown,
13 events at shutdown.

14 MR. STATTEL: Right.

15 MEMBER STETKAR: And nobody has really
16 taken a look at those to see where you are vulnerable
17 to common cause failures that might require a
18 different form of diversity. That is the only
19 question.

20 MR. EAGLE: Keep in mind that the policy,
21 you know, in item 2 it deals with the Safety Analysis
22 Report, you know, the events involved in the Safety
23 Analysis Report. That is your guidance, your key
24 guidance there in general.

25 MR. JUNG: John, I think this is an area

NEAL R. GROSS

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

1 I am not sure staff has gone into a lot of details
2 because we are focusing on generally -- usually, most
3 of the new plants coming in, they are asking for a
4 two-year cycle, fuel cycles, and certain shutdown
5 conditions, duration of that. If you translate that
6 into a PRA initiating event for that particular
7 scenario, and all that, I am not saying it is not
8 addressed by the applicant. I am saying I am not sure
9 we have gone into that much detail on that very
10 specific mid-look operation type of things to say are
11 there any common cause failure aspects that need to be
12 addressed.

13 MEMBER STETKAR: Well, Ian, I have been
14 really careful not to use the letters "PRA" or the
15 term "risk-informed" in any of this. I am trying to
16 stick strictly to a design-basis evaluation of
17 potential common cause failures --

18 MR. JUNG: I understand.

19 MEMBER STETKAR: -- and diversity. I am
20 not particularly interested in somebody's perception
21 of what might be the most important accidents during
22 low power and shutdown. I don't try to presuppose
23 those things.

24 My simple question is, I know in the
25 technical specifications for at least new plants and

1 for some existing plants, there are protection
2 functions that must remain available during shutdown
3 modes. And indeed, for the new plant designs, there
4 is even a larger list of those shutdown protection
5 functions.

6 Those shutdown protection functions,
7 whether or not there are actual Chapter 15 accident
8 analyses done during shutdown is a question. But
9 those protection functions are required. Those
10 protection functions are invoked through the digital
11 protection system.

12 And the question is, does anyone review
13 that digital protection system for the applicant? Is
14 the applicant required to perform that review of that
15 system for those protection functions, in view of
16 common cause failures that may require diversity, in
17 the same level of detail that they are required --
18 "required" is a strong word --

19 MR. STATTEL: For a Chapter 15 accident.

20 MEMBER STETKAR: -- for the Chapter 15
21 accidents?

22 Because, as I said, there could be other
23 types of common cause failures that are invoked for
24 those functions that may need a different type of
25 diversity, other than the diverse functions that are

NEAL R. GROSS

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

1 justified based on the review of the at-power Chapter
2 15 types of accidents.

3 And I think what I am hearing is that it
4 is kind of a gray area. I am wondering whether it
5 needs to be a little bit more explicit because --

6 MR. EAGLE: Okay. Well, keep in mind that
7 the first thing, you have your instrumentation to
8 handle the various types of events. What we are
9 talking about here is that instrumentation, we are
10 starting to assume in common cause failure that it
11 all, basically, the four defensive channels, would
12 basically, we assume, disappear or is no longer
13 effective.

14 So, again, we are pointing back to it does
15 remain just, in general, what kind of functions you
16 have, and that is independent of the analysis report,
17 which covers a lot of areas.

18 MR. JUNG: John, the staff will get back
19 to you on that and look into it a little bit.

20 MEMBER STETKAR: Yes, check it, Ian.
21 Because, as I read through the discussion in the
22 public comments, there was some notion of the fact
23 that the analysis that you needed to perform, the
24 analysis that the applicant would submit to you and
25 the analysis that the staff would review, wasn't

NEAL R. GROSS

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

1 necessarily restricted to power levels above zero.

2 But I also read things, and the reason I
3 asked this question, being aware of tech spec
4 requirements for protection functions during shutdown
5 is the reason I raised this question, and recognizing,
6 you know, this guidance may not be updated for another
7 30 years or so, at the rate that we tend to update
8 regulatory guidance.

9 MR. STATTEL: Just so that I understand
10 what your question is, what you are questioning is the
11 scope of the analysis that the licensee would perform?

12 MEMBER STETKAR: Precisely.

13 MR. STATTEL: Right.

14 MEMBER STETKAR: Does it extend to
15 protection functions, safety protection functions? I
16 would point you to the tech specs.

17 MR. STATTEL: I mean, I am reading point
18 2, right? And it says, basically, "for each event
19 that is evaluated in the accident analysis section".
20 And it really doesn't go beyond that.

21 MEMBER STETKAR: Right.

22 MR. STATTEL: So, from the staff
23 perspective, we would just be making sure that those
24 events are covered in the analysis. Anything beyond
25 that, even if it is a tech spec requirement, it is

NEAL R. GROSS

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

1 kind of outside the scope of our review. I mean this
2 defines the scope of the analysis.

3 MR. EAGLE: It doesn't sit down and go
4 into specific details about what events are to take
5 place when you do the D3 analysis. That simply points
6 to, whatever is done in the normal analysis-type
7 things, then that should be covered in your D3
8 analysis.

9 MR. STATTEL: It's the SAR.

10 MR. EAGLE: Yes, the SAR.

11 MEMBER STETKAR: But we all know that the
12 design-basis accidents that people have been looking
13 at for the last 40 to 50 years are a stylized set of
14 accidents that people use for design-basis conditions,
15 and nobody ever thought of shutdown events when those
16 were created.

17 Well, it is now 2011. I will now use the
18 "R" word. We have done risk assessments of events
19 that have occurred during shutdown, and they don't
20 necessarily pose an insignificant risk, depending on
21 the plant design, depending on a lot. It is very
22 plant-specific.

23 MEMBER BLEY: And we have added regulatory
24 requirements.

25 MEMBER STETKAR: And we have added

1 regulatory requirements. In particular, there are now
2 tech spec requirements that require, legally require,
3 a plant to have operable protection systems and
4 functions to mitigate those accidents. Those are in
5 place right now. They are not hypothetical. They are
6 there.

7 Now whether or not anyone has done a
8 stylized Chapter 15 accident analysis for a rapid
9 boron dilution event for starting up an idle reactor
10 coolant loop that is full of pure water, no, they
11 don't do that.

12 Has anybody looked at LOCAs for mid-loop
13 conditions as a design-basis accident? No, they don't
14 do that. But there are requirements in technical
15 specifications to mitigate against those kinds of
16 events.

17 MR. STATTEL: And wouldn't the safety
18 functions also be credited? In many cases, they are
19 being also credited for --

20 MEMBER STETKAR: In some they might, but
21 the algorithms and the portion of the digital
22 protection system that invoke those things may be
23 different.

24 MR. STATTEL: I am trying to think of a
25 practical example with the reviews that I have

NEAL R. GROSS

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

1 performed, and I am having a hard time coming up with
2 something. Because every safety function that I have
3 reviewed, that they have performed this analysis for,
4 yes, we do review the tech spec because they are often
5 making tech spec changes. But the requirement for
6 diversity of that function is being addressed in the
7 accident analysis portion of that. And I can't think
8 of a case where there is some other function off on
9 the side that would be --

10 MEMBER STETKAR: We are taking probably
11 too much time. I think I have made my point.

12 I seem to recall one new plant design that
13 had kind of an interesting way of dealing with boron
14 dilution events, for example.

15 MR. STATTEL: I see. I see.

16 MEMBER STETKAR: And I can't remember the
17 design. I can't remember the details, and it is not
18 quite pertinent right now.

19 MEMBER BLEY: Well, even more simple than
20 that, we have additional instrumentation that is shut
21 down for measuring level in the loops and that sort of
22 thing, which isn't there. For power, you are not
23 looking at it at power.

24 MEMBER STETKAR: Operation, for example,
25 if you have a plant with pressurizer relief valves for

NEAL R. GROSS

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

1 a pressured water reactor, the algorithms for opening
2 those valves, the number of valves that are opened and
3 the conditions under which they are opened, are very
4 different for cold over-pressure protection than they
5 are for normal over-pressure events.

6 MR. EAGLE: Actually, the bottom line here
7 is this is a little bit out of the scope of the BTP
8 7-19. Basically, put it to Chapter 15 or to the basic
9 Safety Analysis Report, and that is where it should
10 carry the design basis that you should be using or
11 should be analyzing.

12 MEMBER BLEY: I think John is right, we
13 ought to move on. But I think what he has noted is we
14 have got a gap in how we check these things against
15 some of the requirements that are not in Chapter 15.

16 MR. EAGLE: That should be in Chapter 15,
17 you know, the rules and regulations that handle
18 Chapter 15. That is where that should be.

19 What we are saying is, once we have that
20 Chapter 15, then the Safety Analysis Report and the
21 events they look at --

22 MEMBER BLEY: One can cut it various ways,
23 but I see what you are saying.

24 MR. EAGLE: Right.

25 MEMBER STETKAR: Somebody has to take the

1 first step somewhere.

2 MEMBER BLEY: But that guy's not here
3 today.

4 (Laughter.)

5 MR. JUNG: Let's just end the
6 conversation. I am taking that as an action to
7 actually look to new reactors and work with Chapter 15
8 to see what kind of situation, and the tech specs,
9 that might get into this.

10 MEMBER STETKAR: It might even be in
11 existing reactors, depending on-- but I'll grant it,
12 from what Richard says, the existing do give you, you
13 know, for upgrades, do give you a list of the specific
14 safety functions that they are upgrading.

15 MR. STATTEL: Right. Well, we are basing
16 our review on an old system function, and they are
17 pretty well-defined.

18 MR. JUNG: John, I will work with
19 Christina to get back to you on that.

20 MEMBER STETKAR: Thanks.

21 MR. EAGLE: Again, what we said, that the
22 staff quoted the NRC's policy, four-point policy, on
23 D3, and then we added points to emphasize certain
24 things.

25 If the D3 analysis indicates a potential

NEAL R. GROSS

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

1 for a common cause failure, point 3 directs the
2 applicant to identify or add diverse means. Again, we
3 pointed out the safety computer indicated that this is
4 automatic safety functions that we are mainly
5 concerned with.

6 However, we also pointed out -- and, Mr.
7 Brown, this is going back to your point -- that point
8 3 applies. The manual initiation methods of the
9 reactor protection system, if subject to common cause
10 failure, then we are saying point 3 means that if you
11 have a common cause failure that is associated with
12 your manual actions that are used to start the reactor
13 protection system, then you also have to have a
14 diverse system for that. We'll come back to that in
15 a moment.

16 In other words, it could mean two sets of
17 manual initiation instruments, manual instruments.

18 CHAIRMAN BROWN: That fundamentally says,
19 whatever action you take on a division- or system-
20 level, whatever you want to call it, and it operates
21 via the four-division computer-based processing units,
22 then, obviously, that could be affected by a CCF.

23 MR. EAGLE: Right.

24 CHAIRMAN BROWN: So, I understood that
25 point in your thing, which would say, then, I have got

NEAL R. GROSS

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

1 to have some diverse method.

2 MR. EAGLE: Exactly.

3 CHAIRMAN BROWN: A diverse method doesn't
4 necessarily say it has to be part of, in other words,
5 it might not be part of the overall safety system, and
6 just be an analog, like a set of wires down to the
7 final two-out-of-four things --

8 MR. STATTEL: Correct.

9 CHAIRMAN BROWN: -- which you bypass all
10 the computing setups. That could, I guess, qualify as
11 diverse enough, based on the reading --

12 MR. STATTEL: Right, and for the Oconee
13 design, for example --

14 CHAIRMAN BROWN: You don't want to get me
15 started on that one.

16 (Laughter.)

17 MR. STATTEL: Well, for the Oconee design,
18 there is a means of manually initiating or manually
19 taking control of the individual safety components,
20 which is designed to meet the 603 requirement. So,
21 there is a convenient button for the operator to take
22 that manual control.

23 But that is relying on the computer that
24 is subject to the common cause failure to complete
25 that action. So, in addition to that, there is a

NEAL R. GROSS

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

1 manual initiation function that is downstream of that
2 which is completely independent of that computer
3 system.

4 CHAIRMAN BROWN: Okay. Go ahead. Yes, we
5 do need to be moving along here.

6 DR. HECHT: Is that what you meant by
7 special independence requirements for diverse means
8 may apply?

9 MR. EAGLE: Yes. We'll get back to that
10 in just a moment.

11 CHAIRMAN BROWN: There is another slide on
12 independence.

13 MR. EAGLE: Right.

14 CHAIRMAN BROWN: And I want to get to
15 those.

16 MR. EAGLE: Right.

17 CHAIRMAN BROWN: That is about slide 17 or
18 so.

19 MR. EAGLE: Yes.

20 DR. HECHT: Can I just ask one other
21 question?

22 MR. EAGLE: Yes.

23 DR. HECHT: In point 1 and point 3 of SECY

24 93-07 --

25 MR. EAGLE: Yes.

1 DR. HECHT: -- point 3 uses the words
2 "safety function" and point 1 uses the words "I&C
3 system". It doesn't use the words "safety computer"
4 in either case.

5 MR. EAGLE: It uses the term "safety
6 computer systems" in points 1 and 3.

7 CHAIRMAN BROWN: If you go to points 1 and
8 3, you won't find those words. You won't see the
9 words "computer safety system" anywhere. I have made
10 that as an edit note, but I wasn't going to say
11 anything until somebody else said something.

12 (Laughter.)

13 MR. EAGLE: Okay. If you notice, point 4
14 is where it is coming from. It says in point 4, "a
15 safety computer....identified in items 1 and 3 above".
16 That is where it is coming from.

17 CHAIRMAN BROWN: Yes, if you go back to
18 3 --

19 DR. HECHT: I see. Okay.

20 CHAIRMAN BROWN: In point 3, not the words
21 concerning point 3.

22 MR. EAGLE: Yes, yes. It should be items
23 1 and 3 refers to it.

24 Okay, the key point here is that it is
25 emphasizing that this is referring to the automated

NEAL R. GROSS

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

1 safety systems.

2 DR. HECHT: Okay. Thank you. Thank you.

3 MR. EAGLE: Point 4 is providing a set of
4 displays and controls, safety or non-safety, in the
5 main control room. Now these are diverse from any
6 common cause failure vulnerability in the reactor
7 protection system. Basically, these are the controls
8 the operator would use to handle a lot of different
9 instrumentations and equipment.

10 These meet the divisional independence
11 requirements as applicable to the specific design, and
12 these are for manual system-level or division-level,
13 depending on the design, actuation and control versus
14 the idea of component-level. Again, we brought up
15 this idea of component-level, having to do with a lot
16 of different instruments, setting valves, opening
17 things, versus the idea of system-level, where a very
18 limited number of components start the system.

19 Also, the staff interpreted that the
20 critical safety functions, we wanted to emphasize that
21 these were the plant-critical safety functions that
22 come out of the NUREG Supplement 0737.

23 If not subject to common cause failure,
24 some of these displays and manual controls may be
25 credited as all or part of the diverse means directed

NEAL R. GROSS

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

1 by point 3.

2 For digital modifications in operating
3 plants, retention of the existing controls in the main
4 control room may help satisfy point 4.

5 There is a point here that, if the
6 controls or the displays are left in place and are
7 being driven by new digital upgrades, they may not
8 satisfy point 4 after all. Once manual action from
9 the main control room using point 4 controls is
10 completed, controls outside the main control room may
11 be used for long-term management when supported by
12 suitable human factors engineering analysis and
13 procedures.

14 MEMBER STETKAR: Just for clarification,
15 Gene --

16 MR. EAGLE: Yes.

17 MEMBER STETKAR: -- that means, for
18 example, if I have an emergency feedwater system, and
19 I take credit for diverse manual, yadda, yadda,
20 yadda --

21 MR. EAGLE: Right.

22 MEMBER STETKAR: -- I must be able to
23 start it from the main control room. But if I need to
24 control steam generator levels, I can do that locally
25 out in the plant as long as I have the appropriate

NEAL R. GROSS

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

1 justifying human factors engineering analysis to do
2 that. Is that the way that is interpreted?

3 MR. EAGLE: Exactly.

4 MEMBER STETKAR: Okay. Thanks.

5 MR. EAGLE: The big thing was in public
6 comments they emphasized that there may be times, you
7 would have to get into very specific details, but
8 there may come a time when you may need something,
9 particularly we are talking about these plus-72-hour
10 situations when you may have all kinds of things in an
11 emergency that you may need. You might have to
12 realign the equipment valves and things like that.
13 Maybe a piece of equipment has failed, and you might
14 have to realign to be able to take --

15 MEMBER STETKAR: I guess I am stepping
16 back into the first sort of 15 minutes to an hour of
17 an accident, though. When I start my emergency
18 feedwater system, it typically comes on full-bore, and
19 I get full flow to the steam generators, and it is
20 more flow than I need. So, steam generator levels,
21 they initially dip for the cooldown, and then they
22 start to rise pretty quickly.

23 And somehow I need to start to control
24 emergency feedwater or else I overfeed my steam
25 generators, and my pumps may or may not trip,

NEAL R. GROSS

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

1 depending on the design. But since my digital I&C
2 design is now subject to this common cause failure, I
3 somehow need to control level not in 72 hours,
4 probably within the first 30 minutes -- or I don't
5 want to use that term -- within the first hour or so
6 or less.

7 MEMBER BLEY: Much less for some plants.

8 MEMBER STETKAR: Much less for some
9 plants.

10 (Laughter.)

11 That is not a long-term action. And if
12 the guidance says that I can do that manually out in
13 the plant by having operators go out and adjust the
14 flow control valves manually, that is fine, but I
15 would certainly want to see the analyses to justify
16 that. And I am hoping that the guidance is clear
17 enough that those analyses are required.

18 MR. EAGLE: Yes, that comes up in another
19 place where they talk about components versus system-
20 level, and we will talk about that in just a moment.

21 MEMBER STETKAR: Okay.

22 MR. EAGLE: But we also wanted to
23 emphasize that things aren't always limited just to
24 the control room the only thing. They are generally
25 expected to operate from the control room, but there

NEAL R. GROSS

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

1 may come times and situations -- 72 hours was just an
2 example on that.

3 MEMBER STETKAR: Well, I'm trying to
4 understand the thought process that went into some of
5 the words in the guidance.

6 Thanks.

7 MR. EAGLE: Once again, the critical plant
8 safety functions, they come from NUREG-0737,
9 Supplement 1. These are items that you are probably
10 quite familiar with, and they cover a wide area. They
11 are also represented in the safety parameter display
12 system, where they present all kinds of information
13 that is used to support this kind of safety functions.

14 At this time, we are going to examine the
15 independence of the diverse means.

16 MR. STATTEL: Yes, I am just going to say
17 a few words about the independence requirement for the
18 diverse means, diverse, of course, from the safety
19 protection system. Generally, the requirements are
20 derived from IEEE 603, which is the rule-based
21 standard.

22 One thing I want to point out is that the
23 diverse means can be initiated by implementing a
24 safety system, in which case the independence and
25 separation requirements between divisions would have

NEAL R. GROSS

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

1 to be invoked. Or it can be implemented using a non-
2 safety-related system. There are plants out there
3 that have either method, right?

4 And in the case for non-safety-related
5 diverse systems, there are requirements for separation
6 between the safety and the non-safety portions of the
7 I&C systems. In either case, the diverse means should
8 be independent of the safety systems, such that the
9 common cause failure that we are postulating would not
10 affect that diverse system, of course.

11 CHAIRMAN BROWN: Okay. Now this is an
12 interesting slide because when I read your all's 6, 7,
13 8, and 9, the additional under the acceptance criteria
14 part, as I was reading it, I never saw the word in 6,
15 7, 8, or 9 -- the words "independence" were kind of
16 mused, in my opinion. So, I wrote notes, all kinds
17 of notes, okay, all over the page. Where is
18 independence?

19 It looked like to me there was a dichotomy
20 in that, if you had a diverse means that actuated
21 within the safety system, independence was not
22 required. Whereas, if it was a safety-related --
23 excuse me -- if it was a safety-related diverse
24 application, then independence was not required. And
25 then, if you had a diverse non-safety system, it was

NEAL R. GROSS

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

1 required, per Clause 5.6.

2 MR. STATTEL: This issue --

3 CHAIRMAN BROWN: Let me finish.

4 MR. STATTEL: Okay.

5 CHAIRMAN BROWN: If I don't get all this
6 out, I'll forget it all.

7 MR. STATTEL: Okay.

8 CHAIRMAN BROWN: So, I read 6, 7, and 8.
9 Then, in the process of reading all the industry
10 comments on apparently what was your all's initial
11 version of that, where you had the words, for 6, 7, 8,
12 and 9 were the words "if the means is independent",
13 and then "if the means is independent" in 7, and on,
14 ad infinitum.

15 Industry came back and said, oh, no, no,
16 there's no requirement for independence. And you all
17 said, well, absolutely, we agree with that, and you
18 struck the word "independence" from items 6, 7, 8 in
19 the context of this subject.

20 So, I really got confused about how we can
21 have diverse systems, I don't care whether they are
22 safety-related or non-safety-related, and how they can
23 be even credited if they are not independent with each
24 other or from the system itself.

25 MR. STATTEL: Right. This came up during

NEAL R. GROSS

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

1 our discussions and with resolving the comments from
2 industry.

3 Basically, it didn't have a lot to do with
4 incorporating the changes from ISG-02. Basically,
5 when they were reading that, it occurred to us and
6 some utilities that the existing wording from the
7 previous revision didn't really fit when you were
8 implementing the diverse means using a safety system,
9 right?

10 CHAIRMAN BROWN: You just lost me with
11 that statement.

12 MR. STATTEL: I think originally it was
13 written with the assumption that it was going to be
14 non-safety, and the non-safety system had to be
15 separated and independent from the safety protection
16 system, right? I think that was the original
17 verbiage.

18 But when we received the comments and we
19 started having the dialog with NEI and industry, it
20 was apparent that they have an option. They can use
21 a safety or they can use a non-safety to meet these
22 requirements.

23 And basically, it is hard to prescribe
24 what the independence requirements are when they are
25 going to be different depending on which choice, which

NEAL R. GROSS

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

1 fork you take in that path.

2 So, we revised the wording in several of
3 the clauses, and you see that in the comments there,
4 to make it such that, if a licensee chooses to
5 implement the diverse means using a safety system --
6 for example, at one plant that I am familiar with,
7 they chose to implement an ATWS diverse scram system
8 using an ESFAS system, right? So, they have a reactor
9 protection system, four-channel system, and they have
10 a four-channel ESFAS system, which is also safety-
11 related, that implements the ATWS functions.

12 Well, the ATWS functions, if you think
13 about this, they are using the same four divisions, A,
14 B, C, D, as the safety function does. So, you can't
15 stipulate that channel A of the ATWS function needs to
16 be independent electrically from the channel A of the
17 safety function because they are in the same division,
18 right? Now if it was implemented in a non-safety
19 system, you could implement that kind of separation,
20 that kind of independence.

21 So, what we did here is we revised the
22 clauses to incorporate both options for the licensee,
23 right?

24 So, ultimately, the independence we are
25 talking about that we want to verify is that, when the

NEAL R. GROSS

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

1 safety function has a common cause failure that
2 affects all the divisions, that failure is not going
3 to propagate over to the diverse means, whether it is
4 safety or whether it is non-safety.

5 MR. EAGLE: Point 4 is kind of like the
6 bottom line.

7 MR. STATTEL: So, there are different
8 requirements, depending on which choice the individual
9 licensee makes.

10 CHAIRMAN BROWN: That is really not very
11 clear if you read 6, 7, 8, and 9, in my personal
12 opinion. I mean, I go back and it says --

13 MR. STATTEL: Are you referring to the
14 slide numbers?

15 CHAIRMAN BROWN: No, I'm referring to the
16 -- well, no, this slide can stay up. I mean, that is
17 kind of your summary slide.

18 MR. EAGLE: Right. And this is almost a
19 quote right out of where we are talking about various
20 criteria for the diverse means.

21 CHAIRMAN BROWN: Well, I'm looking at
22 acceptance criteria 3.1, item 6. Where is it? Okay,
23 it is the last sentence in there.

24 It says, notice if the diverse system is
25 non-safety, IEEE 603.56, independent, directs the

NEAL R. GROSS

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

1 separation of independence of the safety systems and
2 the diverse means.

3 MR. STATTEL: Right.

4 CHAIRMAN BROWN: Okay? Very explicit,
5 non-safety-related, diverse means; must be
6 independent.

7 MR. STATTEL: Well, from the perspective
8 of --

9 CHAIRMAN BROWN: That is based on IEEE
10 603, in other words, the rule that drives it.

11 MR. STATTEL: From the perspective of a
12 licensee who has implemented diversity using a safety
13 system --

14 CHAIRMAN BROWN: I'm not there yet.

15 MR. STATTEL: -- using the safety systems,
16 that clause doesn't make sense because that is not a
17 clause that is applicable. Okay?

18 CHAIRMAN BROWN: That may be the case.

19 MR. STATTEL: Right.

20 CHAIRMAN BROWN: But I don't see anywhere
21 within the words in 6, 7, 8, or 9 where I could derive
22 the point that a diverse system implemented within the
23 safety system must be independent or should -- must
24 be. Okay, let me phrase that the way I think it ought
25 to be. Must be independent of the safety system

NEAL R. GROSS

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

1 within which it is designed or actuated or
2 implemented. Okay?

3 There is nothing explicitly in there that
4 says that a diverse system implemented within the
5 safety division, whether it be the ESFAS or whether it
6 be the reactor protection system, must be independent
7 of the safety systems, mainline safety systems in each
8 one of those, in either one of those.

9 I didn't see that separation or that
10 independence. It led me to believe, based on reading
11 those words, and then, particularly emphasized by
12 industry comments where they requested you to take out
13 the word "independent". Effectively, they rewrote the
14 words for you and said, "We recommend the wording be"
15 such-and-such.

16 So, that point is lost, as far as I can
17 see from the way this is written right now. Now your
18 four bullets say that independence requirements of
19 diverse means from safety protections are defined in
20 603. That is your first bullet. But how I get that
21 reflected over here in 7-19, in 6, 7, 8, or 9, I don't
22 see that.

23 MR. EAGLE: I think you have to also keep
24 the whole document in mind when putting together,
25 examining the common cause failure in diverse

NEAL R. GROSS

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

1 systems --

2 CHAIRMAN BROWN: There were a few points,
3 there were a few places where you shouldn't have to
4 consult five different references or paragraphs to get
5 a clear picture, is independence required if a diverse
6 means is executed within a safety system itself, as
7 opposed to a separate system.

8 MR. STATTEL: But wouldn't such guidance
9 just be a reiteration of the existing guidance that we
10 have in 603?

11 CHAIRMAN BROWN: I don't know. In 603?
12 I got the flavor out of this that you kind of set 603
13 off to the side relative to the diverse actuation
14 within a system to only apply to non-safety-related
15 diverse systems. That's the way I read it, either
16 rightly or wrongly. But I spent two hours reading
17 this, those four parts and the comments.

18 MR. STATTEL: That wasn't our intent.

19 CHAIRMAN BROWN: Oh, I know it's not your
20 intent; I didn't think it was your intent. So, I was
21 a little bit petrified, is one way of phrasing it,
22 that we would lose that connection between
23 independence of a diverse system implemented within a
24 safety system, and it is within a safety-related
25 system.

NEAL R. GROSS

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

1 MR. EAGLE: That's why this was presented
2 in a special paragraph, special areas, where we talk
3 about the characteristics of the diverse means.
4 That's where it was presented.

5 MR. JUNG: Charlie, we will see whether we
6 can make it clearer and get back to you.

7 But I think the intention was to ensure
8 603 independence requirements in the 5.3 section of
9 the 603 --

10 CHAIRMAN BROWN: Well, the second bullet
11 is very, very nice. It says, "Diverse means could be
12 safety-related and part of a safety division, and
13 would be subject to meeting divisional independence
14 requirements."

15 That is not stated in BTP 7-19. That is
16 a nice bullet.

17 MR. EAGLE: That came right out of 7-19.

18 CHAIRMAN BROWN: Well, you show me those
19 words and I'm happy.

20 (Laughter.)

21 MR. EAGLE: Okay.

22 MEMBER BLEY: Maybe at the break.

23 CHAIRMAN BROWN: Pardon?

24 MEMBER BLEY: I said maybe they can do it
25 at the break.

1 CHAIRMAN BROWN: I'm happy with that.

2 MR. JUNG: I think, Charlie, we can easily
3 fix that.

4 CHAIRMAN BROWN: If that's the case, I'll
5 be willing to read it.

6 MR. EAGLE: We will show it to you at this
7 moment. Do you want to look it up? Here it is.

8 MR. STATTEL: I mean, clearly, we didn't
9 want to discourage people who are designing these
10 systems from using safety --

11 CHAIRMAN BROWN: Oh, I agree with that.
12 I don't disagree with that.

13 That second bullet now resolves
14 fundamentally my issue, but I couldn't find that nice,
15 crisp statement phrased exactly that way. Because
16 bullets 2 and 3 give you fundamentally what I would
17 have expected to see; it has got to be independent in
18 either one of the two cases.

19 And it seems to start getting muddied, and
20 the muddiness increased when I started reading the
21 industry comments, which seemed to emphasize that
22 independence is not -- they specifically say
23 independence is not required. And you all said, "We
24 agree with that."

25 MR. STATTEL: Well, in that condition

NEAL R. GROSS

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

1 where you are implementing your diverse means within
2 the safety instrumentation, then you don't need to
3 show independence between channel A of your safety
4 system and channel A of your diverse system with
5 regard to electrical isolation characteristics.

6 So, anyway, I think we understand your
7 point, and Gene is going to look into that.

8 MR. EAGLE: We'll come back to that in a
9 moment, because these came right out of the BTP 7-19.

10 MR. STATTEL: Hopefully, we will be able
11 to come back --

12 CHAIRMAN BROWN: Don't do that research.
13 We need to get on with the slides here. You've got my
14 point.

15 MR. STATTEL: So, one objective of the D3
16 analysis --

17 CHAIRMAN BROWN: Let John --

18 MR. STATTEL: I'm sorry.

19 MEMBER STETKAR: It doesn't have anything
20 to do with independence. So, reset.

21 MR. STATTEL: Okay.

22 MEMBER STETKAR: But it is within the
23 context of diverse automation. I didn't know where
24 else to bring it up.

25 In acceptance criterion 3.4, if you want

NEAL R. GROSS

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

1 to look at the document -- and just for the record,
2 let me quote from that. It says, "The automated
3 diverse means may be performed by a non-safety system
4 if the system is of sufficient quality to perform the
5 necessary functions under the associated event
6 conditions. The automated diverse means should be
7 similar in quality to systems required by the ATWS
8 rule, 10 CFR 50.62, as described in the enclosure to
9 Generic Letter 85-06, 'Quality Assurance Guidance for
10 ATWS Equipment that is Non-Safety-Related'." I
11 understand that.

12 Then, there is the last sentence that
13 says, "Other systems that are credited in the analysis
14 that are in continuous use -- for example, the normal
15 reactor coolant system, inventory control system, or
16 normal steam generator level control system -- are not
17 required to be upgraded to the augmented quality
18 discussed above."

19 So, why do we need quality equipment,
20 quality non-safety equipment specifically for ATWS
21 protection, but we don't need quality non-safety
22 equipment for inventory control or core heat removal?

23 MR. EAGLE: Because its quality has
24 already been established and it is continually in
25 operation.

1 MEMBER STETKAR: I don't care whether it
2 is in continuous operation. I can run my automobile
3 continuously, too. It isn't all that high quality
4 anymore.

5 I don't understand this dichotomy about
6 calling out things for ATWS quality, and now suddenly,
7 when somebody wants to take credit for some other
8 system as a diverse means, it doesn't have to meet any
9 type of augmented quality standard.

10 MR. EAGLE: This came directly, was
11 carried over from Revision 5, as I recall. The idea
12 here is being expressed that a system just sitting
13 there not doing anything, like ATWS, you know, it
14 needs to have especially emphasis on the quality.
15 Whereas, again, the systems that are in regular use
16 for operations do have their own quality requirements.

17 MEMBER STETKAR: You apparently never
18 operated the Zion plant with our charging pumps, for
19 example.

20 (Laughter.)

21 MR. EAGLE: You know, they are recognizing
22 that there is a problem with the equipment, when it is
23 being used on a continually regular basis, that is
24 easy to recognize. Systems that are just sitting
25 there, for instance, like your air bag --

NEAL R. GROSS

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

1 MEMBER STETKAR: No, I understand. So,
2 the real key is the fact that they must be in
3 continuous use?

4 MR. EAGLE: Yes, because you can recognize
5 a failure, and if you can't be able to recognize that
6 failure that quickly, you need to have an extra higher
7 level of quality.

8 And like I said, one of your best examples
9 is your air bag. It could sit there for years, and
10 every time you turn on your car it tests it. So, it
11 has to be a type of quality because it is not in
12 continual use like the automobile engine. You would
13 quickly detect a problem with that. That is similar
14 to what is being said here.

15 This is also kind of a carryover from Rev.
16 5.

17 MEMBER STETKAR: I understand. There is
18 a lot of stuff that is a carryover from ATWS.

19 MEMBER BLEY: There's one thing here that
20 leaves me a little unsettled, in that some of the
21 controls, not some, all of the newer control systems
22 continually self-test as they are going on, which is
23 a little bit akin to equipment running, and it doesn't
24 seem we are consistent there.

25 MR. STATTEL: Well, as we have stated,

1 this was not part of this particular revision. So, I
2 don't think there were public comments on this
3 particular clause.

4 MEMBER STETKAR: No, there wasn't.

5 MR. STATTEL: But, like Gene said, I think
6 really think the emphasis on quality that was
7 established during the ATWS rule, I think it was
8 primarily directed at systems that are kind of in a
9 standby state waiting to perform their function.
10 Whereas, a feedwater control system which is in
11 continuous operation, it is a fairly reasonable
12 assumption that a feed reg valve will operate on
13 demand when it is continually controlling steam
14 generator level. So, there wasn't as much of a
15 concern.

16 Now I'm just conjecturing here.

17 MEMBER STETKAR: Yes, but the notion is
18 the "continuous operation" is the most important
19 clause in that sentence.

20 MR. STATTEL: Right. Exactly.

21 MEMBER STETKAR: Because I know of some
22 systems that, some plants, new plant designs, that
23 have non-safety makeup systems that are not in
24 continuous operation.

25 So, the question is, if an applicant were

NEAL R. GROSS

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

1 to take credit -- or they're operated periodically.

2 MR. STATTEL: Correct, yes.

3 MEMBER STETKAR: Not continuously.

4 MR. STATTEL: Right.

5 MEMBER STETKAR: If an applicant were
6 going to take credit for that, would you then require
7 that system to meet some sort of quality level?

8 MR. STATTEL: I would say yes.

9 MEMBER STETKAR: Because the pumps aren't
10 always operating.

11 MR. STATTEL: Yes. I would say yes.

12 MEMBER STETKAR: Okay.

13 MR. STATTEL: In the diversity analyses
14 that I have reviewed personally, the systems that I
15 review for these quality characteristics are the ones
16 that are kind of in standby mode.

17 MEMBER STETKAR: Yes. Okay.

18 MR. STATTEL: Right.

19 MEMBER STETKAR: Okay. Thanks.

20 CHAIRMAN BROWN: By the way, this is not
21 in Rev. 5. It is really in ISG-02, at page 2, the
22 fifth paragraph.

23 MR. EAGLE: Okay. I stand corrected then.

24 CHAIRMAN BROWN: No, you just said 5. So,
25 if somebody is looking for it, they are not going to

NEAL R. GROSS

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

1 find that there.

2 MR. EAGLE: I guess it was not good memory
3 on it.

4 By the way, Charlie, these paragraphs on
5 independence that we talked about, if you will look on
6 page 7, under concerning point 3, the specific
7 paragraph was put in on independence. And that is
8 where that was specifically put in to cover these
9 points. In fact, it is almost breaking it down into
10 four points.

11 Okay? So, one of the objectives --

12 CHAIRMAN BROWN: Before you go on, you say
13 that is on -- I've got to make a note here, so I can
14 find this.

15 MR. JUNG: That is on page 7, concerning
16 point 3.

17 CHAIRMAN BROWN: Yes, I found it,
18 concerning point 3, yes.

19 MR. JUNG: The second paragraph of that
20 section, the second sentence.

21 MR. EAGLE: And that was specifically put
22 in to outline these four items or these things.

23 CHAIRMAN BROWN: They are not as crisp, by
24 the way. They're not as crisp as these two, I don't
25 think. I just quickly -- I'll read them again. We're

NEAL R. GROSS

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

1 not going to go any farther on this. There's other
2 needier things to work on also.

3 All right, I got it. Go ahead.

4 We are going to take a break, contrary to
5 what the schedule looks like. Okay?

6 (Laughter.)

7 I will never exist for three hours here
8 with three hours-plus change.

9 So, at a convenient point, separation of
10 subjects, if we could, if you see one, and I didn't
11 know if that would be, if I look ahead, where we start
12 into the stakeholder concerns or --

13 MR. STATTEL: Actually, that would be
14 probably a good point. Let me just say a few words on
15 the current slide. And then, if you have no
16 questions, then we can break at that point.

17 CHAIRMAN BROWN: Okay. Is that acceptable
18 to everybody else? Okay. All right, I didn't want to
19 break in the middle of something that was going on.
20 Thank you.

21 MR. STATTEL: Yes, that's a good point.

22 CHAIRMAN BROWN: Okay.

23 MR. STATTEL: Okay. Really, the purpose
24 of this slide is to point out one of the objectives of
25 performing the D3 analysis would be to determine if

NEAL R. GROSS

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

1 the diverse method is required. Once that
2 determination is made, there are criteria that are
3 applied, and we review to confirm. These criteria are
4 used for designing that diverse system. And that is
5 what this list here is.

6 DR. HECHT: Can I ask a question about the
7 second point, initiated from the control room?

8 MR. STATTEL: Yes.

9 DR. HECHT: Is that true for both
10 automated and manual systems or only for manual
11 systems? Because point 4 of the SECY guidance said
12 specifically for manual control, but here it is not
13 clear if that is for manual or automated control.

14 MR. EAGLE: Remember, point 4 pointed out
15 specifically that it would be from the control room.

16 DR. HECHT: Right.

17 MR. EAGLE: Okay. Point 3 is the point
18 that says you will have a diverse system.

19 DR. HECHT: Right.

20 MR. EAGLE: Point 4 is a set of displays
21 and controls. Now those displays and controls could
22 actually be all or part of the diverse system.

23 DR. HECHT: Right.

24 MR. EAGLE: Right.

25 MR. STATTEL: In reality, I have never

NEAL R. GROSS

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

1 seen an automatic diverse system that is outside of
2 the controls, that is completely outside of the
3 control room.

4 The diverse systems that we have reviewed
5 also have their own manual initiation features, and
6 those are in the control room.

7 MEMBER STETKAR: When you say you haven't
8 seen one that is completely -- you mean that has no
9 controls in the control --

10 MR. STATTEL: Right. Exactly.

11 MEMBER STETKAR: That the cabinets are not
12 in the control room?

13 MR. STATTEL: Not necessarily the cabinet,
14 but one that would have no operator interface in --

15 MEMBER STETKAR: Okay.

16 MEMBER BLEY: But that is what is the
17 intent here, is the operator interface, not the
18 cabinet.

19 MR. STATTEL: Exactly. So, for example,
20 in Oconee, there is a diverse actuation system, and
21 there are override buttons, right? And there are
22 conditions, common cause failure conditions, for
23 example, or spurious actuation conditions, where the
24 operator would need to take action on the diverse
25 system. He has to have those controls in the control

NEAL R. GROSS

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

1 room. He has to have the ability to do that from the
2 control room.

3 DR. HECHT: So, is the point here on 19,
4 when it says, "initiated from the control room," you
5 mean if manually-initiated, then initiated from the
6 control room? Is that what you mean?

7 MR. STATTEL: Yes.

8 DR. HECHT: Because, you know, I can give
9 you a counterargument, and I have not seen or reviewed
10 nearly as many plants as you have, but I could imagine
11 an argument to be made that, if you are going to have
12 automatic diverse means, and it is possible to have
13 all of the signaling and the wires --

14 MR. STATTEL: Locally?

15 DR. HECHT: -- locally, that you might
16 choose to do it that way, and that might be a
17 preferred design.

18 MR. STATTEL: I have not seen that. I
19 mean, the diverse system, like any typical I&C system,
20 requires some operation. Even though it is a standby
21 system that is required for operability, it requires
22 some operator interface. And generally speaking, if
23 it is performing a safety function, right, if it
24 designed to perform a safety function, then it is from
25 within the control room that the operator would be --

NEAL R. GROSS

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

1 DR. HECHT: Well, the operator might
2 monitor it. I mean, there might be an alarm there,
3 but, still, the actual initiation, the relay, you
4 know, making that relay trip might be done locally.
5 I mean, does the guidance --

6 MR. EAGLE: I think that we're simply
7 saying that, if you have a diverse system, that it is
8 to be activated from the control room if it involves
9 any kind of manual part of it. I think that is part
10 of the requirements.

11 CHAIRMAN BROWN: But that doesn't mean the
12 system has to be in the control room. The boxes --

13 MR. EAGLE: Right, the boxes, you know --

14 CHAIRMAN BROWN: It could just be a switch
15 or it could be a whatever, right?

16 DR. HECHT: I didn't see that language
17 when I read the standard. I just saw it right now in
18 this slide.

19 MR. STATTEL: I do see your point here.
20 Because, even on the Aconee system, the actual
21 electronics cabinet is outside of the control room.
22 So, it doesn't require a manual interaction with the
23 system to initiate that.

24 I really think that was intended for the
25 manual initiation of the diverse means.

NEAL R. GROSS

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

1 DR. HECHT: Does this language appear
2 without that "if manually initiated" in the text? Or
3 you don't know yet?

4 MR. STATTEL: I'd have to look that up.

5 MR. EAGLE: I think we are getting to the
6 point where it is indicating that, basically, if you
7 have manual things, we expect them to be in the
8 control room.

9 DR. HECHT: Right. Yes.

10 MR. EAGLE: And you remember, the
11 electronics for the scram are not right there in the
12 control room. They are in the equipment area. It's
13 around. They are still, basically, part of the
14 control room effectively.

15 But the things that the operator uses, any
16 kind of manual thing is usually right there in the
17 control room, typically. It is kind of hard to think
18 about your electronics being, worrying about whether
19 that is actually in the control room per se.

20 DR. HECHT: Now I am reading in Section
21 1.7 of the BTP. It does state that the required
22 safety function can be accomplished via either
23 automated system or manual operator actions performed
24 from the main control room.

25 MR. STATTEL: That is a little bit more

NEAL R. GROSS

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

1 clear than the actual text, yes.

2 MR. EAGLE: Also, we use the term
3 "initiated" from the main control room.

4 DR. HECHT: Well, "initiated" could be
5 automatically initiated, just based on this slide,
6 based on --

7 MR. STATTEL: Yes, I think it is more of
8 an error with the slide than with the --

9 DR. HECHT: Okay. All right.

10 MEMBER STETKAR: Richard, I had one. I'm
11 trying to make Charlie as uncomfortable as possible
12 here for the break.

13 CHAIRMAN BROWN: You will pay the price.

14 (Laughter.)

15 MEMBER STETKAR: I didn't know where to
16 bring this up, but we are sort of touching on it. And
17 tell me whether it is better to discuss it sometime
18 later.

19 Section 3.5 of the acceptance criteria
20 says, "Safety-related commands that direct a component
21 to a safe state must always have the highest priority
22 and must override all over commands."

23 This is under the context of use of manual
24 action as a diverse means of accomplishing safety
25 functions.

1 It is also noted that, "This
2 recommendation does not prohibit the use of manual
3 controls for operating individual safety system
4 components after the corresponding safety system
5 functions have been actuated."

6 There may be common cause failures that
7 initiate a, quote/unquote, "safe state" of a
8 protection function that is not necessarily good for
9 a particular accident scenario. I may not want to
10 blow down my steam generators, for example, during
11 some accident scenarios. I may not want to actuate my
12 diverse -- or not diverse -- blow down the primary
13 system and create a large LOCA during accident
14 scenarios. So, therefore, some of the common cause
15 failures that could actuate those safe-state functions
16 may not be a good thing.

17 That clause of the guidance, though, seems
18 to say that the operator cannot, shall not intervene
19 to be able to stop that.

20 MR. STATTEL: Well, that's interesting
21 about this, but --

22 MEMBER STETKAR: Let me follow on.

23 I am aware of some older European designs.
24 I'm not aware of current features in those designs,
25 but older features of those designs that did, indeed,

NEAL R. GROSS

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

1 have a manual override. It was complex. You had to
2 put in a coded acceptance code before the operators
3 could take control, but specifically for those types
4 of functions, the operators could actually get in and
5 stop this.

6 This seems to say that we can't do that.
7 Is that the intention?

8 MR. STATTEL: That's not the intent.

9 MEMBER STETKAR: Okay.

10 MR. STATTEL: But it is very interesting
11 you bring this point up because this was an issue that
12 came up, actually, during the Oconee inspections.

13 MEMBER STETKAR: Oh.

14 MR. STATTEL: And I'll just briefly
15 describe the situation.

16 Basically, in their simulations they were
17 simulating large break LOCA conditions, right, in
18 which case the pressurizer pressure dropped very
19 rapidly and very far, right? Now the setpoints for
20 the safety system and the diverse system were
21 different.

22 So, when we performed our analysis, we
23 concluded that either system actuating would be
24 sufficient to prevent core damage, but we didn't
25 really postulate, we didn't really see it through.

NEAL R. GROSS

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

1 And they didn't see it until the simulations, where
2 they initiated the LOCA. Then the next step in their
3 EOP was to take manual control of the safety injection
4 pumps and run them back to prevent them from going
5 into a runout condition, which is very similar --

6 MEMBER STETKAR: Yes, I didn't even think
7 of that one, but yes.

8 MR. STATTEL: -- to the one you were
9 describing, right?

10 And when they ran that scenario, they were
11 unable to take manual control. The reason they were
12 unable to take the manual control was because the
13 diverse system had locked into the safety condition.

14 MEMBER STETKAR: Yes. Yes, yes, yes.

15 CHAIRMAN BROWN: Yes. Okay. Go ahead.
16 I'm sorry.

17 MEMBER STETKAR: Are they still working on
18 that?

19 MR. STATTEL: It is a very difficult
20 problem. The way they solved it, and I was not
21 completely comfortable with this, but the way they
22 solved it was, procedurally, they did have an override
23 button on the diverse actuation system. And they put
24 steps in their procedure on normal course, following
25 their EOPs, once the LOCA occurs and you get into that

NEAL R. GROSS

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

1 condition where they need to take manual control of
2 that pump, they procedurally override the diverse
3 system.

4 Now I'll tell you this. I had concerns
5 when they told that to me because here we are, we are
6 going to all this trouble of requiring and installing
7 and designing this diverse system that is truly
8 independent of the safety system. And then, you're
9 putting procedures and you are relying on the operator
10 to do the right thing in order to --

11 MEMBER STETKAR: See, an override is one
12 thing. A manual intervention and reset is something
13 else.

14 MR. STATTEL: Right, right. Now what we
15 told them, the inspection team, we gave them feedback
16 on that response. That was their initial response;
17 just add a step in there to defeat the diverse system.

18 What we required them to do --

19 MEMBER BLEY: Just for me, just for me, is
20 that a momentary switch you have to hold or is that a
21 switch you can throw, override it? If it is switch
22 you can throw, that is really troublesome.

23 MR. STATTEL: No, I believe it was a push
24 button.

25 MEMBER BLEY: So, a guy would have to

NEAL R. GROSS

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

1 stand there and hold it?

2 MR. STATTEL: I mean it takes a deliberate
3 action.

4 MEMBER BLEY: But you push it once and it
5 is overridden or does a guy have --

6 MR. STATTEL: Yes.

7 CHAIRMAN BROWN: Dennis, if you want to
8 stop a pump because it is doing something you don't
9 want it to, you don't want to have to stand there and
10 hold it.

11 MEMBER BLEY: If you can push that button
12 -- can you push it ahead of time and have it disabled?

13 MR. STATTEL: Let me explain what the
14 inspection team suggested and they incorporated in the
15 procedure.

16 We stipulated that prior to taking that
17 action to defeat that diverse system that they would
18 verify, somehow verify and ensure that the safety
19 function had actually performed to completion, right?
20 So, basically, there is a confirmation step prior to
21 taking the action of defeating the --

22 MEMBER BLEY: I'm not asking my question
23 right here.

24 MR. STATTEL: Now it is not an ideal
25 solution, but this is the solution --

NEAL R. GROSS

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

1 MEMBER BLEY: I'm still not asking my
2 question right. To override that system, does the
3 safety injection already have to be engaged and
4 running? Or could I go over there before the
5 accident, override that system, put the cover back on,
6 and then --

7 MR. STATTEL: You can. Yes, you can.
8 That's always been a feature of --

9 MEMBER BLEY: It will lock in override.
10 So, anywhere along the line, somebody could have
11 overridden that and leave it set --

12 MR. STATTEL: Turn power off to the
13 diverse system. I mean there's a lot of ways --

14 MEMBER BLEY: Some things are a lot easier
15 to notice that you did them than others.

16 MR. STATTEL: But the real purpose of
17 having those override buttons --

18 MEMBER BLEY: I understand.

19 MR. STATTEL: -- on the control board was
20 to deal with a spurious actuation, right? That is the
21 primary purpose of having those buttons there.

22 But this was something that really didn't
23 come up in our analysis. However, when they ran their
24 simulations, it was a problem that presented itself.

25 MEMBER STETKAR: I guess coming back, that

NEAL R. GROSS

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

1 is a real interesting actual example.

2 MR. STATTEL: Well, recently, I was at
3 ANS, and I presented this to the industry. Because,
4 honestly, I have been doing a lot of thinking about
5 this particular problem. The solution would be to
6 somehow have the diverse actuation system be aware of
7 whether or not the safety system is actuated.

8 MEMBER STETKAR: Yes.

9 MR. STATTEL: But once you initiate that
10 tie, you can postulate the failure that prevents the
11 diverse system from occurring, from doing its
12 function, right? So, you don't want to really do
13 that.

14 MEMBER STETKAR: Right.

15 MR. STATTEL: That's not the solution.
16 So, actually, at ANS I presented out to the industry:
17 come up with a solution for this because I don't know
18 the solution.

19 MEMBER STETKAR: Okay.

20 MR. STATTEL: It is not an easy problem to
21 solve.

22 But going back to your original
23 question --

24 MEMBER STETKAR: When I read the guidance,
25 though, the guidance seems to say that --

NEAL R. GROSS

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

1 MR. STATTEL: Well, going back to your
2 original question, I think that the reason for the --

3 MEMBER STETKAR: -- we can't intervene.

4 MR. STATTEL: I think that is the reason
5 for the final sentence, though. The recommendation
6 does not prohibit, nor is it intended to prohibit, the
7 use of manual controls for operating individual safety
8 components, right?

9 MEMBER STETKAR: Well, but it is all
10 within the context of getting things started, though,
11 is the problem, right. It leaves a thin, gray area
12 for different interpretation, I think, but the whole
13 context of that section is actually ensuring that the
14 safety functions, you know, that the design-basis safe
15 state is achieved and that the operator cannot prevent
16 that from happening, basically.

17 MR. STATTEL: Right.

18 MEMBER STETKAR: I mean, that is the whole
19 context there.

20 MR. STATTEL: Right.

21 MEMBER STETKAR: The last sentence kind of
22 gives you --

23 MR. STATTEL: Well, the last sentence does
24 kind of give you the out. I mean, it is a manual
25 action. You are relying on the operators to do the

NEAL R. GROSS

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

1 right thing. We put procedural controls in place.

2 MEMBER STETKAR: Well, I mean, the whole
3 notion should be that the safety function is
4 initiated, but the operators have the ability to then
5 intervene and reset, if I can use that term, rather
6 than override or --

7 MR. STATTEL: Sure. Exactly.

8 MEMBER STETKAR: -- block, or something
9 like that.

10 MR. STATTEL: Yes, and those are standard
11 design features with really any engineered safety.

12 MEMBER STETKAR: Current ones, that's
13 true.

14 MR. STATTEL: Right.

15 MEMBER STETKAR: But the concern is here
16 in terms of -- your example is a great example. The
17 diverse system took over --

18 MR. STATTEL: Yes.

19 MEMBER STETKAR: -- and, essentially,
20 could not be reset.

21 MR. STATTEL: That's right.

22 MEMBER STETKAR: So, the question is, you
23 know, if I am doing my D3 analysis now, submitting it
24 to you as the staff, if I have a design that includes
25 now, let me call it a reset function rather than an

NEAL R. GROSS

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

1 override function --

2 MR. STATTEL: Sure.

3 MEMBER STETKAR: -- will the staff
4 interpret that as not acceptable because I am not
5 allowing the automated safe state to take precedence
6 over everything?

7 MR. EAGLE: This gets involved, by the
8 way, with -- for instance, we know that we have like
9 pumps, valves, things like this. And you have, for
10 instance, like the point 4 controls that the operator
11 has to be able to operate those, operate that
12 particular pump. But that pump may be part of your
13 safety system, in which the automatic system suddenly
14 comes in and says I want that pump turned on to start
15 pumping water.

16 And then, let's say you have had a common
17 cause failure. We could postulate that that suddenly
18 tells that pump to turn on, and it is not really
19 needed. It is a failure. So, we need the operator to
20 be able to override it.

21 And many times they have devices called
22 priority modules that just somewhere sits down here
23 just before that pump, and it has safety signals
24 coming in and it has non-safety signals coming in. Of
25 course, it has that separation or division, but then

NEAL R. GROSS

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

1 that little module makes a decision what to actually
2 send to that pump.

3 And so, this item that you are talking
4 about is particularly involved with trying to address
5 what happens if the safety system has gone bad because
6 of common cause failure and it is telling it to do
7 something. How do you get that overridden by the
8 operator or through, say, a non-safety system?

9 MEMBER STETKAR: Precisely.

10 MR. EAGLE: And this was involved with
11 ISG-04. This is one of their big questions they had
12 that it dealt with.

13 And the way we did it, we simply copied
14 the paragraph that they dealt with it and put it right
15 in here. That was the only way we could see how to
16 deal with it because it had already been examined and
17 worked with by ISG-04. So, that is where this area is
18 coming from.

19 MR. STATTEL: To answer your original
20 question, though, in our reviews the principles we
21 look for in design are that the safety function
22 actuates and goes to completion. Once it is
23 completed, the safety injection pumps are running, the
24 valves are positioned to their safety function, then
25 the operator has the ability to assess the situation,

NEAL R. GROSS

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

1 to determine whether or not that safety function has
2 satisfactorily gone to completion, and that he has the
3 ability to take control of those functions in a
4 conscious manner, right?

5 MEMBER STETKAR: And he can intervene.

6 MR. STATTEL: It is not just an automatic
7 thing. He is making that conscious decision. And it
8 is very procedural-directed. So, we look very closely
9 at those procedures, those emergency operating
10 procedures, and we look very carefully at, you know,
11 that they are not just blindly following that cookbook
12 procedure. The procedure has a step in there to
13 confirm safety function actuation, confirm that the
14 pump has started; he has a positive indication of
15 that, and before he takes that action to override that
16 function.

17 So, I mean, it is very important to
18 review.

19 MEMBER STETKAR: I am glad of that. That
20 helps. That is on the practical side.

21 MR. STATTEL: And this was a direct
22 inspection item that we were looking at for Ocone.

23 MR. EAGLE: I might also point out, in
24 support of that, that if you notice, this last set of
25 bullets right here on our slide would support the

NEAL R. GROSS

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

1 instrumentation that can provide the protective
2 function that is needed, and that the safety-related
3 automatic system did not perform the protective
4 function, and then the fact that the automated diverse
5 system or manual diverse system is able to actually
6 accomplish it. So, I thought that kind of points out
7 the same thing you were saying.

8 MR. STATTEL: Yes.

9 MR. EAGLE: We are at this point where, if
10 you would like to take that break --

11 CHAIRMAN BROWN: Yes, we will take a
12 break. The meeting is paused for 15 minutes. We'll
13 come back at 10:32.

14 (Whereupon, the foregoing matter went off
15 the record at 10:16 a.m. and went back on the record
16 at 10:35 a.m.)

17 CHAIRMAN BROWN: The meeting will
18 reconvene.

19 MR. JUNG: Time check. We have like 38
20 slides and then we are at page 11-12.

21 CHAIRMAN BROWN: Oh, I thought we were up
22 to page 20.

23 MR. JUNG: Oh, okay. Sorry about that.

24 CHAIRMAN BROWN: You'll give those folks
25 a heart attack over there.

NEAL R. GROSS

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

1 MR. EAGLE: We were talking up here.

2 CHAIRMAN BROWN: He was impugning my
3 management capabilities here. I was trying to hold
4 John in check.

5 (Laughter.)

6 Go ahead, Gene.

7 MR. EAGLE: Okay. As mentioned earlier,
8 the nuclear energy representatives presented a list of
9 concerns and questions in the form of seven problem
10 statements. An additional issue that was not in the
11 original problem statement emerged later as a common
12 cause failure issue that should be addressed.

13 So, the seven statements are presented
14 here in the next two slides, and I will not bother to
15 quote them because we are going to go through each of
16 these individually.

17 Problem statement 1 was a clarification of
18 what constitutes adequate diversity. In other words,
19 how much diversity is enough?

20 BTP 7-19 as a whole and NUREG-6303 provide
21 general guidance in this area. An additional document
22 has been developed recently. It is NUREG-7007,
23 "Diversity Strategies for Nuclear Power Plant I&C".
24 Now this document was developed jointly by the NRC
25 Research group and Oak Ridge National Laboratory. It

NEAL R. GROSS

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

1 reports extensive studies of diversity techniques
2 worldwide in many types of industries; suggests an
3 analytical method for numerically evaluating diversity
4 in Appendix A.

5 And while well-received, the method has
6 not had a sufficient, what you call, "test of time"
7 yet. And thus, it was not included in Revision 6.

8 CHAIRMAN BROWN: Is this the one that
9 Waterman presented to us where --

10 MR. EAGLE: Yes.

11 CHAIRMAN BROWN: -- he went through the
12 chart and all the stuff with the numerical
13 quantification, and you come up with this
14 quantification of diversity?

15 MR. EAGLE: Correct. In fact, the famous
16 Waterman Wheel was included in that.

17 CHAIRMAN BROWN: Yes. Okay.

18 MR. EAGLE: Rich, I don't know if he wants
19 to make a comment. Or, Russ, any comments on 7007.

20 CHAIRMAN BROWN: You're not forced to do
21 that. I just wanted to make sure I knew it was the
22 same thing, that it hadn't changed.

23 MR. STATTEL: Yes. So, as a consequence,
24 we don't have, when we are performing our reviews, we
25 don't have any direct review guidance to use that

NEAL R. GROSS

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

1 NUREG. However, we do use it. We do pick it up, and
2 we do run the numbers through that to try to give it
3 some basis.

4 So, for the intent of establishing a test
5 of time, we do intend to continue to use that NUREG
6 during our reviews. We have an upcoming review for
7 Diablo Canyon reactor protective system, and we intend
8 to use that as part of the diversity evaluation. But
9 it is not required, and we don't use those numbers as
10 a basis for our safety conclusions.

11 CHAIRMAN BROWN: Okay. We expressed some
12 ambivalence to a numerical quantification when it was
13 talked about.

14 MR. STATTEL: It would be nice. It would
15 be nice to make it completely objective so that we can
16 just crank it through, come up with a number, and say,
17 if it is higher than this number, it is good; if it is
18 lower than that number, it is not. But,
19 unfortunately, the state of the art isn't to that
20 point yet. So, it does require some subjective
21 analysis.

22 CHAIRMAN BROWN: Okay. Okay, that's fine.
23 We'll go on.

24 MR. EAGLE: Problem statement 2, and
25 probably this is one of the harder areas, is

NEAL R. GROSS

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

1 clarification when operator action is acceptable as an
2 independent and diverse means to prevent or mitigate
3 the potential common cause failure of automated
4 reactor protection functions.

5 Of course, the first thing you must do is
6 perform a D3 analysis of the reactor protection system
7 or any new control system using realistic assumptions.
8 If subject to potential common cause failure, then
9 there is a need for a diverse means to perform the
10 safety function subject to the common cause failure.

11 And notice that the diverse means may be
12 automated or manual. Automated diverse means is
13 preferred. If a manual means is selected as the
14 diverse means, acceptability is based on human factor
15 analysis.

16 The original concept was for a 30-minute
17 hard limit that allowed operator action as part of or
18 all of the diverse means only if the protected action
19 was not required for at least 30 minutes. We have
20 discussed that before. Otherwise, the diverse means
21 was expected to be an automated function.

22 We would like to just comment on this
23 beyond 30 minutes for a moment. Even these beyond-30-
24 minute manual actions would require a demonstration
25 through a suitable human factors engineering analysis

NEAL R. GROSS

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

1 that the manual operator actions would be performed
2 adequately from within the main control room.

3 Once again, if a protective function was
4 normally performed by the manual action, then it was
5 expected that the function or an alternate function
6 would still be performed manually, even in the
7 presence of common cause failure. We had talked a
8 little bit about this earlier.

9 MEMBER STETKAR: Eugene, you just said
10 something that I hung up on because you inserted that
11 key little phrase "within the main control room".

12 MR. EAGLE: Right.

13 MEMBER STETKAR: Let me bring you back to
14 the example that I was using where in the main control
15 room I can push a button that will start emergency
16 feedwater.

17 MR. EAGLE: Right.

18 MEMBER STETKAR: If I don't do anything in
19 the plant, the emergency feedwater system will then
20 proceed to fill the steam generators full of water,
21 putting water over in the main steam lines. And it is
22 not clear to me what happens after that.

23 So, is the human factors engineering
24 analysis for -- and I am not going to hang up on this
25 30 minutes -- is the human factors engineering

NEAL R. GROSS

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

1 analysis performed for the entire function, which is
2 initiation of stable secondary heat removal from the
3 emergency feedwater system, which requires local
4 manual control of the valves, or is it only pushing
5 the button to get the thing started, and you don't
6 care after that?

7 MR. EAGLE: Well, again, that falls into
8 the human factors analysis area.

9 MEMBER STETKAR: Well, but you just orally
10 said, "within the main control room". And we have
11 already established that he can locally control the
12 feedwater system or it could be other functions. I
13 just use emergency feedwater because it is clear that
14 they need to do something within the first several
15 minutes of the event. And if they can't control it
16 from inside the control room, it is clear that they
17 need to control it from outside of the control room.

18 MR. EAGLE: Right.

19 MEMBER STETKAR: So, what I am curious now
20 is, is the human factors engineering requirement, when
21 I submit my D3 analysis, and you review it, am I
22 looking at that entire function, including the ex-
23 control room actions associated with it or do I just
24 put my within-the-main-control-room blinders on.

25 MR. STATTEL: I wouldn't presume to speak

NEAL R. GROSS

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

1 for the HFE group that performs those analyses.
2 However, I have read several of those analyses. And
3 for the cases that I have read, it is really just
4 analyzing the need for the diverse functions and the
5 operator's ability to perform the safety function,
6 initiate the safety function.

7 As far as followthrough on getting the
8 plant to a stable condition, generally, those analyses
9 don't go to that level. But there is other guidance
10 that is under development. I believe there is a
11 Chapter 18 in the SRP that is being revised, and they
12 may deal with those issues, but I wouldn't presume to
13 speak for them.

14 MR. JUNG: John, I think you are getting
15 into --

16 MEMBER STETKAR: I'm getting into, what
17 are we reviewing and what are we expecting the
18 applicant to provide in terms of analyses to justify
19 their design? That's what I'm getting into.

20 MR. JUNG: Okay. All right, well, we will
21 combine that with the HFE, but my understanding is, as
22 part of their EOP/AOP development, they will have to
23 address all the human actions that are relied on to
24 safely operate and mitigate. The plant accidents will
25 have to be addressed by the procedures and operator

NEAL R. GROSS

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

1 training. So, it is one area there is sort of a
2 turnover.

3 But, John, I am just going to mention one
4 scenario that we have been getting into for MHI
5 USAPWR. Steam generator tube rupture is one of the
6 cases I think very relevant to it. Typically,
7 although there are automatic systems available for
8 sort of bounding cases, typically, steam generator
9 tube rupture scenarios are handled manually from the
10 start.

11 So, those cases, this particular emphasis
12 we are doing on BTP 7-19 is those accidents or AOOs
13 are typically handled by the human actions, operator
14 actions, pretty rapidly, and beyond, we expect it to
15 be controlled and displays available as part of the
16 dash panel rather than going out and manipulating
17 valves and coming back and communicating. We don't
18 want to overburden operators to mitigate those
19 accidents.

20 But, sooner or later, when a plant gets
21 stabilized, there might be cases where you need local
22 actions. Our guidance is not going too much into it.

23 MEMBER STETKAR: I understand that, Ian,
24 and that is why I raised the question. Because the
25 guidance has now walked me into a corner where it

NEAL R. GROSS

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

1 says, to have an acceptable design for D3 mitigation,
2 all I need to show is that the operators have adequate
3 alarms in the control room and have adequate time,
4 have adequate guidance to walk up to a panel, push a
5 button, and get things started.

6 And therefore, the design is then
7 acceptable. Even though the fact that that design is
8 now putting too much water in places where I don't
9 want that water --

10 MR. STATTEL: Let me point out that the
11 primary purpose of this is to deal with the software
12 or digital system common cause failures. I mean, that
13 is really the scope of this particular guide.

14 MEMBER STETKAR: I understand that.

15 MR. STATTEL: So, those systems, the
16 safety systems for which you are establishing that
17 diversity don't perform those followup actions.

18 MEMBER STETKAR: The safety systems in
19 integrated designs do control feedwater flow. They
20 look at steam generator levels, and they actively
21 control the emergency feedwater control valves.

22 MR. STATTEL: Okay.

23 MEMBER STETKAR: So, they do perform those
24 functions in some designs that I have seen --

25 MR. STATTEL: Okay.

NEAL R. GROSS

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

1 MEMBER STETKAR: -- many of the new ones.
2 They do perform, maintain steam-generator-level
3 function.

4 MR. STATTEL: Well, if those are safety
5 functions for which diversity would be required, then
6 I would imagine they would also, that functionality --

7 MEMBER STETKAR: But everything I read in
8 here, and from what I just heard, says I can perform
9 the followup actions for control outside of the
10 control room.

11 MR. STATTEL: Okay.

12 MEMBER STETKAR: In a new plant design, I
13 have four divisions. They are located in four
14 geographically-diverse parts of the plant. So, I
15 can't do this with one guy standing next to four
16 valves. I need four separate operators to go out and
17 locally manually control four separate valves to
18 prevent overfeeding the steam generators --

19 MR. EAGLE: But this is one of the reasons
20 that we --

21 MEMBER STETKAR: -- to accomplish the same
22 function that is accomplished by the integrated,
23 normal protection system. You're telling me that I
24 don't need to look, when I perform my D3 analysis for
25 diversity for that function, that I don't need to look

NEAL R. GROSS

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

1 at the human factors engineering for the operators
2 going out in the plant and controlling those valves.
3 That's what I interpret what you said.

4 MR. STATTEL: I guess I am not getting the
5 integrated perspective because all of the systems that
6 I have reviewed, the ability of the operator to
7 complete those functions is not affected by a common
8 cause failure of a digital system, right?

9 MEMBER STETKAR: If the normal system, the
10 normal protection system --

11 MR. STATTEL: Right.

12 MEMBER STETKAR: -- starts the pumps,
13 looks at steam generator levels, and throttles the
14 control valves to maintain level. That's what it
15 does.

16 MR. STATTEL: Yes.

17 MEMBER STETKAR: It does all of that. So,
18 if the operators don't do anything and the system
19 works fine, I have emergency feedwater controlling
20 level in all four steam generators perfectly.

21 Now, if a common cause failure occurs, and
22 that system doesn't do anything, now we need to get
23 emergency feedwater to the steam generators.

24 MR. STATTEL: There would be a diverse
25 system to actuate that.

NEAL R. GROSS

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

1 MR. EAGLE: Exactly, and it would be doing
2 the same, it is to do the replacement function.

3 MR. STATTEL: Right.

4 MEMBER STETKAR: Okay, but you are telling
5 me that all I need to do is start the flow; I don't
6 need to control the valves --

7 MR. EAGLE: We never said that.

8 MEMBER STETKAR: -- and my D3 analysis
9 doesn't have to show -- see, where I'm getting to is
10 you say that those follow-on functions can be
11 performed locally in the plant.

12 MR. EAGLE: We didn't say that.

13 MEMBER STETKAR: Yes, you did.

14 MR. EAGLE: No, we said that --

15 MEMBER STETKAR: I walked you into the
16 corner about two hours ago that said --

17 MR. EAGLE: No, we said that there may
18 come a point where you may need to be able to perform
19 certain functions outside the control room. In other
20 words, we have also continued to emphasize that
21 instrumentation would be in the control room.

22 MEMBER STETKAR: Oh, my God, the steam
23 generators are getting too full. I don't have enough
24 people and I can't get to the places to control
25 levels. I know that I'm in trouble.

NEAL R. GROSS

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

1 MR. EAGLE: Okay. Well, you mentioned
2 that the automatic systems, part of it is to control
3 the levels. Okay. If that automatic system has been
4 lost due to a common cause failure, you need to
5 provide a diverse means. That diverse means needs to
6 replace that function. And whatever that function
7 needed to do, that diverse mean would need to take
8 care of it. And it should have the controls in the
9 control room to be able to do that. If you are going
10 to be able to use it manually or if you choose an
11 automated system, it should be able to complete it.

12 It says very clearly it has to be able to
13 complete the same function. That is the whole idea of
14 a diverse --

15 MEMBER STETKAR: Well, the reason I asked
16 the question earlier was in point 4 it says, "Once
17 manual actuation from the main control room using the
18 point 4 displays and controls has been completed,
19 controls outside the main control room for long-term
20 management of these plant-critical safety functions
21 may be used when supported by suitable HFE analysis
22 and site-specific procedures or instructions." That's
23 what it says.

24 MR. EAGLE: Right.

25 MEMBER STETKAR: And I asked you, on that

1 point, does that apply for things like emergency
2 feedwater actuation where they need to go out and
3 locally control the feedwater valves, and the answer
4 was, yes, they could do that locally. And I can
5 accept that.

6 MR. EAGLE: If they needed to. It does
7 not stop -- however, point 4 clearly says that point
8 4 instruments and controls are from the control room.
9 That's right directly out of the policy.

10 And we also pointed out, just emphasizing
11 there may come a point where you may need to go out
12 and do things outside.

13 MEMBER STETKAR: Let me ask you, I
14 guess -- we may not be communicating very well -- is
15 the following design acceptable: the operator can
16 manually initiate each division. Let's say you only
17 need one division. So, he can manually start
18 emergency feedwater flow by pushing a button in the
19 main control room on the diverse actuation panel with
20 no control of feedwater flow, no automatic control of
21 feedwater flow and no manual control of feedwater flow
22 from the main control room. Is that design okay?

23 MR. STATTEL: Yes, it is.

24 MR. EAGLE: Well, that was a diverse
25 system.

1 MEMBER STETKAR: Now, in the human factors
2 engineering part of that design, it is clear that I
3 need to justify the ability that the operators have
4 sufficient instrumentation and time, and things like
5 that, to walk up to the panel and push the button to
6 get it started. That is really clear to me.

7 What's not clear, and what I thought --
8 and I'm learning more -- what's not clear is whether
9 or not that human factors engineering part of that
10 diverse system design also extends out to include the
11 manual local actions that are required to fully
12 implement that function in the plant.

13 And that is why I am kind of hanging up on
14 it. Because if the design to get it started --

15 MR. STATTEL: But there are different
16 types and there is more than one HFE analysis that is
17 required to support plant operations. When I look at
18 BTP 19 and the scope of BTP, which is really dealing
19 with software or digital system common cause failures,
20 we are really concentrating on the effect of those
21 failures and the ability for the operators to cope
22 with those effects, right?

23 Now, going to your example, I have worked
24 at Calvert Cliffs. They had exactly the system you
25 are talking about. They have an aux feed initiation,

NEAL R. GROSS

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

1 and it doesn't control level at all. There is no
2 level-control algorithm in that at all. It initiates,
3 and then, at some point the operator has to scale back
4 the flow in order to keep the generator from
5 overfilling.

6 Now, in their case -- and a lot of this is
7 very design-specific -- in their case, they have
8 procedures where they can take manual control of the
9 aux feed valves and throttle them back from the remote
10 shutdown panel in that area. And it is done with
11 pneumatic valves, right? It is not using any digital
12 system at all.

13 Now the operator's ability to perform that
14 function is not something I would be looking for from
15 a D3, from a software common cause failure
16 perspective. In that particular design, I would be
17 looking to see that there is a diverse means of
18 initiating aux feedwater flow.

19 As far as the operator's ability to follow
20 up with that, I believe that is a separate analysis
21 normally. It could be the same analysis. But,
22 oftentimes, there are multiple analyses that go into
23 supporting the operations of the plant.

24 MEMBER STETKAR: I think, in the interest
25 of time, and I know we should keep moving, but I need

NEAL R. GROSS

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

1 to think much more about that.

2 MR. EAGLE: Let me summarize here. Keep
3 in mind that we are talking about, if you have an
4 automatic system and it fails due to common cause
5 failure, you need to have a diverse system that can
6 replace that function. And whatever that function was
7 doing, it would need diverse means to be able to
8 replace that.

9 Now you might choose to have part of it
10 automatic and part of it manual.

11 MEMBER STETKAR: Yes.

12 MR. EAGLE: That is one of the key things.

13 Remember, also, point 4, remember, is a
14 set of controls and instrumentation that is completely
15 independent of the reactor protection system. So, now
16 if part of your analysis and the things is that, okay,
17 we've got this system that fails, and now we have to
18 push some buttons on it, and part of the analysis
19 might be that part of that function is now being able
20 to control it. Remember, you have your point-4-type
21 controls that are independent of that automatic
22 system. And they are not failed. They are diverse
23 and independent from the automatic system.

24 And, remember, what we are trying to do is
25 replace that automatic system that has gone down, and

NEAL R. GROSS

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

1 we assume it is completely out of that; even though
2 maybe only a portion of it failed, we assume for the
3 moment that the whole thing fails. And whatever part
4 of it fails or whatever function we can't accomplish,
5 we have to have a diverse means. That is what BTP
6 7-17 is dealing with.

7 MEMBER STETKAR: I understand all of that.
8 But I also understand that, as an applicant, I must
9 perform a D3 analysis --

10 MR. EAGLE: Right.

11 MEMBER STETKAR: -- and submit it to the
12 staff. And the staff needs to review that analysis
13 and make a determination about the adequacy of the
14 diverse protection system design --

15 MR. EAGLE: Right.

16 MEMBER STETKAR: -- to mitigate those
17 postulated common cause failures.

18 I understand all of that. Where, quite
19 frankly, I am hanging up is the proposed diverse
20 design says all I need is a button in the main control
21 room to push to start the pump because I am not
22 required in my D3 analysis to look at human factors
23 engineering of any ex-control room operator actions.
24 And if the staff during their review says that the
25 guidance --

NEAL R. GROSS

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

1 MR. EAGLE: I don't think there is
2 anything saying that.

3 MEMBER STETKAR: -- doesn't require that,
4 then I never examine whether or not it would be, I'll
5 use the word prudent, to have manual control of those
6 valves on the panel in the control room versus out in
7 the plant.

8 And the staff will never ask them about
9 that.

10 MR. STATTEL: But if you throw the digital
11 aspects of that out, I guess my question, really more
12 for the HFE folks, would be, what mechanism do you use
13 to require that analysis, even in an analog system, I
14 mean with no diverse system at all, right?

15 MR. JUNG: Rich, let me.

16 John, I think this might help. If you
17 look at the ISG-05 which is being converted into
18 Chapter 18, if you look at the ISG-05, what it says is
19 for diversity and defense-in-depth, if you are relying
20 on manual operator action to meet the acceptance
21 criteria of BTP 7-19, which refers to eventually
22 radiological consequences of Part 100 for PAs or AOs,
23 it specifically requires a very detailed systematic
24 analysis. And then, recognizing the need to develop
25 detailed plant procedures, AOPs, EOPs, and even severe

NEAL R. GROSS

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

1 accident management guidelines, it is an iterative
2 process.

3 So, they will go through life-cycle
4 development of the HFE. They have to continuously
5 evaluate the requirements.

6 So, the answer to your question are some
7 of these manual actions for short-term and long-term,
8 are they covered by HFE, the answer is yes. And that
9 is why we have so much struggling because, at least
10 for new reactors, the requirements are clear. But are
11 you going to see that, the details now? The answer is
12 no. That is why HFE life cycle has to go through the
13 ITAAC process to confirm that.

14 I think, eventually, you will see those
15 cases. But I think you are going, also, into some
16 areas where it may not be specific to D3 itself. It
17 might be the question of all the details, the long-
18 term human actions. Is there human factors
19 engineering to be applied? That is the even more
20 general question.

21 If you want me to bring somebody from HFE
22 to confirm that --

23 MEMBER STETKAR: No, I don't. No, I don't
24 particularly care about HFE. I care about guidance
25 that narrows the scope of a review down to something

NEAL R. GROSS

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

1 that is very explicit that can be referred to by
2 applicants and by staff reviewers to exclude
3 evaluations of required functions. That is what I am
4 concerned about, quite frankly.

5 MR. JUNG: I don't think that is the
6 intention.

7 MEMBER STETKAR: I hope it is not the
8 intent, but I see it creeping in that direction here.

9 MR. EAGLE: I think it is quite clear that
10 the BTP 7-19 is simply saying that, if you have a
11 failed automatic system, you have to provide a diverse
12 means. Now you can choose to do that diverse means,
13 and diverse mean is to replace that automatic
14 function. That diverse means can be automatic or
15 manual, or it may be a combination.

16 It doesn't say anything about only one
17 button or being pushed or things like that. It says,
18 if you choose the manual, then you have to justify it
19 by human factors analysis, and that's it. That's the
20 bottom line. There's no more details that you would
21 be provided.

22 The analysis then shifts over to the like
23 ISG-05 or the Appendix 18-A.

24 CHAIRMAN BROWN: Can I make just one
25 observation? Because I have been through this, but I

NEAL R. GROSS

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

1 wanted to hear all the dialog.

2 If you go to your BTP 7-19, the writeup on
3 concerning point 4, the clarification, and I'm using
4 this similar to what you just told me when I was
5 questioning the independence thing. Okay. And I've
6 found that.

7 In the concerning point 4, you state, "The
8 separate set of displays and controls are for manual
9 system-level or division-level, depending on the
10 design, actuation and control of equipment to manage
11 the plant-critical safety functions. See B-1.2
12 above."

13 That is one statement that says I have got
14 to manage the plant-critical safety functions.

15 MEMBER STETKAR: Right.

16 CHAIRMAN BROWN: Then, the last paragraph
17 states, "Once manual actuation from the MCR using
18 point 4 displays has been completed, controls outside
19 the MCR for long-term management of these plant-
20 critical safety functions may be used when supported
21 by suitable HFE analysis and site-specific...."

22 MEMBER STETKAR: So, that, to me, sounded
23 good. But when I asked them about what the scope of
24 the HFE analysis that would be reviewed, that's why I
25 hung up; they said "within the main control room".

NEAL R. GROSS

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

1 CHAIRMAN BROWN: Yes, I know, but that's
2 not -- I agree with you. That's why I went back to
3 re-read this, and it looks like that was not a good
4 statement.

5 MEMBER STETKAR: I hope that was simply a
6 misstatement, although there seems to be --

7 MR. EAGLE: We want to make it quite clear
8 that you need to have controls in the main control
9 room for carrying on things. It doesn't necessarily
10 mean you can't use other controls outside, but we need
11 to have controls right there in front of the operator
12 to handle everything, basically, as much as possible.

13 CHAIRMAN BROWN: Yes, but this says very
14 clearly you can use stuff outside as long as you have
15 done an analysis that shows that the operator actions
16 outside the main control room can manage the plant-
17 critical functions.

18 MR. STATTEL: I did not mean to imply that
19 the need for performing --

20 CHAIRMAN BROWN: And you said, "No, we
21 stopped with the MCR push button." And I think that
22 is what we hung up on.

23 MEMBER BLEY: Rich, could you say that
24 again? I couldn't hear.

25 CHAIRMAN BROWN: I'm sorry.

NEAL R. GROSS

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

1 MR. STATTEL: When I made the statement,
2 I did not mean to imply that the need to perform the
3 required HFE reviews for those operator actions would
4 be obviated based on the fact that it is not in the
5 scope of this BTP, right?

6 So, like when you refer to these manual
7 operator actions that are not related to a digital
8 system, I mean the scope here is clearly a computer
9 system, right? It is in the title of the BTP.

10 So, if that was the case, then they could
11 simply not use a computer system and, therefore, not
12 require an HFE analysis. All we're saying here is
13 that, if you are creating this diverse means and you
14 are relying on a manual operator action, the
15 assessment of the ability of the operators to complete
16 that action in the required time needs to be
17 considered.

18 The follow-on actions, those are separate
19 requirements. They are not initiated by performing
20 the D3 analysis.

21 MR. EAGLE: Another thing is that we have
22 got two things here. We have tried to emphasize that
23 point 3 says that you will provide a diverse function
24 to replace an automatic function. That's it.

25 Now we go to point 4. That is a whole

1 separate thing. That is your main controls the
2 operator uses to start all those pumps and everything,
3 and that's covered by point 4.

4 We said that some of your diverse systems,
5 part of the point 4 controls, you may be taking credit
6 for them as the diverse system. So, remember, you
7 have these regular standard controls that you're
8 operating on that are called for by point 4 that are
9 independent and diverse from your safety system. And
10 these things, when you use these or operate them, they
11 are from the control room, but there may come a time
12 when the operators need to use something outside. And
13 that is why that particular came -- but keep in mind,
14 that doesn't necessarily mean that we are talking
15 about the diverse system at this point.

16 CHAIRMAN BROWN: Okay. Well, I am going
17 to take management action right here on managing this
18 meeting for a second here. We are going to have to
19 start moving on a little bit.

20 MR. EAGLE: Okay, we will go ahead then.

21 CHAIRMAN BROWN: And we will ruminate on
22 what you have --

23 MR. EAGLE: Okay. Keep in mind that a lot
24 of times these things try to keep a general picture,
25 and they can't go into an excessive amount of details.

NEAL R. GROSS

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

1 Anyway, we were talking about the
2 stakeholders. We got into our first one, and we were
3 into the second one.

4 We talked about the fact we had a 30-
5 minute hard limit for a while, and that limit began to
6 be changed and ended up in the final version. The
7 final version is where it appears that BTP 7, Revision
8 6, is simply, it does allow both manual and automatic
9 systems. You can make a choice. The automatic is
10 preferred.

11 And if you chose for the diverse system to
12 be part or all manual, then you need to perform a
13 human factors analysis. And this is carried on as
14 directed to Appendix 18-A, which ISG-05 has been
15 rolled into a document called SRP, Chapter 18,
16 Appendix 18-A.

17 At this time, it has not been issued, but
18 it is going to be issued. But there has been some
19 delays due to priorities.

20 CHAIRMAN BROWN: Are we going to see that?

21 MR. EAGLE: What?

22 CHAIRMAN BROWN: Are we going to see that?

23 MR. EAGLE: You've already seen Appendix
24 18-A.

25 MEMBER BLEY: Well, we've seen the BTP.

NEAL R. GROSS

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

1 MR. JUNG: Yes, according to the SRP
2 update, the process, I am sure Christina is going to
3 be notified for an opportunity to consider HRS --

4 CHAIRMAN BROWN: Okay. I had asked that
5 question once before on 18-A.

6 MR. EAGLE: Yes, but you have already seen
7 it, I understand.

8 MEMBER BLEY: I think we saw ISG-05.

9 CHAIRMAN BROWN: We saw ISG-05.

10 MR. EAGLE: ISG-05. Okay. I'm sorry.

11 CHAIRMAN BROWN: But we have not seen how
12 it was really wrapped into an appendix yet.

13 MEMBER BLEY: Maybe it has been changed
14 somehow, which happens occasionally.

15 CHAIRMAN BROWN: I don't want to mouse-
16 milk this. I just wanted to make sure that we had an
17 opportunity, as a Subcommittee, to see this and
18 determine what path we wanted to take.

19 MR. JUNG: Charlie, I will take an action
20 to the HFE group to work with Christina on the status
21 and their intent.

22 CHAIRMAN BROWN: Okay. Yes, I would
23 appreciate that.

24 MR. EAGLE: Yes, we would like to get the
25 priority pushed up on that.

NEAL R. GROSS

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

1 MEMBER BLEY: I do want to say, though,
2 that I am glad in these various documents you have
3 adopted the approach you have taken here in referring
4 to that one and requiring an analysis rather than some
5 arbitrary time limit. Some things are easier to do in
6 one minute than others are in 30. So, an arbitrary
7 time limit just didn't make sense. This is good -- if
8 we like 18-A.

9 MEMBER SIEBER: Continuous control
10 operation like regulating feedwater requires
11 individual attention constantly from an operator.
12 When you have four steam generators, it is very
13 difficult for one operator to control level in four
14 steam generators.

15 I don't think you have diversity amongst
16 the feedwater control systems. And so, if you have a
17 failure in one, what's the chances of having in all
18 four?

19 And I know that, since I have tried this,
20 you just can't do it without cycling the pumps, and
21 you aren't going to do that very often.

22 MR. STATTEL: That's true. And that would
23 be something that would be taken into consideration on
24 the HFE analysis, the ability of the operator to
25 perform that function.

NEAL R. GROSS

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

1 MEMBER SIEBER: Yes, well, let's hope the
2 HFE analysis is good enough to take into account what
3 the real demand on the operator is because you don't
4 typically staff the control room to be able to do that
5 kind of a manual operation. It takes extra people to
6 do it. You know, you have two operators. They are
7 going to be busy if some big event is going on.

8 MR. EAGLE: One final thing is that we did
9 go back and add a very special note to dealing with
10 the diverse means. We would like to go into that note
11 now.

12 The first thing to have a better
13 understanding is the terms time available and time
14 required. The time available, just to restate our
15 understanding, is that time available can be
16 considered as the period between when an automatic
17 safety system fails to actuate, when the actuation
18 should have occurred, due to common cause failure, and
19 the time when a substitute actuated system or safety
20 function must be performed. In other words, this must
21 be performed when you are really getting into serious
22 problems.

23 And the time required can be considered as
24 the time required for a licensed reactor operator to
25 recognize a failure due to a common cause failure,

1 determine actions needed, and then accomplish the
2 needed safety function, including recovery from any
3 operator error.

4 And this was the note that was placed in
5 there to provide particular emphasis in looking at
6 these 30 minutes or less or looking at human factors
7 or looking at whether you need an automatic system.

8 As the difference between time available
9 and time required decreases, there can be increasing
10 uncertainty in the estimate of time required for
11 operator action. The uncertainty could invalidate a
12 conclusion that the operators can perform the action
13 reliably within the time available. For actions with
14 a limited margin of time to act, such as less than 30
15 minutes between the time available and the time
16 required, a more focused staff review will be
17 performed.

18 And this is the note that was included in
19 BTP 7-19, Rev. 6, to try to give a little extra
20 emphasis.

21 CHAIRMAN BROWN: This is largely a fallout
22 of, I mean, we wrote a letter where we proposed all
23 this.

24 MEMBER STETKAR: I've got a very specific
25 comment on this.

1 CHAIRMAN BROWN: Yes.

2 MEMBER STETKAR: The first sentence says,
3 "As the difference between the time available and time
4 required decreases, there can be increasing
5 uncertainty in the estimate of the time required for
6 operator action."

7 The uncertainty in the time required for
8 operator action does not depend at all on the
9 difference between the time available and the time
10 required. How long is required for me to pick up this
11 coffee cup and bring it to my lips does not depend
12 upon anything in terms of the time available to do
13 that.

14 Now why am I hanging up on this point?
15 The reason I am hanging up on this point is that this
16 focuses strictly on the time required for a person to
17 perform a particular action. It says that, when I
18 have a small margin, I can have increased uncertainty
19 in that parameter. That's not true. The uncertainty
20 in that parameter is whatever it was.

21 In application, what people will do is
22 they will focus entirely on that parameter because the
23 Branch Technical Position focuses on that parameter.
24 And you will see time/motion studies saying my thermal
25 hydraulics analysis says I have 37.26 minutes to do

NEAL R. GROSS

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

1 this. And, lo and behold, I have done these
2 time/motion studies, and I can accomplish this with an
3 error of plus or minus five minutes within 18.275
4 minutes, not recognizing that there might be
5 uncertainty of about 15 minutes, plus or minus, in the
6 37-minute time available.

7 I guarantee you that people will focus
8 only on the time required and not uncertainties in the
9 time available.

10 MR. STATTEL: I guess I am not
11 understanding the question.

12 MEMBER STETKAR: You're not, which it is
13 fairly clear from the phrase in that note.

14 MR. STATTEL: I mean, if the difference
15 is --

16 MEMBER STETKAR: Let me read you
17 something.

18 MR. STATTEL: -- 30 seconds between time
19 available and time required, you are telling me there
20 is no difference in uncertainty than if there were
21 five minutes?

22 MEMBER STETKAR: Suppose that --

23 MR. STATTEL: I have more confidence that
24 the operator will be able to perform that action in
25 the required time.

NEAL R. GROSS

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

1 MEMBER STETKAR: Richard, suppose that the
2 nominal scenario that I ran, my thermal hydraulics
3 analysis, said there's 15 minutes available.

4 MR. STATTEL: Okay.

5 MEMBER STETKAR: But if I look at the
6 range of scenarios and uncertainties, I might have 15
7 minutes plus or minus 10. I could have as small as
8 five and as large as twenty-five. That is probably
9 large uncertainty, but I will use that as an example.

10 MR. STATTEL: Okay.

11 MEMBER STETKAR: If I use the 15 minutes
12 as my target, and now do a very detailed analysis to
13 say that I have high confidence that I can do it
14 within that 15 minutes, I am not addressing all of the
15 uncertainties.

16 MR. STATTEL: I guess where our
17 differences are are where you apply uncertainties. To
18 me, the certainty is a confidence level that the
19 operator will perform within the required time, within
20 the 15 minutes. That's the way I'm thinking.

21 What you're thinking is the uncertainty is
22 what is actually required.

23 MEMBER STETKAR: The uncertainty is, can
24 the operator perform what is required within the
25 context of the scenario --

NEAL R. GROSS

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

1 MR. STATTEL: Right.

2 MEMBER STETKAR: -- that demands that
3 action?

4 MR. STATTEL: Okay.

5 MEMBER STETKAR: Okay? And there are two
6 parts of the uncertainty.

7 Now let me read something. I would just
8 like to read this into the record. You guys can read
9 the transcript. It keeps the same intent, I believe,
10 but defocuses the one parameter. And as I read
11 through this -- let me just read a proposal.

12 "As the difference between time available
13 and time required for operator action decreases,
14 uncertainties in the estimates for both of these times
15 must be evaluated carefully. These uncertainties
16 could invalidate a conclusion that operators can
17 perform the action reliably within the time available.
18 For actions with limited margin, such as less than 30
19 minutes between time available and time required, a
20 more focused staff review will be performed."

21 Now what I read says there are
22 uncertainties in both of those parameters, and you
23 need to be aware of both of those levels of
24 uncertainty and be careful about both of them as the
25 margin decreases, which I think is the intent, the

NEAL R. GROSS

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

1 fundamental intent of our comments in our letter.

2 The only reason I bring this up is I don't
3 want either applicants or the staff to focus solely on
4 detailed time/motion studies of the time required to
5 perform a particular action and ignore the possible
6 uncertainties and the fact that the time available for
7 that action could also have large uncertainty in it.

8 MR. EAGLE: But I think the time available
9 comes much closer to being a constant. In other
10 words, you establish first the time available because
11 this is the time between when an automatic function
12 should have operated and, all of a sudden, you've got
13 serious problems. And I think you really need to
14 define that first.

15 There may be some uncertainty in that, but
16 it is much closer to being a constant once you have
17 done your studies or looked at it. And then, it is
18 the operators where probably the greater uncertainty
19 may be located. Because we notice here, we mention
20 the fact that it has got to cover a number of things
21 here that may be not quite pinned down as much,
22 including, for example, what happens if the operator
23 made an error. He first has to recognize that he has
24 a problem. And if we assume that the common cause
25 failure has taken out a lot of his instrumentation, it

NEAL R. GROSS

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

1 may be a moment before he recognizes that.

2 Then, he has to determine his actions, and
3 he may be under pressure. There may be mistakes made.
4 And so, this is, to me, really where the real
5 uncertainty is.

6 I think if you look at the percentage of
7 uncertainties in the two different items, it would be,
8 seriously, the larger and the most significant
9 uncertainty would be in the time required. Because,
10 basically, the time available is going to be kind of
11 like almost defined as a constant once you have looked
12 at it.

13 MEMBER BLEY: Dr. Stetkar challenged your
14 assumption about that, and I agree with him because
15 the time available depends on the exact scenario you
16 were going through. Some of them have shorter times;
17 some have much longer.

18 MR. EAGLE: That's true.

19 MEMBER BLEY: So, all he is saying is you
20 need to warn people to be careful about potential
21 uncertainties in the time available, and I certainly
22 agree with him.

23 MR. STATTEL: I understand your point and
24 it is well-taken. I think there is a poor choice of
25 words here, honestly.

NEAL R. GROSS

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

1 MEMBER STETKAR: I think that the sense --

2 MR. STATTEL: Our objective -- I just want
3 to articulate this -- our objective was really to
4 establish a means of getting to a reasonable assurance
5 determination. That was our objective.

6 I think there was a poor choice of words
7 there, in fact.

8 MEMBER STETKAR: I think the intent is
9 really clear. And I actually like the intent. It is
10 simply thinking ahead about where people, both
11 applicants and reviewers, will focus their effort. I
12 believe that the words could be revised a bit to kind
13 of head off a possible too much of a focus in one area
14 without at least some sort of acknowledgment in the
15 other area.

16 MR. STATTEL: Understood.

17 MEMBER STETKAR: And again, it is
18 especially important when those margins start to get
19 fairly small. But that is exactly where people are
20 going to be doing the more in-depth analyses. It is
21 exactly where the staff is going to be putting more
22 effort and time into their reviews and asking a lot
23 more questions. So, those are the areas where we want
24 to be pretty careful to --

25 DR. HECHT: Isn't this really like just a

1 stress strength analysis where you have uncertainty --

2 MR. EAGLE: Yes, it is the same thing.

3 DR. HECHT: -- on the stress. And so, if
4 you have uncertainty on the time available, and you
5 have uncertainty on the time required, Gene, I think
6 you feel that the uncertainty on the time available is
7 much less, but you can still put some kind of a sigma
8 on that. And then, you can just use that same
9 equation for margin of safety.

10 MR. EAGLE: But, again, I would like to
11 point out, going back to it, that you are establishing
12 the time available. It is true certain areas will be
13 different times available. But that has to be
14 established first as the time available. And that,
15 basically, is, when do we get into real serious
16 problems? And obviously, there would be a little bit
17 of plus and minus, but I think that margin of
18 uncertainty will be fairly small --

19 MEMBER BLEY: That's what we are
20 disagreeing with. You're saying the same thing. We
21 disagree with your point on that one.

22 MEMBER STETKAR: Yes, we have seen from
23 some of the PRA things that we have done that, when
24 you depart from the specific design-basis accident
25 scenario and ask questions about, well, these other

NEAL R. GROSS

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

1 conditions could be occurring, they are not considered
2 in part of the design-basis accident because you have
3 had to consider a simultaneous loss of offsite power.
4 You have had to consider the specific power level.
5 You have to consider very many things that precisely
6 determine that scenario.

7 When you get a little bit away from that,
8 some of the times in terms of the time available, some
9 of the rates at which levels change, can be affected
10 by those assumptions. And indeed, for some types of
11 scenarios, those uncertainties may be rather small;
12 for other types of stylized scenarios, they might be
13 actually fairly large compared to estimated operator
14 response times.

15 MR. STATTEL: I think what is on a sliding
16 scale is not the degree of uncertainty. That can be
17 established. What is on a sliding scale would be the
18 degree or level of assurance that you have that the
19 operator --

20 MEMBER STETKAR: Of that margin, that's
21 it.

22 MR. STATTEL: Uh-hum.

23 MR. JUNG: John, I think your points are
24 well-taken. We will --

25 MEMBER STETKAR: Read the quote that I

NEAL R. GROSS

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

1 have put in the record.

2 MR. JUNG: We agree with the sentence,
3 that sentence is not --

4 MEMBER STETKAR: I don't think it changes
5 the intent at all. It just may refocus some of the
6 efforts, both on the part of the applicant and in
7 terms of the review.

8 MR. JUNG: If you look at this note, you
9 know, the time available, the time required, manual
10 action, all that is actually human factors engineering
11 evaluation; that is covered.

12 The way I look at it is a more focused
13 review. Remember, we are in a BTP 7-19 digital I&C
14 design review. What we are saying is those manual
15 actions are relied on. Human Factors will do all the
16 margin analysis.

17 In addition to that, digital I&C, in
18 general, is going to make sure those systems that are
19 being relied on, manual controls and all of that, we
20 are going to do a more focused review to make sure
21 those improvements relied upon are really a good
22 quality and meet independence and all that. That was
23 the main intention here.

24 And then, there is a human factors
25 engineering piece it has to meet in 18-A.

NEAL R. GROSS

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

1 MR. STATTEL: Right. Without putting a
2 number to it. Because once you put a number to it, as
3 you stated, I mean, the actions can be complex and
4 they can take longer than --

5 CHAIRMAN BROWN: When we discussed this in
6 our report on 1.62, Reg Guide 1.62, and we mentioned
7 this time available as the time gets shorter, the
8 difference gets shorter, we didn't get into defining
9 the nuances of time available and time required in
10 other than a conceptual manner.

11 And I believe it was cranked into, it is
12 in 1.62 now, as it was issued, if I remember
13 correctly. This roughly follows with some additional
14 definition that has now been applied, which raises
15 some questions.

16 We ought to try to get this resolved
17 before 7-19 goes out, is all the point I would like to
18 make on this. However we come out, I think we would
19 like to see something before, how we resolve this one
20 way or the other.

21 MR. EAGLE: By the way, we didn't include
22 these definitions in there, partly because they are
23 covered elsewhere.

24 CHAIRMAN BROWN: Oh, I know. Well, I
25 presume they are going to be in 18-A --

1 MR. EAGLE: Yes.

2 CHAIRMAN BROWN: -- if I'm not mistaken,
3 which we will then see.

4 So, you're right -- well, we will have to
5 make a decision on how we go on that.

6 MR. EAGLE: Yes, the note is in there, but
7 not the definition.

8 CHAIRMAN BROWN: I understand that. Yes,
9 I read --

10 MR. EAGLE: It would depend on that kind
11 of vagueness that you, the rough understanding --

12 CHAIRMAN BROWN: Okay. Move on. Okay.

13 MR. EAGLE: Point 3, problem statement 3,
14 was a clarification on component-level versus system-
15 level. This goes back into some of the things we have
16 been talking about. The diverse means is performed in
17 a system-level basis for each division to retain the
18 policy in the SRM, SECY 93-087. It does not prohibit
19 the use of manual controls operating individual safety
20 components after the safety system functions have
21 actuated.

22 A potential for common cause failure in
23 digital safety systems should be considered in new
24 plants as well as in upgrades to existing plants.
25 However, there is no intent to have a backfit of

NEAL R. GROSS

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

1 current nuclear power plants at this time.

2 Point 4, set of controls and displays,
3 safety or non-safety. They list plant-critical safety
4 functions. And if credited, here again, if credited
5 as a diverse means, it should function downstream of
6 any common-cause-failure-affected components.

7 Problem statement 4 was a clarification on
8 the consideration of effects of common cause failure
9 on protective functions from fail to actuate and
10 spurious actuations. In general, spurious actuation
11 is a lesser safety concern than failure to actuate
12 because spurious actuations are usually annunciated
13 and, thereby, immediately detected.

14 Spurious actuations of safety-related
15 digital protection systems resulting from common cause
16 failure do not need to be addressed beyond what is
17 already set forth in plant design-basis evaluations.
18 The design of diverse automated or diverse manual
19 means should address how to minimize the potential for
20 spurious actuations of the reactor protection system
21 caused by the diverse means.

22 MEMBER STETKAR: I need to weigh-in here
23 again. What technical basis do you have for the
24 statement that says, "Spurious actuation is a lesser
25 safety concern than failure to actuate"?

NEAL R. GROSS

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

1 MR. EAGLE: Okay.

2 MEMBER STETKAR: What analyses have you
3 performed to justify that statement? Because it
4 appears in a couple of places in the Branch Technical
5 Position.

6 MR. EAGLE: Okay.

7 MEMBER STETKAR: So, if you can give me a
8 reference, I will go read those.

9 MR. EAGLE: I can't give you a reference
10 right now.

11 MEMBER STETKAR: I would like one, if you
12 have one.

13 MR. EAGLE: Basically, the concept is that
14 spurious actuation will be noticed and action can be
15 taken.

16 MEMBER STETKAR: We have both
17 deterministic and probabilistic regulatory guidance
18 for fire analysis that spends a lot of effort looking
19 at the effects of multiple spurious actuations. They
20 are called multiple spurious operations in that
21 context.

22 That regulatory guidance explicitly states
23 that there is no limit on the number of multiple
24 spurious operations that must be evaluated and that
25 the designs of those protection systems or alternate

NEAL R. GROSS

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

1 mitigation functions, however you want to characterize
2 them, must explicitly account for those multiple
3 spurious operations without regard to whatever
4 analyses have been done in the deterministic accident
5 analyses.

6 So, I'm curious how these statements
7 saying that, for a common cause failure -- by the way,
8 fires, for the record, are also considered to be
9 beyond-design-basis events. So, I am working in the
10 same space here.

11 I'm curious how this guidance under BTP
12 7-19 is consistent with the guidance that we have for
13 both deterministic and probabilistic evaluation of
14 fires in a nuclear plant.

15 MR. STATTEL: Well, these positions were
16 established as part of a Working Group 2, ISG-02,
17 development process, as you are aware.

18 MEMBER STETKAR: Yes. And I think we
19 commented pretty significantly about this one there,
20 too.

21 MR. STATTEL: Well, at the time when the
22 Working Groups were meeting, there was an argument and
23 counterargument from the industry where the
24 consequences of the spurious actuation could outweigh
25 the benefits of having the diverse system, right?

NEAL R. GROSS

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

1 And I think -- and I can't really speak to
2 the basis of the final wording that is in here -- but
3 I think the NRC took a position to basically avoid
4 that argument, right? In other words, I don't want to
5 put a diverse system in because it can increase the
6 probability of inducing a spurious failure, which
7 could result in a LOCA. If you initiate safety
8 injection, you could fill up the pressurizer and go
9 solid, right?

10 Use the probabilities of that to outweigh
11 the benefits of having the diverse system. We are
12 kind of avoiding the probability argument.

13 MEMBER STETKAR: And I don't want to get
14 into a probability argument right now.

15 MR. STATTEL: But I think that is the
16 reason why these words are this way.

17 MEMBER STETKAR: Let me step you back,
18 though. I am not talking about design of the diverse
19 system.

20 MR. STATTEL: Okay.

21 MEMBER STETKAR: Just forget the diverse
22 system for a moment.

23 MR. STATTEL: Okay.

24 MEMBER STETKAR: And just look at the D3
25 analysis for my existing protection system. I need to

NEAL R. GROSS

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

1 do a D3 analysis for my existing protection system and
2 evaluate the effects of possible common cause failures
3 in that system.

4 And I use that analysis as a basis, then,
5 for defining the functions, whether they are manual,
6 whether they are safety-related, automatic, non-
7 safety-related, of my diverse system.

8 MR. STATTEL: Right.

9 MEMBER STETKAR: So, forget the diverse
10 system now. Just think about the D3 analysis that I
11 need to do for my existing protection system. This
12 tells me that I do not need to look at spurious
13 actuations within that context, as I understand it.

14 MR. STATTEL: Well, spurious actuations
15 are a reality even with analog systems. It is not
16 just a phenomena for digital systems.

17 And the second point here points out that
18 the requirements to avoid the consequences of spurious
19 actuations is set forth in the plant design basis.

20 MEMBER STETKAR: Okay.

21 MR. STATTEL: It is covered in the plant
22 design basis evaluations.

23 MEMBER STETKAR: I wanted to hear you say
24 that.

25 MR. STATTEL: Where argument from the

NEAL R. GROSS

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

1 industry came in was that, by adding the diverse
2 system -- and I know you want to push it off to the
3 side, but that was really the crux of where this
4 language came from -- by adding a diverse system in on
5 top of the safety system, by definition, that diverse
6 system has some potential, however small it is, for
7 spuriously actuating the safety function, right?

8 So, having two systems that can
9 potentially spuriously actuate is obviously going to
10 have a larger probability than one, right? By
11 definition, you are always going to be increasing the
12 probability of causing a spurious actuation.

13 MEMBER STETKAR: I have met an awful lot
14 of really smart designers in my life.

15 MR. STATTEL: Uh-hum.

16 MEMBER STETKAR: And given a problem,
17 knowledge of a particular problem, it has been my
18 experience that designers can get pretty creative
19 about how to design something that works around that
20 problem. And that is why I want to push off the
21 diverse system for the moment.

22 MR. STATTEL: Okay.

23 MR. EAGLE: That is point 3, by the way.
24 And actually, there are two different types of
25 spurious actuations we are talking about. The first

NEAL R. GROSS

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

1 two deal with those caused by the common cause
2 failure. The second one is the one caused by the
3 diverse system, which you want to push aside.

4 So, basically, what we are really probably
5 talking about is those first two bullets.

6 MEMBER STETKAR: That's exactly right.

7 Now the second bullet is kind of a
8 paraphrase of things that I have read. In Section 3.7
9 of the BTP, the actual quote is, it appears in Section
10 1.8 and 3.7, but 3.7 is the acceptance criteria.

11 It says, "In general, spurious trips and
12 actuations are of a lesser safety concern than
13 failures to trip or actuate. There may be plant and
14 safety system challenges and stresses. However,
15 challenges that are significant are already set forth
16 in plant design-basis evaluations." That sort of
17 points to that second bullet.

18 However, I will ask you, does the plant
19 design-basis safety evaluation for a small LOCA event
20 consider, for example, a simultaneous steam line break
21 event? The answer to that is, no, it does not.

22 However, if a common cause failure of my
23 integrated protection system during a small LOCA event
24 can rapidly blow down automatically all four of my
25 steam generators, giving me something that looks

NEAL R. GROSS

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

1 like -- because they blowdown valves are large enough
2 to, for example, take 110 percent of full reactor
3 power -- that type of event is not evaluated in the
4 design-basis safety evaluation. So, I can't say that
5 it is bounded by a steam line or it is bounded by a
6 small LOCA. It is just simply not evaluated. It is
7 something that my integrated protection system can do.

8 And I have a couple of other examples
9 here, but in the interest of time, I won't mention
10 them.

11 Now, if I am not required to think about
12 that type of an event when I do, as an applicant, my
13 D3 analysis, then my designers don't know about those
14 conditions. So that, when they design the diverse
15 system, they may include protections against that,
16 recognizing that the diverse system could also have
17 some of its own spurious actuation concerns associated
18 with it.

19 But because of those types of events,
20 conditions --

21 MR. STATTEL: But for those systems, we
22 would expect a failure modes, an effect analysis to be
23 performed, and for safety systems, a hazards analysis.
24 And that becomes part of the design basis for those
25 systems.

1 And it is a presumption that the spurious
2 actuation aspects of a system, those failure modes,
3 are to be considered in the denial.

4 MEMBER STETKAR: Yes, but, typically, they
5 only do a single channel failure mode. They only do
6 a single failure mode. They rely on the diversity.

7 MR. STATTEL: Okay. You're talking about
8 common cause failure?

9 MEMBER STETKAR: They rely on the D3
10 stuff. I'm not worried about a single channel, you
11 know, a single relief valve opening. I am worried
12 about the system opening all relief valves.

13 MEMBER BLEY: But, I mean, we are putting
14 the system in to take care of common cause failure.
15 So, if, in fact, the system can generate accidents we
16 have never seen before, and these words tell you not
17 to look for them -- well, not these words; the other
18 words you had -- tell you not to look for them, then
19 that is troublesome.

20 I understand the argument that you didn't
21 want to dismiss these systems, but it seems that, if
22 you have them, you ought to look for potential harm
23 they could do and fix it, not say, "I don't want it"
24 because of that.

25 MR. STATTEL: But I think that was the

1 intent of the second bullet, that those failure modes
2 would be considered.

3 MEMBER STETKAR: I've got two or three
4 other examples, but in the interest of time, I just
5 brought up the steam line break with small LOCA
6 because it is one.

7 And I hate to do this because I always
8 tell people I am not an attorney and don't want to be
9 an attorney, but it is also notable that the lead-in
10 to this was that we do explicitly require people to
11 look at and evaluate, explicitly evaluate, the effects
12 from multiple spurious operations in all of our fire
13 regulatory guidance. And I don't understand why, if
14 the potential consequences of multiple spurious
15 operations are important enough to require an
16 evaluation for fires, why they are not important
17 enough to merit an evaluation under the context of
18 integrated digital protection systems.

19 There are a lot of analogies between fires
20 and what can happen in fires and the things --

21 MR. STATTEL: I understand. I am sure
22 those discussions were held when ISG-02 was presented.

23 (Laughter.)

24 CHAIRMAN BROWN: Hold it.

25 MR. STATTEL: But our task --

NEAL R. GROSS

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

1 CHAIRMAN BROWN: Hold it.

2 MR. STATTEL: But our task was to
3 incorporate the results of that.

4 CHAIRMAN BROWN: Richard, we've got 10
5 more slides to go. So, we have got to move along
6 here.

7 MEMBER BLEY: Can I say one more thing,
8 back on the slide you were on?

9 CHAIRMAN BROWN: Of course.

10 MEMBER BLEY: We have been talking about
11 bullet 2. Bullet 3 says, well, for tripping a
12 reactor, we want you to minimize the potential. If we
13 said that same word under bullet 2, I don't think I
14 would be as concerned.

15 MR. JUNG: Just one context is, remember,
16 the safety system is pure saturation. You know,
17 design-basis evaluation is one aspect. But you have
18 to think about, what is required to be high-quality
19 safety-related software systems? Now you are talking
20 about 603 requirements apply. Members heard about
21 systematic life-cycle process that it needs to go
22 through.

23 What I am saying is there is a significant
24 set of requirements in place to minimize the potential
25 reliability concerns over the safety systems

NEAL R. GROSS

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

1 themselves. That is, actually, a majority of our
2 review. We focus on safety system designs themselves.
3 From architecture, from software development, life
4 cycle, redundancy, and functional diversity, all that
5 is in place.

6 So, it is not like there is no, absolutely
7 no measure for the quality because, eventually,
8 software causing spurious actuation means there are
9 some quality concerns out of nowhere. We are not even
10 talking about -- remember, the policy says the design-
11 basis event concurrent with a common cause failure.

12 But this particular one actually we
13 discussed even beyond the policy scope. What if there
14 is no initiating event in place? You know, your
15 normal condition; suddenly, something takes place.
16 Because of software common cause failure, there is a
17 question about what is the trajectory; what initiates
18 that? Because software reacts to it when something
19 triggers it.

20 So, we had these discussions multiple
21 times. It is not really clear. But I want the
22 Members to be aware there is significant quality
23 requirements for the software themselves that provide
24 certain reasonable assurance that may address this
25 concern.

NEAL R. GROSS

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

1 MR. STATTEL: And there are some relevant
2 precedents as well. As you know, in boiling water
3 reactors, they all have the depressurization function.
4 And it was recognized very early on in that design
5 that the consequences of actuating those squib valves
6 was very severe.

7 And in response to that, the design of
8 that system incorporates some arming functions that
9 prevent, that are specifically designed to prevent
10 spurious actuations of those systems. And that has
11 been very successful to date, those techniques that
12 they applied.

13 So, really, that is the type of design
14 process and design-basis capturing that we are
15 alluding here. Those weren't driven. Those designs
16 were not driven by regulations. Regulations did not
17 drive General Electric to incorporate those measures.
18 It was really more addressing the failure modes that
19 existing in that system.

20 MR. EAGLE: We want to go on to slide 5.

21 This is clarification on design attributes
22 that are sufficient to eliminate consideration of
23 common cause failure. There have been many attributes
24 that would be very helpful, particularly like high-
25 quality software, V&V, all kinds of tests and

NEAL R. GROSS

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

1 everything, that could be used to help reduce the
2 probability of a common cause failure software
3 failure.

4 However, there are two that could be
5 identified, but either one of them would be sufficient
6 to eliminate consideration of common cause failure.
7 One of them would be if there is sufficient diversity
8 in the reactor protection system, and this is
9 evaluated on a case-by-case basis. Again, the
10 analysis, as it goes through, should be able to
11 identify that you have sufficient diversity at that
12 point.

13 The second one is testability. And we are
14 again quoting from ISG-04, the 100 percent
15 testability. If every possible combination of inputs
16 tested, and every possible sequence of device states
17 tested, and all outputs are verified for every case,
18 expected responses are known, tested, and found to be
19 100 percent correct, then the testability requirement
20 has been met. That could help eliminate the idea of
21 a common cause failure of that component or that group
22 of components.

23 DR. HECHT: Can I ask a question about
24 this?

25 MR. EAGLE: Yes, yes.

1 DR. HECHT: Is this with respect only to
2 actuation or with respect to subsequent control? So,
3 for example, what we have been talking about, an
4 injection system or an aux feedwater system, or
5 something like that, if the only issue is turning the
6 pumps on, that a single-shot action. The requirements
7 of 100 percent testing might potentially be met. But
8 if the function goes on to subsequent monitoring and
9 closely controlled, then it is not possible.

10 But does the testability, would it be a
11 feasible, licensable device that I can do something
12 which only actuates, thereby, avoiding the subsequent
13 need for closed-loop control, and then get it licensed
14 without the need for diversity if I can do 100 percent
15 testing?

16 MR. STATTEL: What I would say is it
17 depends. The answer to that, it depends on the
18 specific design. The intended applicability is to
19 ensure performance of the safety function. If the
20 safety function is defined as just actuate, and it
21 doesn't include the followup action in the safety
22 analysis, then it wouldn't include it. If it does
23 include that followup action, as was stated earlier
24 with integrated systems, then I would expect that it
25 would be included in this.

NEAL R. GROSS

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

1 MR. EAGLE: Yes, for example, if your
2 device was so simple that the only thing you had to do
3 was take several inputs and do an output, then that
4 probably could be 100 percent tested. But if that
5 device has to feed into some other group of devices
6 and has to have more complex type types, then it is
7 probably unlikely you are going to be able to do 100
8 percent testing. And therefore, you would need to
9 take a look at common cause failure.

10 DR. HECHT: Does the guidance here reflect
11 concerns about corrupted input or spurious inputs or
12 things like that as part of that?

13 MR. EAGLE: It says, "Every possible
14 combination of inputs."

15 DR. HECHT: So, that would include
16 corruption?

17 MR. EAGLE: That would include --

18 MR. STATTEL: This gets very difficult.
19 This criteria gets very difficult to meet as soon as
20 you --

21 (Laughter.)

22 MEMBER STETKAR: Once you look at that
23 "every possible combination" phrase.

24 CHAIRMAN BROWN: Once you have more than
25 one line of code, you're lost.

NEAL R. GROSS

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

1 DR. HECHT: As long as that is understood,
2 I'm --

3 CHAIRMAN BROWN: Yes, I think this is a
4 throwaway.

5 MEMBER STETKAR: I wouldn't expect many
6 people to invoke that.

7 MR. STATTEL: Even with the Wolf Creek
8 application, which was a main steam and feedwater
9 isolation function, it was receiving a digital input
10 and simply sending a digital output to those valves.
11 But even in that case, the 100 percent testability
12 argument, actually, when you did the math, it became
13 a lot of iterations of testing. And because of that,
14 we --

15 CHAIRMAN BROWN: Well, you have got to
16 test every possible form of that data that comes in
17 under corruption and everything else.

18 MR. EAGLE: Sorry.

19 (Laughter.)

20 CHAIRMAN BROWN: No, that's okay. That's
21 all right.

22 MR. EAGLE: Some of these are almost like
23 apple pie and motherhood. So, we will move through
24 these slides very quickly.

25 Another condition that came up was the

NEAL R. GROSS

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

1 echelons of defense. As you know from 603, it talked
2 about four items of what we call echelons of defense,
3 the idea that the operator is our main control with
4 his hands-on manual controls. If that fails to stop
5 something, you have the reactor trip system. You have
6 the engineering safety features that are supposed to
7 automatically come in. A fourth line of defense is
8 the monitoring indications. These were pointed out as
9 actually being conceptual more than absolutely hard,
10 fast divisions.

11 Combining maybe introduced new common
12 cause failure concepts. Remember that, originally,
13 you had the silos of the analog, each analog channel
14 coming through for various types of parameters. If
15 one of those failed, you had four different divisions,
16 and you had one channel fail, but you still had the
17 rest of that division intact.

18 Once you combine all those parameters
19 together in some kind of digital system, now if you
20 lose that digital system, you have lost that entire
21 division. However, in a common cause failure, you
22 could lose the entire four divisions. So, you do
23 definitely have different types of interactions when
24 you have common cause failure.

25 A D3 analysis, acceptable methods is done

NEAL R. GROSS

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

1 through 6303. It is subject to a potential common
2 cause failure. A diverse means needs to be provided.

3 CHAIRMAN BROWN: Before you leave this --

4 MR. EAGLE: Yes?

5 CHAIRMAN BROWN: Just from where I come,
6 I got wrapped around the axle on this whole issue of
7 combining into a single computer --

8 MR. EAGLE: Eight.

9 CHAIRMAN BROWN: -- both the ESFAS, EFS,
10 EFAS, ESFA, however you want to call it, and the
11 reactor trip system, and you all make this specific
12 comment in here: NRC regulations do not require, nor
13 does this guidance imply, that the echelons of defense
14 must be, the RTS and ESFAS echelons must be
15 independent or diverse from each other with respect to
16 CCF.

17 What?

18 MR. STATTEL: That's just a true
19 statement.

20 (Laughter.)

21 CHAIRMAN BROWN: Well, I love true
22 statements, but, I mean, why would you ever accept a
23 combined system? I mean, I just almost fall off the
24 cliff thinking that you would ever accept a combined
25 system where, instead of a reactor trip system, which

NEAL R. GROSS

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

1 has got its four divisions, and an ESFAS system, where
2 it has got its four divisions, they are separate, and
3 now I am going to stuff them into one thing.

4 I have reduced my baskets. I have gone
5 from eight baskets, if you want to call it that, down
6 to four baskets. And the more you lump stuff into one
7 area, the more likelihood you have of nailing yourself
8 to the wall on some type of a failure that locks
9 everything up.

10 MR. STATTEL: The reason it is written
11 this way is to purposely not be prescriptive and drive
12 design.

13 CHAIRMAN BROWN: Why not?

14 (Laughter.)

15 MR. STATTEL: Well, I mean --

16 CHAIRMAN BROWN: I think you are bending
17 over backwards to the point of just saying, well, gee,
18 we'll accept anything as long as it is not so ugly
19 that I don't have to put a mask over it.

20 MR. STATTEL: Well, in the case of Oconee,
21 they did combine echelons of defense. So, the same
22 process --

23 CHAIRMAN BROWN: Yes, I know; that one
24 slipped by me.

25 MR. STATTEL: However, when they performed

NEAL R. GROSS

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

1 their diversity analysis, the postulated failure mode
2 was a loss of all of those functions simultaneously in
3 all four divisions. So, as long as they follow that
4 analysis through, it is hard to come up with a
5 regulatory means for denying the applicability.

6 CHAIRMAN BROWN: Well, why shouldn't I
7 just have one division of something, put all the eggs
8 in one basket? And therefore, I will define that
9 as --

10 MR. STATTEL: It would have been a lot
11 easier for us for sure.

12 (Laughter.)

13 CHAIRMAN BROWN: -- subject to CCF, and I
14 will have a diverse, you know, so I will have two
15 things instead of eight things. I mean, at some
16 point, it is like the time difference between time
17 available and time required. The fewer things you
18 have to deal with, the more likely you are to screw
19 stuff up.

20 MR. EAGLE: The counterargument to that,
21 by the way, is the idea of digital equipment
22 increasing the capability, better able to handle
23 things, providing more efficiency --

24 CHAIRMAN BROWN: I am going to tell you,
25 quite frankly, in 1978 I went out for my first

NEAL R. GROSS

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

1 microprocessor-based system for an aircraft carrier.
2 The vendor came in and said, "Gee, why do you have a
3 microprocessor in every instrument? We can use,
4 instead of 28, we can use four, and we can manage this
5 entire protection system with four microprocessors,"
6 et cetera.

7 We looked at him and said, "You're nuts.
8 We don't even know how to do anything in 1978, 1979,
9 regarding safety system software," and threw him out
10 of the office.

11 He never said a study. So, we had 28. It
12 worked beautifully.

13 So, I mean, that whole idea, because of
14 the capability, just does not hold water.

15 MEMBER SIEBER: They were all TRS80s.

16 CHAIRMAN BROWN: It was a Z80, as a matter
17 of fact. Don't laugh.

18 MEMBER SIEBER: Right, I know.

19 CHAIRMAN BROWN: It was the only mill-
20 qualified microprocessor in 1979.

21 MEMBER SIEBER: Pretty fast.

22 MR. STATTEL: The current state of affairs
23 is we don't have a regulatory means for driving
24 designs in that direction. That's the bottom line.

25 CHAIRMAN BROWN: All right. Go on.

NEAL R. GROSS

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

1 DR. HECHT: But don't you still have the
2 independence requirement for the diversity --

3 MR. EAGLE: Oh, yes, the four divisions.

4 MR. STATTEL: We do, and we do review
5 these designs that combine these echelons to those
6 requirements.

7 CHAIRMAN BROWN: Yes, I understand that.

8 We've got to get on. Let's go on. I have
9 vented my spleen.

10 MR. EAGLE: This reemphasizes, Mr. Brown,
11 the fact that we do need the common cause failure, the
12 diverse means, because of the possibility of losing
13 all those.

14 Problem statement 7 was clarification on
15 whether a CCF is classified as a single failure in
16 design-basis event evaluations. Again, CCF is not
17 classified as a single failure, as defined in Reg
18 Guide 1.53. It is considered beyond-design-basis.

19 Digital reactor protection systems,
20 however, should be protected against common cause
21 failure. That is basically the bottom-line theme
22 throughout BTP 7, Revision 6.

23 Postulated common cause failures need not
24 be considered as a single failure in design-basis
25 evaluations. Analysis of common cause failures

NEAL R. GROSS

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

1 coincident with the design-basis events can use
2 realistic assumptions. And again, we define realistic
3 assumptions.

4 And there was one additional one. We have
5 actually already brought this up, but there was an
6 additional item that came up. And this was where that
7 there was actually possibility of two manual
8 initiation systems.

9 Now IEEE 603 states basically that you are
10 required to have a manual ability to initiate the
11 automatic reactor protection system. But it doesn't
12 say, other than saying you need a minimum number of
13 components and this type of thing from the control
14 room, it doesn't state that you have to be completely,
15 that you can't go through the automatic system. So,
16 if you do go through the automatic system, then there
17 is a possibility you will need -- that system could be
18 subject to a common cause failure and, therefore,
19 would require a diverse means to initiate the manual
20 actuations or manual initiations. Therefore, you
21 would have two systems.

22 So, what would be the criteria you would
23 need so we could only have one system? So, the two
24 could be combined under these circumstances: the
25 reactor manual protection activation system is

NEAL R. GROSS

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

1 independent and diverse from the actual automatic
2 reactor protection system. It has to be safety-
3 related and not subject to the same potential common
4 cause failure as the automated reactor protection
5 system.

6 I believe that is what we discussed here
7 shortly before.

8 CHAIRMAN BROWN: Okay. Yes. That just
9 says, whatever it is, if your manual means goes
10 through the processor, the computers, then you have
11 got to have an independent, separate, manual actuation
12 system. I mean, it may be an automated system, but it
13 is a separately automated system. It is not
14 necessarily analog.

15 MR. EAGLE: Well, now this is the manual
16 system. In other words, right, if you have got those
17 two buttons that scram the plant --

18 CHAIRMAN BROWN: Yes, I understand, but
19 you have got the one that goes to the automated
20 system, and the other one you haven't defined -- as
21 long as it is independent --

22 MR. EAGLE: Right.

23 CHAIRMAN BROWN: -- from the primary
24 safety system and it's diverse. It doesn't mean,
25 because I haven't seen -- maybe I've missed them -- it

NEAL R. GROSS

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

1 doesn't say it can't be software-based as long as it
2 is suitably diverse from the primary software-based
3 system. Is that --

4 MR. EAGLE: Correct.

5 CHAIRMAN BROWN: You haven't precluded
6 that?

7 MR. EAGLE: Right.

8 MR. STATTEL: Depending on the design --

9 CHAIRMAN BROWN: Yes, okay. I just want
10 to make sure I understood that nuance in terms of how
11 you all were thinking about it.

12 MR. EAGLE: Yes, we used one example of
13 saying one possibility would be like a hardwired
14 system. It is just an example.

15 CHAIRMAN BROWN: Yes.

16 MR. EAGLE: But it could also be software,
17 too.

18 Also, we received a considerable number of
19 public comments, approximately 70. Ninety percent of
20 them came from NEI. They are included in various
21 information that was made available to the Committee.
22 And we would like to point out some of the more
23 notable ones.

24 In some instances, comments led to
25 additional clarification for clearer understanding and

NEAL R. GROSS

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

1 improvement.

2 Staff agreed with some comments in
3 principle, but not with the specific rewording
4 recommendations. Staff addressed them based on
5 principle or accepted portion.

6 The staff agreed that not all reactor
7 protection system safety functions may be disabled by
8 a common cause failure, but pointed out that assuming
9 all reactor protection system functions are disabled
10 is a worst-case bounding condition.

11 Based on digital operating experience,
12 several comments challenged why CCF was considered
13 beyond-design-bases. And until there is a revision of
14 the Commission policy, Revision 6 states that CCF is
15 beyond-design-basis.

16 A comment stated that the intent of BTP
17 7-19 is not to protect the digital safety systems, but
18 to protect the plant. The staff accepted the comment
19 and addressed it accordingly.

20 The staff accepted a comment expressing
21 concern that, after actuation of the ESF functions
22 from the main control room, the need may exist for
23 some use of local controls later. And for instance,
24 just one example might be like beyond 72 hours,
25 although maybe it might be shorter times and maybe

NEAL R. GROSS

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

1 other special circumstances.

2 Comments challenged the concept that
3 diverse means had to be both independent and diverse.
4 We have discussed this. The staff prepared a
5 paragraph discussing independence. That was in under,
6 we talked about that one on page 7 concerning point 3.

7 Also, there were several notable
8 clarifications in BTP 7-19, Revision 6, that were of
9 interest. Based on the ACRS letter on Reg Guide 1.62,
10 "Manual Initiation of Protective Actions," "system
11 level" was changed to "system or division level,"
12 depending on the design.

13 IEEE 603 requires manual initiation of
14 automated functions. There is no requirement the
15 manual initiation be independent from the automated
16 actuation. If subject to the same postulated common
17 cause failure as automated functions, then an
18 additional diverse means for manual initiation is
19 needed. We, of course, talked about that as part of
20 the extra item.

21 The use of the term "diverse backup
22 method" was replaced with simply the "diverse means"
23 to mach with the Four-Point D3 Policy and because some
24 current nuclear power plants use the term in their
25 main system called "primary" and "backup".

NEAL R. GROSS

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

1 Again, the 100 percent testing definition
2 was copied directly from ISG-04. A common cause
3 failure that affects normal displays or controls
4 should not prevent an operator from manually
5 initiating safety functions. Guidance on
6 prioritization of commands to an actuated component
7 were copied from ISG-04.

8 Since single failures concurrent with a
9 common cause failure are not required to be postulated
10 and normal equipment alignment is assumed, diverse
11 actuation of one division is sufficient, provided that
12 one division is in service. That is somewhat of a
13 caveat and oftentimes leads to a more complex system
14 of the diverse, perhaps with several different
15 subdivisions involved in the diverse method.

16 CHAIRMAN BROWN: Don't bother with 39 and
17 40.

18 MR. EAGLE: Okay. Okay.

19 CHAIRMAN BROWN: They are just a summary.

20 MR. EAGLE: Yes. Okay.

21 CHAIRMAN BROWN: I just wanted to do two
22 things. First, relative to the comment on the
23 independence issue, where you pointed me back to
24 concerning point 3 on page 7 --

25 MR. EAGLE: Yes. Right.

NEAL R. GROSS

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

1 CHAIRMAN BROWN: -- and a couple of the
2 statements from industry on items 6, 7, 8, and 9,
3 which we discussed earlier.

4 I see the words in concerning point 3. I
5 went and read them as we were talking here. Yet, if
6 I go back and I read the industry comments, they make
7 very clear statements which seem to be inconsistent a
8 little bit with -- I'm not saying what you don't have
9 in concerning point 3 isn't there. To me, that's
10 fairly clear. But, yet, they make statements there's
11 no requirement for independence between automatic and
12 manual functions. Okay? And then, they go on to say
13 there's no need for independence to cope with common
14 cause failures.

15 And you agreed with both of those. All
16 four times you agreed with it, as they made that point
17 repeatedly.

18 So, they deleted all those words of
19 independence. I see this. I see your all's words
20 about agreeing with that. And then, I look at the
21 words over here where you have assuaged me somewhat
22 relative to the thing by saying, really, you've got to
23 have independence from your manual means --

24 MR. EAGLE: Right.

25 CHAIRMAN BROWN: -- one way or another

1 from your automatic systems. Forget about what you
2 call it; you've got to have an independent operation.
3 But, yet, they are saying you don't need independence.

4 So, I don't know whether comments and
5 resolution of comments can come back to bite you
6 sometimes, but that --

7 MR. EAGLE: Basically --

8 CHAIRMAN BROWN: Go ahead.

9 MR. EAGLE: Yes, basically, we were in
10 agreement that, when you say "independence" and
11 "diverse", that we agreed that basically both "and's"
12 together, that they didn't necessarily have to be both
13 independent and diverse, that diverse was obviously
14 the main point. And that when they took over the
15 independence as a separate look-see or a separate
16 requirement, it covered the independence.

17 CHAIRMAN BROWN: But if I have an
18 automatic system that is my primary system, and I am
19 going to have a diverse, I am required to have a
20 diverse system, doesn't it, by definition, have to be
21 independent from the primary system?

22 MR. EAGLE: Basically, obviously, it is
23 independent.

24 CHAIRMAN BROWN: But that's not -- that
25 seems to be --

1 MR. STATTEL: Well, I think it was more of
2 a clarification. If you read the original words --

3 CHAIRMAN BROWN: In?

4 MR. STATTEL: -- in what they were
5 commenting on --

6 CHAIRMAN BROWN: Yes, I didn't see the
7 originals.

8 MR. STATTEL: Right. The originals, based
9 on what they were commenting on, it could be
10 interpreted to literally impose requirements that
11 didn't exist with regard to independence of the
12 system, particularly when you were using a safety
13 system to implement your diverse function, right? So,
14 it was really more of a literal interpretation, and we
15 provided the clarification and gave that dividing
16 point between safety and non-safety.

17 CHAIRMAN BROWN: Okay. Let me phrase this
18 another way. I have got four divisions of automated
19 microprocessor, computer-based divisions.

20 MR. STATTEL: Yes, yes.

21 CHAIRMAN BROWN: And I have got a diverse
22 manual system that is within that. In other words, it
23 doesn't get compromised by CCF.

24 MR. STATTEL: Okay.

25 CHAIRMAN BROWN: Okay? Doesn't that imply

NEAL R. GROSS

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

1 in some way that it is independent of the computer-
2 based functionality of each division, within each
3 division?

4 MR. STATTEL: Yes, it is implied in an
5 automatic system and in a manual system, usually it
6 implies independence. They're different systems.

7 CHAIRMAN BROWN: There is no need for
8 independence to cope with CCF; that is a direct
9 statement by industry four times. Okay?

10 MR. STATTEL: Honestly, I think it may be
11 taken out of context a little bit.

12 CHAIRMAN BROWN: I'm just reading the
13 words as you all phrased them in the --

14 MR. STATTEL: Well, right, but I think you
15 really have to look at the original wording of the
16 BTP.

17 CHAIRMAN BROWN: All right. I'll stop
18 right there. I just want to make sure that the
19 independence issue is of primary interest to me all
20 the way along.

21 MR. EAGLE: Right. We basically agreed
22 with industry that the idea of independence and
23 diverse did not have to be linked together. Actually,
24 the diversity by itself, and then the independence
25 examination by itself --

NEAL R. GROSS

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

1 CHAIRMAN BROWN: I, quite frankly, can't
2 see how you can have one without the other.

3 MR. EAGLE: It depends on where it is.

4 CHAIRMAN BROWN: But I'm not real smart.

5 MR. EAGLE: But their claim was that, if
6 you have, for instance, if you have four divisions of
7 diversity, and they could be actually included in the
8 safety divisions, but they would be there without
9 being independent --

10 MR. STATTEL: Right, without being
11 electrically independent.

12 MR. EAGLE: -- electrically independent,
13 they could be in the same division. But they would be
14 independent of each other, the four --

15 CHAIRMAN BROWN: When you say
16 "electrically independent," okay, let's stop right
17 there.

18 MR. STATTEL: Powered by the same source.
19 They have the same power.

20 CHAIRMAN BROWN: I might work on that one
21 a little bit.

22 MR. STATTEL: Well, they were; they are.
23 They are.

24 CHAIRMAN BROWN: No, I understand that.

25 MR. STATTEL: So, I mean, that is

NEAL R. GROSS

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

1 literally where the interpretation issues came up on
2 those comments. Because the wording was originally
3 written --

4 CHAIRMAN BROWN: Hold it. But if the
5 power source cannot be compromised by the CCF --

6 MR. STATTEL: See, you're talking four
7 divisions here.

8 CHAIRMAN BROWN: I understand.

9 MR. STATTEL: There's four divisions of
10 the safety, and there's four divisions of the
11 diverse --

12 CHAIRMAN BROWN: I'm just saying, but if
13 they're all the same and they can't be compromised by
14 the power supplies themselves feeding the diverse
15 system, can't be compromised by the CCF, then, in
16 fact, it can be considered to be independent from CCF.
17 In other words, you have used independence to cope for
18 CCF.

19 MR. STATTEL: But, I mean, if you make a
20 statement that they have to have a different power
21 source --

22 CHAIRMAN BROWN: I'm not saying that.

23 MR. STATTEL: But, I mean, if you made
24 that statement -- this is akin to what was in the
25 original wording -- if you make a statement that the

NEAL R. GROSS

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

1 diverse system has to be independently powered by a
2 different source, then that precludes me from
3 implementing that within the safety systems because
4 there are only four safety divisions.

5 CHAIRMAN BROWN: I got that.

6 MR. STATTEL: So, I have to use the same
7 power source, right? So, we didn't want to --

8 CHAIRMAN BROWN: No, you don't have to.
9 You can put separate power sources within each
10 division to power that particular part of it. So,
11 there is no preclusion of that. It just a matter of
12 evaluating the whole system.

13 MR. EAGLE: I believe when designs are
14 doing that, they have dual power supplies inside each
15 division.

16 CHAIRMAN BROWN: Well, you could have two
17 pairs of dual power supplies.

18 (Laughter.)

19 All right. Let me just finish up. I
20 wanted to see if there are any open items here. I am
21 not going to work on this one anymore, but John
22 brought up the issue of the words on time
23 available/time required. And I think you agreed to
24 try to come up with a --

25 MR. STATTEL: We will look at his quote.

NEAL R. GROSS

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

1 He gave us a quote.

2 CHAIRMAN BROWN: Yes, and see how that
3 fits into the context.

4 MR. STATTEL: Right.

5 CHAIRMAN BROWN: I'm looking at my other
6 notes. Where are the other notes?

7 The manual control and override. John had
8 to leave for another meeting. So, I didn't see that
9 as being open at this point, by the time we finished.
10 I don't know how anybody else looked at that. There's
11 a number of nuances that we went through in the
12 discussion.

13 But, Dennis, do you? Or, Jack, do you?

14 MS. ANTONESCU: ISG-05.

15 CHAIRMAN BROWN: Doesn't some of that get
16 covered by 18-A, when we get to that, in terms of
17 manual operations? So, I didn't see that we needed to
18 take that. Okay.

19 And I guess on, let's see, the spurious
20 actuation ones, John still wanted to ruminate on that.
21 How do you propose we address that? I mean, I presume
22 this will be -- are we going to set this up for a full
23 Committee meeting? We hadn't really talked about that
24 yet. They're about to issue this.

25 MEMBER BLEY: Were you expecting a letter

NEAL R. GROSS

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

1 on this?

2 CHAIRMAN BROWN: I don't think they were,
3 but you can answer that yourself.

4 MEMBER SIEBER: We decide whether they get
5 a letter or not.

6 MEMBER BLEY: Well, I know, but sometimes
7 they --

8 CHAIRMAN BROWN: But were you all
9 expecting a letter on this?

10 MR. JUNG: Not necessary. Revision 1 has
11 been reviewed by ACRS. It is the last step. Another
12 letter will just --

13 CHAIRMAN BROWN: Revision 1 of?

14 MR. JUNG: ISG-02. A lot of these
15 subjects we discussed --

16 CHAIRMAN BROWN: Oh, yes. Yes, I went
17 through them one-by-one on these. They did crank them
18 all in.

19 MEMBER BLEY: I don't remember what we
20 said then on spurious actuations. I think John
21 probably said something. I mean, he may want to get
22 a letter out on that because he sees that as a key
23 issue.

24 MEMBER SIEBER: Well, the argument was in
25 fire protection spurious actuations was a big deal.

NEAL R. GROSS

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

1 Here they say don't worry about them. So, you have
2 got to decide, am I going to worry about them because
3 it's a big deal or I'm not going to worry about them
4 because I don't have to?

5 CHAIRMAN BROWN: Well, the statement was
6 just a base statement. It just said there's less
7 concern, period, and there was no presentation of a
8 set of considerations as to why it was considered of
9 lesser severity.

10 MEMBER SIEBER: Well, you could make the
11 distinction that fire is a separate element as opposed
12 to all the other kinds of requirements.

13 MEMBER BLEY: No, he was just using that
14 as an example, though.

15 MEMBER SIEBER: Yes.

16 MEMBER BLEY: If you anchor it in
17 regulation in one place, why not the other? The
18 underlying question was, if you put a new system in
19 and were looking at common cause failure, why ought
20 you not look at significant events that could be
21 there? We heard the staff argument that they think
22 that is covered in the normal design review, and that
23 wasn't clear to all of us. So, I don't know where
24 that sits.

25 CHAIRMAN BROWN: The spurious actuations

NEAL R. GROSS

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

1 issue?

2 MEMBER BLEY: Yes. I don't know where
3 John sits on that.

4 CHAIRMAN BROWN: Okay.

5 MEMBER BLEY: You know, you are probably
6 not going to close it in the sense you are trying to
7 close things. I think that will continue as a
8 concern. What the Committee does about that, the
9 Committee will have to decide.

10 CHAIRMAN BROWN: Yes. Okay. Well, I
11 guess, right now, from a standpoint of what we expect
12 back, it would be just the one item. And I will try
13 to get with John.

14 Did you have something, Jack? I'm sorry,
15 I didn't go around the table to see if you --

16 MEMBER SIEBER: Yes, well, this is a way
17 to do it.

18 (Laughter.)

19 But, in any event, one of the things that
20 sort of troubles me is all of this seems to be
21 directed toward actuations of safety systems. In
22 other words, you close a circuit breaker someplace and
23 everything starts and happens automatically. And if
24 it doesn't, some operator can go and flip a switch and
25 make it happen.

NEAL R. GROSS

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

1 On the other hand, there is a whole series
2 of safety systems, and the aux feed is one of them,
3 where you require modulating control. In other words,
4 you have to use a three-element control system in
5 order to control the regulating valves or, if they are
6 electric-driven, aux feed pumps, or the turbine
7 throttle valve for steam-driven aux feed pumps.

8 That requires manual operator action on a
9 continuous basis. He doesn't run and flip a switch
10 and say, "I did my job." He has to pay attention to
11 what is going on.

12 Now the question is, are we just talking
13 about actuating safety systems or are we talking about
14 operating safety systems, once they are actuated, to
15 maintain the right parameters? And the impression I
16 got was we don't consider these auxiliary control
17 systems that operate regulating valves, and so forth,
18 as part of the actuation system. And therefore, it is
19 not covered by this.

20 CHAIRMAN BROWN: Well, I guess I tried to
21 think about that, as John was going through it. And
22 if you went back and looked at the concerning point 4,
23 there were two specific statements in there where it
24 stated that you had to manage the plant-critical
25 safety functions, one.

NEAL R. GROSS

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

1 MEMBER SIEBER: Right.

2 CHAIRMAN BROWN: And then, the last
3 paragraph explicitly states, once manual actuation is
4 performed from the MCR using these displays and
5 controls, controls outside the MCR for long-term
6 management of these plant-critical safety systems may
7 be used when supported by HFE analyses.

8 So, that is how I walked away from what
9 you have to do downstream. You have got to look at
10 that after you have actuated it. And if you need to
11 modulate stuff, then you have got to know that you
12 have got the analyses that says I can go do that
13 within the context --

14 MEMBER SIEBER: Well, we tried to do that.
15 It's very difficult.

16 CHAIRMAN BROWN: I'm not disagreeing. I
17 have watched people try to control steam generators
18 during a rapid ship transient maneuver where it's
19 really hard.

20 MEMBER SIEBER: Yes. The other thing is
21 you let it flood and let the relief valves take care
22 of it, but I don't particularly like to rely on relief
23 valves opening and closing as a way to regulate
24 pressure or heat removal or anything else. Sooner or
25 later, one of them is going to stick.

NEAL R. GROSS

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

1 MR. STATTEL: I don't disagree that an HFE
2 analysis should be performed for those situations.

3 MEMBER SIEBER: I know you don't.

4 MR. STATTEL: I'm not seeing the
5 connection to where the BTP 19 would drive performance
6 of that analysis, because those are things that are
7 required outside of the scope of a common cause
8 failure.

9 MEMBER SIEBER: Well, and I agree with
10 that. The regulations, the way they are written,
11 don't encompass that aspect of it. On the other hand,
12 from a practical standpoint, from the operator's
13 standpoint, you have to deal with it. No place do we
14 deal with it that I know of.

15 MR. EAGLE: To follow up on that, I just
16 want to reemphasize that the --

17 MEMBER SIEBER: So, yes, I understand how
18 the regulations are put together and what you are
19 trying to do.

20 MR. EAGLE: Right.

21 MEMBER SIEBER: I just think there is an
22 outlier.

23 MR. EAGLE: I just want to reemphasize
24 that one point. Remember, what we are looking at is
25 the common cause failure of the automated system, the

NEAL R. GROSS

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

1 automated reactor protection system. And once you
2 have that failure, then you need to provide a diverse
3 means that will accomplish that same function. Okay?

4 We also stated that, if you are already
5 doing something manually and you have a common cause
6 failure, you are still expected to be doing it
7 manually. You just may have to do some different
8 equipment.

9 So, remember, the BTP 7-19 is still
10 focused mainly on the failure of the automatic reactor
11 protection system.

12 MEMBER SIEBER: Right.

13 MR. EAGLE: So, you're right about getting
14 into manual stuff. Once you get over there, anything
15 falling through that needs to be manual, that may be
16 outside of the scope of the --

17 MEMBER SIEBER: That's right.

18 MR. EAGLE: -- key idea of replacing the
19 automatic system.

20 MEMBER SIEBER: Yes, it's still a problem,
21 but it's probably outside the scope of this.

22 CHAIRMAN BROWN: Okay. I'm not going to
23 be able to resolve this here. So, you should just be
24 aware that these two items, that we still need to
25 resolve what we are going to do, and that would be on

NEAL R. GROSS

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

1 the follow-on operations and the spurious actuation.
2 Since John had to leave to go to another meeting, we
3 will probably have to independently come to that
4 conclusion.

5 Myron, did you have any comment?

6 DR. HECHT: Possibly a third one, and that
7 is on page 35.

8 CHAIRMAN BROWN: Slide 35?

9 DR. HECHT: Yes, slide 35. Excuse me. In
10 response to a public comment, "Staff agreed that not
11 all RPS safety functions may be disabled by a CCF, but
12 pointed out that assuming all RPS functions are
13 disabled is a worst-case bounding condition."

14 And I am just wondering if that is always
15 the case.

16 MR. EAGLE: Well, the idea was, if you
17 lose everything, in other words, you just assume that
18 the entire automatic reactor protection system has
19 disappeared, then it is hard to imagine not that being
20 pretty close to a bounding condition.

21 The public comments pointed out that you
22 may have a failure in your reactor, in some part of
23 this calculational system, but it may not fail other
24 parts. And that may be true. We couldn't disagree
25 with that.

NEAL R. GROSS

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

1 But if you just assume that whatever
2 failure takes out everything, then your diverse system
3 has to be able to replace the functionality or the
4 safety function that was lost for that particular
5 event.

6 MR. STATTEL: I can only speak for the
7 analyses that have been performed. And we have used
8 those bounding assumptions.

9 DR. HECHT: Well, I know that that is an
10 assumption. But is there a partial failure mode of --
11 let's extend it to more than the RPS or I guess
12 several critical functions that are listed in 603. I
13 don't remember them all.

14 Is it possible that two systems fighting
15 with each other, when one system has a partial failure
16 mode, could be worse than if the primary system
17 totally fails? And shouldn't that be shown as part of
18 an analysis?

19 MR. STATTEL: I would expect --

20 DR. HECHT: It might be a trivial one,
21 but --

22 MR. STATTEL: I would expect those types
23 of failure modes to be identified in the failure modes
24 and effects analysis, and, also, to be included in the
25 hazards analysis, which is part of the design process.

NEAL R. GROSS

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

1 So, we do review those documents as well.

2 MR. JUNG: Myron, for new reactors we get
3 into that question and we work with them. But if you
4 look at the diverse means that we looked at, they are
5 looking at plant condition diverse ways. So, a
6 reactor level, water level, is changing either through
7 partial or not. Actually, diverse means actually
8 don't know exactly what caused the primary system.
9 So, some of the partial situations we looked at, we
10 couldn't come up with a good reason why failure to
11 actuate cannot be a bounding case.

12 For example, certain water flow coming in
13 from two pumps instead of two pumps and one pump comes
14 along type of things. We are assuming that already
15 two pumps are not doing anything. So, if you have one
16 pump providing water, what we can see is maybe there
17 is additional time available for the backup diverse
18 means to kick in a little bit later. So, maybe more
19 time.

20 We couldn't come up with a scenario where
21 there is some more urgent need that is beyond the
22 bounding. So, we couldn't come with a really good
23 reason for it.

24 MEMBER BLEY: I think the only thing that
25 comes to mind is, if somehow one of these partial

NEAL R. GROSS

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

1 failure modes isn't recognized as failure, such that
2 the diverse system gets actuated. And I can't give
3 you -- I haven't dug deeply on that, but there might
4 be some partial failure that looks like the system
5 worked.

6 So, if the diverse system worked, I think
7 you would be all right. But if it doesn't know it has
8 got to work, that would seem to be one that could get
9 you into lots of unanalyzed conditions. I don't know
10 if you guys --

11 CHAIRMAN BROWN: You are talking about it
12 disguising the need to actuate a diverse system in one
13 way, shape, or form?

14 MEMBER BLEY: Somehow.

15 CHAIRMAN BROWN: Yes.

16 MEMBER BLEY: Yes, such that it --

17 CHAIRMAN BROWN: Whether manually or --

18 MEMBER BLEY: Such that it is close enough
19 to good that the system doesn't realize it ought to
20 start.

21 CHAIRMAN BROWN: Operators don't run them
22 or --

23 MEMBER BLEY: But, then, you can rely on
24 the operators. So, I would agree, you would probably
25 have more time then, if that happens.

NEAL R. GROSS

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

1 MR. STATTEL: But, even in those cases,
2 there are instructions for the operators, and there
3 are PAMS variables. There are Reg Guide 1.97
4 variables that are provided to the operators to
5 confirm that the water is getting to where it needs to
6 go.

7 MEMBER BLEY: That's true. That's true.

8 MR. EAGLE: Another thing that might be
9 pointed out, I think Rich pointed out, was a lot of
10 times, the way it is set up, like if you have a
11 parameter, you know, the automatic system, the reactor
12 protection system would kick in at this point. But if
13 it doesn't kick in, right below it may be a parameter
14 that is feeding directly to the diverse system, and
15 that would be, if it doesn't do the first one, then
16 the second one catches it.

17 MEMBER BLEY: The only thing I would
18 suggest there is, when situations get real complex,
19 which this might be, we have seen incidents in the
20 last couple of years where it is real hard for
21 operators to figure them out. So, that would be the
22 one spot, but I don't think that is a big deal.

23 CHAIRMAN BROWN: Okay.

24 MEMBER BLEY: Anyway, we've got another
25 meeting, Charlie.

1 CHAIRMAN BROWN: I know. I'm going to
2 close this off right now.

3 We will try to get back to you. Well, not
4 try; we will get back to you in one way, shape, or
5 form as to the next step on this. We need to resolve
6 whether with a full Committee meeting or whether we
7 are going to write on it or not, based on a couple of
8 these concerns.

9 MR. JUNG: I think you ought to leave it
10 up to the ACRS to decide that.

11 CHAIRMAN BROWN: Yes, we won't dally on
12 it. Okay? I mean, obviously, we are not going to do
13 anything this week.

14 MR. JUNG: Understand.

15 MEMBER BLEY: But we have a meeting, a
16 full Committee meeting, this week to talk about. We
17 need to talk about it

18 CHAIRMAN BROWN: Yes. Yes, we've got time
19 to discuss it.

20 All right. The meeting is adjourned.

21 Thank you very much, gentlemen.

22 (Whereupon, at 12:23 p.m., the meeting was
23 adjourned.)

24

25



**Presentation to ACRS on
Standard Review Plan
Branch Technical Position 7-19
Revision 6**

September 7, 2011

Richard Stattel, NRR/DE/EICB

Gene Eagle, NRO/DE/ICE2

Ian Jung, NRO/DE/ICE2

Russell Sydnor, RES/DE/DICB

**BRANCH TECHNICAL POSITION (BTP) 7-19 Revision 6,
“GUIDANCE FOR EVALUATION OF DIVERSITY AND
DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED
INSTRUMENTATION AND CONTROL SYSTEMS”**

PURPOSE OF BRIEFING:

Highlight and identify the key questions or concerns from DI&C-ISG-02 and discuss the resulting guidance incorporated into this revised BTP 7-19

Current Status of BTP 7-19 Revision 6:

- Sent to OMB June, 2011 (Congressional Review Act)
- Expected to be issued by September 30, 2011

Agenda

1. General Basis and Purpose of BTP 7-19 Revision 6
2. Background
3. NRC Four-Point Policy on Defense-in-Depth and Diversity (D3)
4. Comments on NRC Four-Point Policy on D3
5. Plant Critical Safety Functions
6. Independence of the Diverse Means
7. General Criteria of the Diverse Means
8. Stakeholder Concerns From DI&C-ISG-02
9. Public Comments and Staff Response
10. Notable Clarifications in BTP 7-19 Revision 6
11. Summary and Questions

General Basis for BTP 7-19

- Despite the use of quality software development techniques and extensive testing, digital systems generally cannot be proven to be error-free
- Software based digital systems are considered susceptible to the same error appearing in identical copies of the software-based logic and architecture that are present in redundant divisions of safety-related systems
- Therefore, software-based or software-logic-based digital system development errors are a credible source for a potential common-cause failure (CCF)
- In BTP 7-19, software includes firmware and logic developed from software-based development systems

General Basis for BTP 7-19

- In summary, while the NRC staff considers (software) CCF in digital systems to be beyond design basis, nuclear power plants should be protected against the effects of anticipated operational occurrences (AOOs) and postulated accidents with a concurrent CCF in the digital protection system

Purpose of BTP 7-19

- Purpose of BTP 7-19 is to provide guidance for digital, software-based or software-logic-based Reactor Protection Systems (RPS) {i.e., Reactor Trip System (RTS) and Engineered Safety Features Actuation System(ESFAS)}
- Provide guidance for evaluating applicant's:
 - D3 assessment
 - Diversity in design
 - Design of manual controls and displays
- Ensure conformance with NRC position on D3
- Specifically verify:
 - Adequate defense-in-depth
 - Adequate diversity
 - Displays and manual controls for (plant) critical safety functions are diverse from automatic portions of RPS

Background

- In March 2007 BTP 7-19 Revision 5 was issued in anticipation of new reactor applications
- In November 2006 industry representatives claimed to Commission that there was still confusion or insufficient guidance in digital I&C area and needed additional guidance for licensing certainty
 - In early 2007 Steering Committee formed and a Project Plan developed
 - Seven Task Working Groups (TWGs) formed
 - TWG#2 on D3 formed with members from NRR, RES and NRO
 - Significant stakeholder involvement through many public meetings

Background

- Initial issue of Interim Staff Guidance (ISG) for D3 in September 2007
 - DI&C-ISG-02 Revision 1
 - Addressed seven problem statements from industry
- ACRS reviewed the draft of DI&C-ISG-02 Revision 1
 - ISG will help licensing review
 - The staff should determine the conditions under which operator manual actions can be credited as a diverse protective function
 - The issue of spurious actuation needed to be examined further

Background

- DI&C-ISG-02 Revision 2 (currently effective) was issued in June 2009
 - Additional clarification and editorial changes
 - The ACRS letter on DI&C-ISG-02 Revision 1 addressed
 - Clarified option for manual operator action as diverse protective action
 - Must be justified using HFE methods in ISG-05
- BTP 7-19 Revision 6 development incorporated DI&C-ISG-02 Revision 2

NRC Four-Point Policy on D3

[from SRM on SECY-93-087 in Item 18, II.Q]

1. “The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.”
2. “In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.”

NRC Four-Point Policy on D3 (cont)

[from SRM on SECY-93-087 in Item 18, II.Q]

3. “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions”

4. “A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.”

Comments on NRC Four-Point Policy on D3

Concerning Point 2

- The term “best-estimate methods” is more accurately referred to as “realistic assumptions” – defined as normal plant conditions corresponding to the event:
 - Power levels
 - temperatures
 - pressures
 - flows and
 - equipment alignment

Comments on NRC Four-Point Policy on D3

Concerning Point 3:

- If D3 analysis indicates potential for CCF, Point 3 directs applicant to identify or add a diverse means
- “Safety Computer System in points 1 and 3” refers to the automated safety–related RTS and ESFAS
- Point 3 also applies to manual initiation methods of RTS and ESFAS, if subject to CCF
- Special independence requirements for diverse means may apply

Comments on NRC Four-Point Policy on D3

Concerning Point 4

- Directs providing a set of displays and controls (safety or non-safety) in main control room (MCR)
- Diverse from any CCF vulnerability in RTS or ESFAS
- Meets divisional independence requirements as applicable to specific design implementation
- For manual, system level or divisional level (depending on design) actuation and control [versus only component level actuation and control]

Comments on NRC Four-Point Policy on D3

Concerning Point 4 (cont)

- For control and management of “(plant) critical safety functions”
- If not subject to CCF, some of these displays and manual controls may be credited as all or part of diverse means directed by Point 3
- For digital modifications in operating plants, retention of existing controls in MCR may help satisfy Point 4
- Once manual actuation from MCR using Point 4 controls is completed, controls outside MCR may be used for long-term management when supported by suitable HFE analysis and procedures

Plant Critical Safety Functions

From NUREG-0737, Supplement 1

- Reactivity Control
- Reactor core cooling and heat removal from primary system
- Reactor coolant system integrity
- Radioactivity control
- Containment conditions

Independence of the Diverse Means

- Independence requirements of diverse means from safety protection system (i.e., physical and electrical, and communication separation) are defined in IEEE Std. 603
- Diverse means could be safety-related and part of a safety division, and would be subject to meeting divisional independence requirements
- Diverse means could be non-safety-related; then the IEEE Std. 603 requirement to separate safety from non-safety equipment would still apply and would require independence of the two systems
- In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system

General Criteria for the Diverse Means

- If D3 assessment reveals a potential for a CCF, the method for accomplishing the diverse means should be:
 - at the system or division level (depending on design)
 - initiated from the control room
 - capable of responding with sufficient time available for the operator to determine the need for protective actions even with indicators that may be malfunctioning due to the CCF if credited in the D3 coping analysis
 - appropriate for the event
 - supported by sufficient instrumentation that indicates
 - the protective function is needed
 - the safety-related automated system did not perform the protective function, and
 - whether the automated diverse means or manual action is successful in performing the safety function

Stakeholder Concerns from DI&C-ISG-2 Incorporated

1. Clarification on what constitutes adequate diversity, i.e., how much diversity is enough
2. Clarification when operator action is acceptable as a diverse means for addressing a CCF of automated Reactor Protection System functions
3. Clarification on Point 4 needed on component-level versus system-level actuation; and applicability to current NPPs
4. Clarification on consideration of effects of CCF on the protective function from “failure to actuate” and “spurious actuation”

Stakeholder Concerns from DI&C-ISG-2 Incorporated (continued)

5. Clarification on design attributes that are sufficient to eliminate consideration of CCF
6. Clarification on combining “echelons of defense”
7. Clarification on whether CCF is classified as a “single failure” in design basis event evaluations

Problem Statement from DI&C-ISG-02

1. Clarification on what constitutes adequate diversity, i.e.:
1) how much diversity is enough; 2) Are there precedents for good engineering practice; 3) Can sets of diversity attributes and criteria provide adequate diversity; 4) How much credit can be taken for design-in robustness in determining the appropriate amount of diversity; and 5) Are there standards that can be endorsed?

- BTP 7-19 as a whole and NUREG-6303 provides general guidance
- NUREG/CR-7007, “Diversity Strategies For NPP I&C,” developed
 - Developed jointly by NRC Research and Oak Ridge National Laboratory
 - Reports extensive study of diversity techniques world wide
 - Suggests an analytical method for numerically evaluating diversity
 - While well received, method has not had a sufficient “test of time” yet
 - Not included in Revision 6

Problem Statement from DI&C-ISG-02

2. Clarification when operator action is acceptable as an *independent* and *diverse* means to prevent or mitigate the potential CCF of automated RPS functions

potential

- Perform a D3 analysis of RPS using realistic assumptions
- If subject to potential CCF, need a *diverse* means to perform the safety function subject to the CCF
- Diverse means may be *automated or manual*
- Automated diverse means is preferred
- If manual means is selected as diverse means, acceptability is based on HFE analysis

Option for Manual Operator Action as All or Part of Diverse Means

- **BTP 7-19 Revision 6:**
 - If manual operator actions are used as the diverse means or as part of the diverse means to accomplish a safety function, a suitable HFE analysis should be performed by the applicant to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular AOO or postulated accident
 - The acceptability of such actions is to be reviewed by the NRC staff in accordance with Appendix 18-A of SRP Chapter 18, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," which has been reviewed by the ACRS; and is to be issued, but delayed due to higher priorities
 - Note is added to emphasize staff special concerns with using manual action as part of or all of the diverse means

Time Available & Time Required Understanding

The **time available** can be considered as the period between when an automated safety system fails to actuate (when actuation should have occurred) due to CCF, and the time when a substitute actuated system or safety function **must perform**.

The **time required** can be considered as the time required for a licensed reactor operator to **recognize** a failure due to CCF, **determine** actions needed, and then **accomplish** the needed safety function, including recovery from any operator error .

Special Note on Manual Action in Diverse Means**

“As the difference between Time Available and Time Required decreases, there can be increasing uncertainty in the estimate of time required for operator action. The uncertainty could invalidate a conclusion that operators can perform the action reliably within the time available. For actions with a limited margin of time to act, such as less than 30 minutes between the Time Available and the Time Required, a more focused staff review will be performed.”

** The preferred diverse means is an automatic system

Problem Statement from DI&C-ISG-02

3. Clarification on Point 4 needed on component-level versus system-level actuation; and applicability to current NPPs

- Diverse means performed on a system-level basis for each division to retain the policy in SRM on SECY 93-087
- Does not prohibit use of manual controls operating individual safety system components after the safety system function actuates
- Potential for CCF in digital safety systems should be considered in new plants and in upgrades to existing plants (backfit of current NPP equipment is not intended)
- Point 4 (set of displays and controls) expanded to clarify:
 - Safety or non-safety
 - List plant critical safety functions
 - If credited, a diverse means should function downstream of any CCF-affected component

Problem Statement from DI&C-ISG-02

4. Clarification on consideration of effects of CCF on protective functions from “fail to actuate” and “spurious actuation.”

- In general, spurious actuation is a lesser safety concern than failure to actuate because spurious actuations are usually annunciated and thereby immediately detected
- Spurious actuations of safety-related digital protection system resulting from CCF do not need to be addressed beyond what is already set forth in plant design basis evaluations
- Design of diverse automated or diverse manual means should address how to minimize the potential for spurious actuation of the RPS caused by the diverse means

Problem Statement from DI&C-ISG-02

5. Clarification on design attributes that are sufficient to eliminate consideration of CCF

- Diversity – Sufficient diversity in RPS
 - Evaluate on a case-by-case basis
- Testability – 100% tested
 - Every possible combination of inputs tested, and
 - Every possible sequence of device states tested, and
 - All outputs are verified for every case
 - Expected response known, tested, and found to be 100% correct

Problem Statement from DI&C-ISG-02

6. Clarification on combining “echelons of defense”

- *NUREG/CR-6303 Echelons of Defense*
 - Control system
 - Reactor Trip System (RTS)
 - Engineered Safety Features Actuation System (ESFAS)
 - Monitoring and indicators
- *RTS and ESFAS may be combined*
 - Four echelons are conceptual
 - Combining may introduce new CCF concerns
 - Need D3 analysis (acceptable method in NUREG/CR-6303)
 - If subject to potential CCF, need diverse means

Problem Statement from DI&C-ISG-02

7. Clarification on whether CCF Classified as a “single failure” in design basis event (DBE) evaluations

- CCF is not classified as a single failure (as defined in RG 1.53)
 - CCF considered beyond design basis
 - Digital RPS should be protected against CCF
 - Postulated CCF need not be considered a single failure in DBE evaluations
 - Analysis of CCFs coincident with DBEs can use realistic assumptions
 - Realistic assumptions are plant operating at normal power level (for the event), temperatures, pressures, flows for the event, with normal plant equipment alignment

Combining two manual initiation systems

- Two manual initiation systems may be needed
 - One ***required*** by IEEE Std. 603-1991 (safety-related)
 - One independent and diverse (safety or non-safety) needed per BTP 7-19, ***IE*** RPS manual initiation safety system subject to CCF
- Two manual actuation systems may be combined if
 - RPS manual actuation system is independent and diverse from automated RPS
 - Safety-related
 - Not subject to same potential CCF as automated RPS

Notable Public Comments and Staff Response

- In some instances comments led to additional clarification for clearer understanding and improved explanation
- Staff agreed with some comments in principle , but not with the specific rewording recommendations. Staff addressed them based on principle or accepted portion
- Staff agreed that not all RPS safety functions may be disabled by a CCF, but pointed out that assuming all RPS functions are disabled is a worst case bounding condition
- Based on digital operating experience, several comments challenged why CCF was considered beyond design basis; until there is a revision of the Commission policy, Revision 6 states that CCF is beyond design basis

Notable Public Comments and Staff Response

- A comment stated that the intent of BTP 7-19 is not to protect the digital safety systems, but to protect the plant; staff accepted the comment and addressed accordingly
- Staff accepted a comment expressing concern that after actuation of ESF functions from the MCR, the need may exist for some use of local controls later (e.g., 72+ hours after event)
- Comments challenged the concept that the diverse means had to be both independent and diverse; staff prepared a paragraph discussing independence

Notable Clarifications in BTP 7-19 Revision 6

- Based on ACRS letter on RG 1.62, *Manual Initiation of Protective Actions*, “system level” was changed to “system or division level (depending on the design)”
- IEEE Std. 603 requires manual initiation of automated functions. There is no requirement the manual initiation be independent from the automated actuation. If subject to same postulated CCF as automated functions, then an additional diverse means for manual initiation is needed.
- The use of the term “diverse backup method” was replaced with “diverse means” to match with the Four-Point D3 Policy and because some current NPP RPS portions termed “primary” and “backup”

Notable Clarifications in BTP 7-19 Revision 6

- The 100% testing definition was copied directly from DI&C-ISG-04
- A CCF that affects normal displays or controls should not prevent an operator from manually initiating safety functions
 - Guidance on prioritization of commands to an actuated component were copied from DI&C-ISG-04
- Since single failures concurrent with a CCF are not required to be postulated and normal equipment alignment is assumed, diverse actuation of one division is sufficient provided that division will be in service

BTP 7-19 Revision 6

Summary

- Revision 6 of BTP 7-19 is an extensive revision providing significant specific guidance in answering a number of stakeholder concerns
- It incorporates the current interim guidance in DI&C-ISG-02 Revision 2
- Revision 6 of BTP 7-19 is expected to be issued by September 30, 2011
- ACRS review and advice of this revision are appreciated

Questions?