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

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

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

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

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

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

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

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

(No response.)

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

A transcript of the meeting is being kept

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

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

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

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

MR. JUNG: Thanks, Charlie.

Good morning, members.

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

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

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

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

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

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

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

And with that, I will turn it over to Gene

Eagle.

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

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

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 the safety-related systems. Therefore, software-based or software-logic-based digital system development errors are a credible source for common cause failure. In BTP 7-19, software includes firmware and logic developed from software-based development systems.

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

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

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

MR. EAGLE: Yes.

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

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

CHAIRMAN BROWN: 087?

MR. JUNG: Right.

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

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

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

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

MR. JUNG: Right.

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

MR. EAGLE: Right.

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

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

design basis.

So, those are some general alignments on that argument.

CHAIRMAN BROWN: Okay. All right, go ahead.

Thank you.

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

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

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

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

The issue of diversity --

MR. EAGLE: Yes.

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

designs. That's just the way it was.

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

CHAIRMAN BROWN: Pardon?

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

CHAIRMAN BROWN: Oh, okay.

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

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

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

CHAIRMAN BROWN: Okay. I am just trying

to get --

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

CHAIRMAN BROWN: Yes, okay.

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

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

CHAIRMAN BROWN: Yes.

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

CHAIRMAN BROWN: No, I understand that problem exactly.

MR. EAGLE: Okay. Yes.

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

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

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

(Laughter.)

MR. STATTEL: Well, right.

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

MEMBER STETKAR: Like the whole plant?

CHAIRMAN BROWN: Like the whole system.

(Laughter.)

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

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

CHAIRMAN BROWN: Okay. Thank you.

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

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

Working Groups were formed.

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

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

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

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

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

The staff should determine the conditions

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

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

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

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

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

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

Go back just one moment.

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

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

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

MR. EAGLE: What?

CHAIRMAN BROWN: Say that 30-minute thing again.

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

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

MR. EAGLE: Okay.

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

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

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

MR. EAGLE: Yes, right.

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

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

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

CHAIRMAN BROWN: Okay.

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

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

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

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

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

MR. STATTEL: Okay. We understand that.

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

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

a strong basis.

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

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

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

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

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

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

operator action as a diverse means.

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

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

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

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

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

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

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

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

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

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

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

DR. HECHT: Okay. Thank you.

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

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

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

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

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

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

CHAIRMAN BROWN: Question?

MR. EAGLE: Yes.

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

MR. EAGLE: Yes.

CHAIRMAN BROWN: We have automated protection systems.

MR. EAGLE: Right.

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

MR. EAGLE: Yes.

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

MR. EAGLE: Right.

CHAIRMAN BROWN: And that's allowed.

MR. EAGLE: That's allowed.

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

MR. EAGLE: Right.

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

MR. EAGLE: Right.

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

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

CHAIRMAN BROWN: Okay. All right.

MR. STATTEL: Very simply, there are two

distinct requirements regarding manual operations.

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

CHAIRMAN BROWN: That's okay.

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

CHAIRMAN BROWN: Okay.

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

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

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

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

MR. STATTEL: It does.

CHAIRMAN BROWN: But that doesn't dictate

how --

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

CHAIRMAN BROWN: Yes.

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

CHAIRMAN BROWN: Or trip the breakers --

MR. STATTEL: Right.

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

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

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

MR. STATTEL: That is one requirement, right.

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

MR. STATTEL: Yes, it is.

CHAIRMAN BROWN: Okay. I'm trying to

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

MR. STATTEL: Right.

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

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

CHAIRMAN BROWN: Yes, I understand. Okay.

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

CHAIRMAN BROWN: Okay.

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

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

MR. EAGLE: Okay.

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

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

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

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

DR. HECHT: Can I just ask a question?

MR. EAGLE: Yes.

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

MR. EAGLE: Do you want to answer that?

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

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

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

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

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

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

DR. HECHT: Yes.

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

DR. HECHT: Okay.

MR. JUNG: That was the genesis of that.

DR. HECHT: Right.

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

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

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

So, that is the one option. If somebody

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

DR. HECHT: Thank you.

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

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

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

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

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

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

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

MR. STATTEL: Okay.

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

the Chapter 15 accident analysis.

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

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

MEMBER STETKAR: I'm talking about zero power.

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

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

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

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

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

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

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

MR. EAGLE: Right.

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

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

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

MR. STATTEL: Yes.

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

MR. STATTEL: Right.

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

And those systems know whether you are at power. They know power levels. They know whether you are shut down. They invoke certain algorithms when you are shut down. They invoke different algorithms when you are at power.

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

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

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

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

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

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

MEMBER STETKAR: Okay.

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

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

MR. STATTEL: Right.

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

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

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

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

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

MR. JUNG: I understand.

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

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

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

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

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

MR. STATTEL: For a Chapter 15 accident.

MEMBER STETKAR: -- for the Chapter 15 accidents?

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

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

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

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

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

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

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

necessarily restricted to power levels above zero.

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

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

MEMBER STETKAR: Precisely.

MR. STATTEL: Right.

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

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

MEMBER STETKAR: Right.

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

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

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

MR. STATTEL: It's the SAR.

MR. EAGLE: Yes, the SAR.

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

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

MEMBER BLEY: And we have added regulatory requirements.

MEMBER STETKAR: And we have added

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

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

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

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

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

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

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

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

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

MR. STATTEL: I see. I see.

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

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

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

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

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

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

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

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

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

MR. EAGLE: Right.

MEMBER STETKAR: Somebody has to take the

first step somewhere.

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

(Laughter.)

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

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

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

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

MEMBER STETKAR: Thanks.

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

If the D3 analysis indicates a potential

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

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

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

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

MR. EAGLE: Right.

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

to have some diverse method.

MR. EAGLE: Exactly.

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

MR. STATTEL: Correct.

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

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

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

(Laughter.)

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

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

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

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

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

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

CHAIRMAN BROWN: There is another slide on independence.

MR. EAGLE: Right.

CHAIRMAN BROWN: And I want to get to those.

MR. EAGLE: Right.

CHAIRMAN BROWN: That is about slide 17 or so.

MR. EAGLE: Yes.

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

MR. EAGLE: Yes.

DR. HECHT: In point 1 and point 3 of SECY 93-07 --

MR. EAGLE: Yes.

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

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

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

(Laughter.)

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

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

DR. HECHT: I see. Okay.

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

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

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

safety systems.

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

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

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

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

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

by point 3.

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

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

MEMBER STETKAR: Just for clarification, Gene --

MR. EAGLE: Yes.

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

MR. EAGLE: Right.

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

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

MR. EAGLE: Exactly.

MEMBER STETKAR: Okay. Thanks.

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

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

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

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

MEMBER BLEY: Much less for some plants.

MEMBER STETKAR: Much less for some plants.

(Laughter.)

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

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

MEMBER STETKAR: Okay.

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

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

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

Thanks.

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

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

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

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

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

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

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

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

required, per Clause 5.6.

MR. STATTEL: This issue --

CHAIRMAN BROWN: Let me finish.

MR. STATTEL: Okay.

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

MR. STATTEL: Okay.

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

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

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

MR. STATTEL: Right. This came up during

our discussions and with resolving the comments from industry.

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

CHAIRMAN BROWN: You just lost me with that statement.

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

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

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

fork you take in that path.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MR. STATTEL: Right.

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

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

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

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

CHAIRMAN BROWN: I'm not there yet.

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

CHAIRMAN BROWN: That may be the case.

MR. STATTEL: Right.

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

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

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

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

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

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

systems --

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

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

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

MR. STATTEL: That wasn't our intent.

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

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

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

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

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

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

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

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

(Laughter.)

MR. EAGLE: Okay.

MEMBER BLEY: Maybe at the break.

CHAIRMAN BROWN: Pardon?

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

CHAIRMAN BROWN: I'm happy with that.

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

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

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

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

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

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

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

MR. STATTEL: Well, in that condition

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

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

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

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

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

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

CHAIRMAN BROWN: Let John --

MR. STATTEL: I'm sorry.

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

MR. STATTEL: Okay.

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

In acceptance criterion 3.4, if you want

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

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

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

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

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

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

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

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

(Laughter.)

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

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

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

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

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

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

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

MR. STATTEL: Well, as we have stated,

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

MEMBER STETKAR: No, there wasn't.

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

Now I'm just conjecturing here.

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

MR. STATTEL: Right. Exactly.

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

So, the question is, if an applicant were

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

MR. STATTEL: Correct, yes.

MEMBER STETKAR: Not continuously.

MR. STATTEL: Right.

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

MR. STATTEL: I would say yes.

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

MR. STATTEL: Yes. I would say yes.

MEMBER STETKAR: Okay.

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

MEMBER STETKAR: Yes. Okay.

MR. STATTEL: Right.

MEMBER STETKAR: Okay. Thanks.

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

MR. EAGLE: Okay. I stand corrected then.

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

find that there.

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

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

Okay? So, one of the objectives --

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

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

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

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

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

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

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

All right, I got it. Go ahead.

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

(Laughter.)

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

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

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

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

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

CHAIRMAN BROWN: Okay.

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

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

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

MR. STATTEL: Yes.

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

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

DR. HECHT: Right.

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

DR. HECHT: Right.

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

DR. HECHT: Right.

MR. EAGLE: Right.

MR. STATTEL: In reality, I have never

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

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

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

MR. STATTEL: Right. Exactly.

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

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

MEMBER STETKAR: Okay.

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

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

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

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

MR. STATTEL: Yes.

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

MR. STATTEL: Locally?

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

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

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

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

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

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

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

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

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

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

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

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

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

DR. HECHT: Right. Yes.

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

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

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

MR. STATTEL: That is a little bit more

clear than the actual text, yes.

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

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

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

DR. HECHT: Okay. All right.

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

CHAIRMAN BROWN: You will pay the price.

(Laughter.)

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

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

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

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

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

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

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

MEMBER STETKAR: Let me follow on.

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

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

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

MR. STATTEL: That's not the intent.

MEMBER STETKAR: Okay.

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

MEMBER STETKAR: Oh.

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

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

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

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

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

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

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

MEMBER STETKAR: Yes. Yes, yes, yes.

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

MEMBER STETKAR: Are they still working on that?

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

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

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

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

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

What we required them to do --

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

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

MEMBER BLEY: So, a guy would have to

stand there and hold it?

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

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

MR. STATTEL: Yes.

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

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

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

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

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

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

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

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

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

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

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

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

MEMBER BLEY: I understand.

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

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

MEMBER STETKAR: I guess coming back, that

is a real interesting actual example.

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

MEMBER STETKAR: Yes.

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

MEMBER STETKAR: Right.

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

MEMBER STETKAR: Okay.

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

But going back to your original question --

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

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

MEMBER STETKAR: -- we can't intervene.

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

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

MR. STATTEL: Right.

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

MR. STATTEL: Right.

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

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

right thing. We put procedural controls in place.

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

MR. STATTEL: Sure. Exactly.

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

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

MEMBER STETKAR: Current ones, that's true.

MR. STATTEL: Right.

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

MR. STATTEL: Yes.

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

MR. STATTEL: That's right.

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

override function --

MR. STATTEL: Sure.

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

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

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

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

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

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

MEMBER STETKAR: Precisely.

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

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

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

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

MEMBER STETKAR: And he can intervene.

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

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

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

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

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

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

MR. STATTEL: Yes.

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

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

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

CHAIRMAN BROWN: The meeting will reconvene.

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

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

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

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

MR. EAGLE: We were talking up here.

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

(Laughter.)

Go ahead, Gene.

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

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

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

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

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

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

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

MR. EAGLE: Yes.

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

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

CHAIRMAN BROWN: Yes. Okay.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MR. EAGLE: Right.

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

MR. EAGLE: Right.

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

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

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

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

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

MR. EAGLE: Right.

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

MR. STATTEL: I wouldn't presume to speak

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

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

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

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

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

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

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

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

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

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

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

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

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

MEMBER STETKAR: I understand that.

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

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

MR. STATTEL: Okay.

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

MR. STATTEL: Okay.

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

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

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

MR. STATTEL: Okay.

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

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

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

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

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

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

MR. STATTEL: Right.

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

MR. STATTEL: Yes.

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

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

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

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

MR. STATTEL: Right.

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

MR. EAGLE: We never said that.

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

MR. EAGLE: We didn't say that.

MEMBER STETKAR: Yes, you did.

MR. EAGLE: No, we said that --

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

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

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

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

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

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

MR. EAGLE: Right.

MEMBER STETKAR: And I asked you, on that

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

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

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

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

MR. STATTEL: Yes, it is.

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

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

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

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

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

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

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

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

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

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

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

to think much more about that.

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

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

MEMBER STETKAR: Yes.

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

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

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

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

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

MR. EAGLE: Right.

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

MR. EAGLE: Right.

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

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

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

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

And the staff will never ask them about that.

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

MR. JUNG: Rich, let me.

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

accident management guidelines, it is an iterative process.

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

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

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

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

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

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

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

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

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

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

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

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

wanted to hear all the dialog.

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

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

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

MEMBER STETKAR: Right.

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

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

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

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

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

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

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

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

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

CHAIRMAN BROWN: I'm sorry.

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

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

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

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

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

Now we go to point 4. That is a whole

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

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

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

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

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

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

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

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

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

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

CHAIRMAN BROWN: Are we going to see that?

MR. EAGLE: What?

CHAIRMAN BROWN: Are we going to see that?

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

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

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

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

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

MEMBER BLEY: I think we saw ISG-05.

CHAIRMAN BROWN: We saw ISG-05.

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

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

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

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

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

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

MR. EAGLE: Yes, we would like to get the priority pushed up on that.

MEMBER BLEY: I do want to say, though, that I am glad in these various documents you have adopted the approach you have taken here in referring to that one and requiring an analysis rather than some arbitrary time limit. Some things are easier to do in one minute than others are in 30. So, an arbitrary time limit just didn't make sense. This is good -- if we like 18-A.

MEMBER SIEBER: Continuous control operation like regulating feedwater requires individual attention constantly from an operator. When you have four steam generators, it is very difficult for one operator to control level in four steam generators.

I don't think you have diversity amongst the feedwater control systems. And so, if you have a failure in one, what's the chances of having in all four?

And I know that, since I have tried this, you just can't do it without cycling the pumps, and you aren't going to do that very often.

MR. STATTEL: That's true. And that would be something that would be taken into consideration on the HFE analysis, the ability of the operator to perform that function.

MEMBER SIEBER: Yes, well, let's hope the HFE analysis is good enough to take into account what the real demand on the operator is because you don't typically staff the control room to be able to do that kind of a manual operation. It takes extra people to do it. You know, you have two operators. They are going to be busy if some big event is going on.

MR. EAGLE: One final thing is that we did go back and add a very special note to dealing with the diverse means. We would like to go into that note now.

The first thing to have a better understanding is the terms time available and time required. The time available, just to restate our understanding, is that time available can be considered as the period between when an automatic safety system fails to actuate, when the actuation should have occurred, due to common cause failure, and the time when a substitute actuated system or safety function must be performed. In other words, this must be performed when you are really getting into serious problems.

And the time required can be considered as the time required for a licensed reactor operator to recognize a failure due to a common cause failure,

determine actions needed, and then accomplish the needed safety function, including recovery from any operator error.

And this was the note that was placed in there to provide particular emphasis in looking at these 30 minutes or less or looking at human factors or looking at whether you need an automatic system.

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 the 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.

And this is the note that was included in BTP 7-19, Rev. 6, to try to give a little extra emphasis.

CHAIRMAN BROWN: This is largely a fallout of, I mean, we wrote a letter where we proposed all this.

MEMBER STETKAR: I've got a very specific comment on this.

CHAIRMAN BROWN: Yes.

MEMBER STETKAR: The first sentence says, "As the difference between the time available and time required decreases, there can be increasing uncertainty in the estimate of the time required for operator action."

The uncertainty in the time required for operator action does not depend at all on the difference between the time available and the time required. How long is required for me to pick up this coffee cup and bring it to my lips does not depend upon anything in terms of the time available to do that.

Now why am I hanging up on this point? The reason I am hanging up on this point is that this focuses strictly on the time required for a person to perform a particular action. It says that, when I have a small margin, I can have increased uncertainty in that parameter. That's not true. The uncertainty in that parameter is whatever it was.

In application, what people will do is they will focus entirely on that parameter because the Branch Technical Position focuses on that parameter. And you will see time/motion studies saying my thermal hydraulics analysis says I have 37.26 minutes to do

this. And, lo and behold, I have done these time/motion studies, and I can accomplish this with an error of plus or minus five minutes within 18.275 minutes, not recognizing that there might be uncertainty of about 15 minutes, plus or minus, in the 37-minute time available.

I guarantee you that people will focus only on the time required and not uncertainties in the time available.

MR. STATTEL: I guess I am not understanding the question.

MEMBER STETKAR: You're not, which it is fairly clear from the phrase in that note.

MR. STATTEL: I mean, if the difference is --

MEMBER STETKAR: Let me read you something.

MR. STATTEL: -- 30 seconds between time available and time required, you are telling me there is no difference in uncertainty than if there were five minutes?

MEMBER STETKAR: Suppose that --

MR. STATTEL: I have more confidence that the operator will be able to perform that action in the required time.

MEMBER STETKAR: Richard, suppose that the nominal scenario that I ran, my thermal hydraulics analysis, said there's 15 minutes available.

MR. STATTEL: Okay.

MEMBER STETKAR: But if I look at the range of scenarios and uncertainties, I might have 15 minutes plus or minus 10. I could have as small as five and as large as twenty-five. That is probably large uncertainty, but I will use that as an example.

MR. STATTEL: Okay.

MEMBER STETKAR: If I use the 15 minutes as my target, and now do a very detailed analysis to say that I have high confidence that I can do it within that 15 minutes, I am not addressing all of the uncertainties.

MR. STATTEL: I guess where our differences are are where you apply uncertainties. To me, the certainty is a confidence level that the operator will perform within the required time, within the 15 minutes. That's the way I'm thinking.

What you're thinking is the uncertainty is what is actually required.

MEMBER STETKAR: The uncertainty is, can the operator perform what is required within the context of the scenario --

MR. STATTEL: Right.

MEMBER STETKAR: -- that demands that action?

MR. STATTEL: Okay.

MEMBER STETKAR: Okay? And there are two parts of the uncertainty.

Now let me read something. I would just like to read this into the record. You guys can read the transcript. It keeps the same intent, I believe, but defocuses the one parameter. And as I read through this -- let me just read a proposal.

"As the difference between time available and time required for operator action decreases, uncertainties in the estimates for both of these times must be evaluated carefully. These uncertainties could invalidate a conclusion that operators can perform the action reliably within the time available. For actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed."

Now what I read says there are uncertainties in both of those parameters, and you need to be aware of both of those levels of uncertainty and be careful about both of them as the margin decreases, which I think is the intent, the

fundamental intent of our comments in our letter.

The only reason I bring this up is I don't want either applicants or the staff to focus solely on detailed time/motion studies of the time required to perform a particular action and ignore the possible uncertainties and the fact that the time available for that action could also have large uncertainty in it.

MR. EAGLE: But I think the time available comes much closer to being a constant. In other words, you establish first the time available because this is the time between when an automatic function should have operated and, all of a sudden, you've got serious problems. And I think you really need to define that first.

There may be some uncertainty in that, but it is much closer to being a constant once you have done your studies or looked at it. And then, it is the operators where probably the greater uncertainty may be located. Because we notice here, we mention the fact that it has got to cover a number of things here that may be not quite pinned down as much, including, for example, what happens if the operator made an error. He first has to recognize that he has a problem. And if we assume that the common cause failure has taken out a lot of his instrumentation, it

may be a moment before he recognizes that.

Then, he has to determine his actions, and he may be under pressure. There may be mistakes made. And so, this is, to me, really where the real uncertainty is.

I think if you look at the percentage of uncertainties in the two different items, it would be, seriously, the larger and the most significant uncertainty would be in the time required. Because, basically, the time available is going to be kind of like almost defined as a constant once you have looked at it.

MEMBER BLEY: Dr. Stetkar challenged your assumption about that, and I agree with him because the time available depends on the exact scenario you were going through. Some of them have shorter times; some have much longer.

MR. EAGLE: That's true.

MEMBER BLEY: So, all he is saying is you need to warn people to be careful about potential uncertainties in the time available, and I certainly agree with him.

MR. STATTEL: I understand your point and it is well-taken. I think there is a poor choice of words here, honestly.

MEMBER STETKAR: I think that the sense --

MR. STATTEL: Our objective -- I just want to articulate this -- our objective was really to establish a means of getting to a reasonable assurance determination. That was our objective.

I think there was a poor choice of words there, in fact.

MEMBER STETKAR: I think the intent is really clear. And I actually like the intent. It is simply thinking ahead about where people, both applicants and reviewers, will focus their effort. I believe that the words could be revised a bit to kind of head off a possible too much of a focus in one area without at least some sort of acknowledgment in the other area.

MR. STATTEL: Understood.

MEMBER STETKAR: And again, it is especially important when those margins start to get fairly small. But that is exactly where people are going to be doing the more in-depth analyses. It is exactly where the staff is going to be putting more effort and time into their reviews and asking a lot more questions. So, those are the areas where we want to be pretty careful to --

DR. HECHT: Isn't this really like just a

stress strength analysis where you have uncertainty --

MR. EAGLE: Yes, it is the same thing.

DR. HECHT: -- on the stress. And so, if you have uncertainty on the time available, and you have uncertainty on the time required, Gene, I think you feel that the uncertainty on the time available is much less, but you can still put some kind of a sigma on that. And then, you can just use that same equation for margin of safety.

MR. EAGLE: But, again, I would like to point out, going back to it, that you are establishing the time available. It is true certain areas will be different times available. But that has to be established first as the time available. And that, basically, is, when do we get into real serious problems? And obviously, there would be a little bit of plus and minus, but I think that margin of uncertainty will be fairly small --

MEMBER BLEY: That's what we are disagreeing with. You're saying the same thing. We disagree with your point on that one.

MEMBER STETKAR: Yes, we have seen from some of the PRA things that we have done that, when you depart from the specific design-basis accident scenario and ask questions about, well, these other

conditions could be occurring, they are not considered in part of the design-basis accident because you have had to consider a simultaneous loss of offsite power. You have had to consider the specific power level. You have to consider very many things that precisely determine that scenario.

When you get a little bit away from that, some of the times in terms of the time available, some of the rates at which levels change, can be affected by those assumptions. And indeed, for some types of scenarios, those uncertainties may be rather small; for other types of stylized scenarios, they might be actually fairly large compared to estimated operator response times.

MR. STATTEL: I think what is on a sliding scale is not the degree of uncertainty. That can be established. What is on a sliding scale would be the degree or level of assurance that you have that the operator --

MEMBER STETKAR: Of that margin, that's it.

MR. STATTEL: Uh-hum.

MR. JUNG: John, I think your points are well-taken. We will --

MEMBER STETKAR: Read the quote that I

have put in the record.

MR. JUNG: We agree with the sentence, that sentence is not --

MEMBER STETKAR: I don't think it changes the intent at all. It just may refocus some of the efforts, both on the part of the applicant and in terms of the review.

MR. JUNG: If you look at this note, you know, the time available, the time required, manual action, all that is actually human factors engineering evaluation; that is covered.

The way I look at it is a more focused review. Remember, we are in a BTP 7-19 digital I&C design review. What we are saying is those manual actions are relied on. Human Factors will do all the margin analysis.

In addition to that, digital I&C, in general, is going to make sure those systems that are being relied on, manual controls and all of that, we are going to do a more focused review to make sure those improvements relied upon are really a good quality and meet independence and all that. That was the main intention here.

And then, there is a human factors engineering piece it has to meet in 18-A.

MR. STATTEL: Right. Without putting a number to it. Because once you put a number to it, as you stated, I mean, the actions can be complex and they can take longer than --

CHAIRMAN BROWN: When we discussed this in our report on 1.62, Reg Guide 1.62, and we mentioned this time available as the time gets shorter, the difference gets shorter, we didn't get into defining the nuances of time available and time required in other than a conceptual manner.

And I believe it was cranked into, it is in 1.62 now, as it was issued, if I remember correctly. This roughly follows with some additional definition that has now been applied, which raises some questions.

We ought to try to get this resolved before 7-19 goes out, is all the point I would like to make on this. However we come out, I think we would like to see something before, how we resolve this one way or the other.

MR. EAGLE: By the way, we didn't include these definitions in there, partly because they are covered elsewhere.

CHAIRMAN BROWN: Oh, I know. Well, I presume they are going to be in 18-A --

MR. EAGLE: Yes.

CHAIRMAN BROWN: -- if I'm not mistaken, which we will then see.

So, you're right -- well, we will have to make a decision on how we go on that.

MR. EAGLE: Yes, the note is in there, but not the definition.

CHAIRMAN BROWN: I understand that. Yes, I read --

MR. EAGLE: It would depend on that kind of vagueness that you, the rough understanding --

CHAIRMAN BROWN: Okay. Move on. Okay.

MR. EAGLE: Point 3, problem statement 3, was a clarification on component-level versus system-level. This goes back into some of the things we have been talking about. The diverse means is performed in a system-level basis for each division to retain the policy in the SRM, SECY 93-087. It does not prohibit the use of manual controls operating individual safety components after the safety system functions have actuated.

A potential for common cause failure in digital safety systems should be considered in new plants as well as in upgrades to existing plants. However, there is no intent to have a backfit of

current nuclear power plants at this time.

Point 4, set of controls and displays, safety or non-safety. They list plant-critical safety functions. And if credited, here again, if credited as a diverse means, it should function downstream of any common-cause-failure-affected components.

Problem statement 4 was a clarification on the consideration of effects of common cause failure on protective functions from fail to actuate and spurious actuations. 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 systems resulting from common cause failure do not need to be addressed beyond what is already set forth in plant design-basis evaluations. The design of diverse automated or diverse manual means should address how to minimize the potential for spurious actuations of the reactor protection system caused by the diverse means.

MEMBER STETKAR: I need to weigh-in here again. What technical basis do you have for the statement that says, "Spurious actuation is a lesser safety concern than failure to actuate"?

MR. EAGLE: Okay.

MEMBER STETKAR: What analyses have you performed to justify that statement? Because it appears in a couple of places in the Branch Technical Position.

MR. EAGLE: Okay.

MEMBER STETKAR: So, if you can give me a reference, I will go read those.

MR. EAGLE: I can't give you a reference right now.

MEMBER STETKAR: I would like one, if you have one.

MR. EAGLE: Basically, the concept is that spurious actuation will be noticed and action can be taken.

MEMBER STETKAR: We have both deterministic and probabilistic regulatory guidance for fire analysis that spends a lot of effort looking at the effects of multiple spurious actuations. They are called multiple spurious operations in that context.

That regulatory guidance explicitly states that there is no limit on the number of multiple spurious operations that must be evaluated and that the designs of those protection systems or alternate

mitigation functions, however you want to characterize them, must explicitly account for those multiple spurious operations without regard to whatever analyses have been done in the deterministic accident analyses.

So, I'm curious how these statements saying that, for a common cause failure -- by the way, fires, for the record, are also considered to be beyond-design-basis events. So, I am working in the same space here.

I'm curious how this guidance under BTP 7-19 is consistent with the guidance that we have for both deterministic and probabilistic evaluation of fires in a nuclear plant.

MR. STATTEL: Well, these positions were established as part of a Working Group 2, ISG-02, development process, as you are aware.

MEMBER STETKAR: Yes. And I think we commented pretty significantly about this one there, too.

MR. STATTEL: Well, at the time when the Working Groups were meeting, there was an argument and counterargument from the industry where the consequences of the spurious actuation could outweigh the benefits of having the diverse system, right?

And I think -- and I can't really speak to the basis of the final wording that is in here -- but I think the NRC took a position to basically avoid that argument, right? In other words, I don't want to put a diverse system in because it can increase the probability of inducing a spurious failure, which could result in a LOCA. If you initiate safety injection, you could fill up the pressurizer and go solid, right?

Use the probabilities of that to outweigh the benefits of having the diverse system. We are kind of avoiding the probability argument.

MEMBER STETKAR: And I don't want to get into a probability argument right now.

MR. STATTEL: But I think that is the reason why these words are this way.

MEMBER STETKAR: Let me step you back, though. I am not talking about design of the diverse system.

MR. STATTEL: Okay.

MEMBER STETKAR: Just forget the diverse system for a moment.

MR. STATTEL: Okay.

MEMBER STETKAR: And just look at the D3 analysis for my existing protection system. I need to

do a D3 analysis for my existing protection system and evaluate the effects of possible common cause failures in that system.

And I use that analysis as a basis, then, for defining the functions, whether they are manual, whether they are safety-related, automatic, non-safety-related, of my diverse system.

MR. STATTEL: Right.

MEMBER STETKAR: So, forget the diverse system now. Just think about the D3 analysis that I need to do for my existing protection system. This tells me that I do not need to look at spurious actuations within that context, as I understand it.

MR. STATTEL: Well, spurious actuations are a reality even with analog systems. It is not just a phenomena for digital systems.

And the second point here points out that the requirements to avoid the consequences of spurious actuations is set forth in the plant design basis.

MEMBER STETKAR: Okay.

MR. STATTEL: It is covered in the plant design basis evaluations.

MEMBER STETKAR: I wanted to hear you say that.

MR. STATTEL: Where argument from the

industry came in was that, by adding the diverse system -- and I know you want to push it off to the side, but that was really the crux of where this language came from -- by adding a diverse system in on top of the safety system, by definition, that diverse system has some potential, however small it is, for spuriously actuating the safety function, right?

So, having two systems that can potentially spuriously actuate is obviously going to have a larger probability than one, right? By definition, you are always going to be increasing the probability of causing a spurious actuation.

MEMBER STETKAR: I have met an awful lot of really smart designers in my life.

MR. STATTEL: Uh-hum.

MEMBER STETKAR: And given a problem, knowledge of a particular problem, it has been my experience that designers can get pretty creative about how to design something that works around that problem. And that is why I want to push off the diverse system for the moment.

MR. STATTEL: Okay.

MR. EAGLE: That is point 3, by the way. And actually, there are two different types of spurious actuations we are talking about. The first

two deal with those caused by the common cause failure. The second one is the one caused by the diverse system, which you want to push aside.

So, basically, what we are really probably talking about is those first two bullets.

MEMBER STETKAR: That's exactly right.

Now the second bullet is kind of a paraphrase of things that I have read. In Section 3.7 of the BTP, the actual quote is, it appears in Section 1.8 and 3.7, but 3.7 is the acceptance criteria.

It says, "In general, spurious trips and actuations are of a lesser safety concern than failures to trip or actuate. There may be plant and safety system challenges and stresses. However, challenges that are significant are already set forth in plant design-basis evaluations." That sort of points to that second bullet.

However, I will ask you, does the plant design-basis safety evaluation for a small LOCA event consider, for example, a simultaneous steam line break event? The answer to that is, no, it does not.

However, if a common cause failure of my integrated protection system during a small LOCA event can rapidly blow down automatically all four of my steam generators, giving me something that looks

like -- because they blowdown valves are large enough to, for example, take 110 percent of full reactor power -- that type of event is not evaluated in the design-basis safety evaluation. So, I can't say that it is bounded by a steam line or it is bounded by a small LOCA. It is just simply not evaluated. It is something that my integrated protection system can do.

And I have a couple of other examples here, but in the interest of time, I won't mention them.

Now, if I am not required to think about that type of an event when I do, as an applicant, my D3 analysis, then my designers don't know about those conditions. So that, when they design the diverse system, they may include protections against that, recognizing that the diverse system could also have some of its own spurious actuation concerns associated with it.

But because of those types of events, conditions --

MR. STATTEL: But for those systems, we would expect a failure modes, an effect analysis to be performed, and for safety systems, a hazards analysis. And that becomes part of the design basis for those systems.

And it is a presumption that the spurious actuation aspects of a system, those failure modes, are to be considered in the denial.

MEMBER STETKAR: Yes, but, typically, they only do a single channel failure mode. They only do a single failure mode. They rely on the diversity.

MR. STATTEL: Okay. You're talking about common cause failure?

MEMBER STETKAR: They rely on the D3 stuff. I'm not worried about a single channel, you know, a single relief valve opening. I am worried about the system opening all relief valves.

MEMBER BLEY: But, I mean, we are putting the system in to take care of common cause failure. So, if, in fact, the system can generate accidents we have never seen before, and these words tell you not to look for them -- well, not these words; the other words you had -- tell you not to look for them, then that is troublesome.

I understand the argument that you didn't want to dismiss these systems, but it seems that, if you have them, you ought to look for potential harm they could do and fix it, not say, "I don't want it" because of that.

MR. STATTEL: But I think that was the

intent of the second bullet, that those failure modes would be considered.

MEMBER STETKAR: I've got two or three other examples, but in the interest of time, I just brought up the steam line break with small LOCA because it is one.

And I hate to do this because I always tell people I am not an attorney and don't want to be an attorney, but it is also notable that the lead-in to this was that we do explicitly require people to look at and evaluate, explicitly evaluate, the effects from multiple spurious operations in all of our fire regulatory guidance. And I don't understand why, if the potential consequences of multiple spurious operations are important enough to require an evaluation for fires, why they are not important enough to merit an evaluation under the context of integrated digital protection systems.

There are a lot of analogies between fires and what can happen in fires and the things --

MR. STATTEL: I understand. I am sure those discussions were held when ISG-02 was presented.

(Laughter.)

CHAIRMAN BROWN: Hold it.

MR. STATTEL: But our task --

CHAIRMAN BROWN: Hold it.

MR. STATTEL: But our task was to incorporate the results of that.

CHAIRMAN BROWN: Richard, we've got 10 more slides to go. So, we have got to move along here.

MEMBER BLEY: Can I say one more thing, back on the slide you were on?

CHAIRMAN BROWN: Of course.

MEMBER BLEY: We have been talking about bullet 2. Bullet 3 says, well, for tripping a reactor, we want you to minimize the potential. If we said that same word under bullet 2, I don't think I would be as concerned.

MR. JUNG: Just one context is, remember, the safety system is pure saturation. You know, design-basis evaluation is one aspect. But you have to think about, what is required to be high-quality safety-related software systems? Now you are talking about 603 requirements apply. Members heard about systematic life-cycle process that it needs to go through.

What I am saying is there is a significant set of requirements in place to minimize the potential reliability concerns over the safety systems

themselves. That is, actually, a majority of our review. We focus on safety system designs themselves. From architecture, from software development, life cycle, redundancy, and functional diversity, all that is in place.

So, it is not like there is no, absolutely no measure for the quality because, eventually, software causing spurious actuation means there are some quality concerns out of nowhere. We are not even talking about -- remember, the policy says the design-basis event concurrent with a common cause failure.

But this particular one actually we discussed even beyond the policy scope. What if there is no initiating event in place? You know, your normal condition; suddenly, something takes place. Because of software common cause failure, there is a question about what is the trajectory; what initiates that? Because software reacts to it when something triggers it.

So, we had these discussions multiple times. It is not really clear. But I want the Members to be aware there is significant quality requirements for the software themselves that provide certain reasonable assurance that may address this concern.

MR. STATTEL: And there are some relevant precedents as well. As you know, in boiling water reactors, they all have the depressurization function. And it was recognized very early on in that design that the consequences of actuating those squib valves was very severe.

And in response to that, the design of that system incorporates some arming functions that prevent, that are specifically designed to prevent spurious actuations of those systems. And that has been very successful to date, those techniques that they applied.

So, really, that is the type of design process and design-basis capturing that we are alluding here. Those weren't driven. Those designs were not driven by regulations. Regulations did not drive General Electric to incorporate those measures. It was really more addressing the failure modes that existing in that system.

MR. EAGLE: We want to go on to slide 5.

This is clarification on design attributes that are sufficient to eliminate consideration of common cause failure. There have been many attributes that would be very helpful, particularly like high-quality software, V&V, all kinds of tests and

everything, that could be used to help reduce the probability of a common cause failure software failure.

However, there are two that could be identified, but either one of them would be sufficient to eliminate consideration of common cause failure. One of them would be if there is sufficient diversity in the reactor protection system, and this is evaluated on a case-by-case basis. Again, the analysis, as it goes through, should be able to identify that you have sufficient diversity at that point.

The second one is testability. And we are again quoting from ISG-04, the 100 percent testability. If every possible combination of inputs tested, and every possible sequence of device states tested, and all outputs are verified for every case, expected responses are known, tested, and found to be 100 percent correct, then the testability requirement has been met. That could help eliminate the idea of a common cause failure of that component or that group of components.

DR. HECHT: Can I ask a question about this?

MR. EAGLE: Yes, yes.

DR. HECHT: Is this with respect only to actuation or with respect to subsequent control? So, for example, what we have been talking about, an injection system or an aux feedwater system, or something like that, if the only issue is turning the pumps on, that a single-shot action. The requirements of 100 percent testing might potentially be met. But if the function goes on to subsequent monitoring and closely controlled, then it is not possible.

But does the testability, would it be a feasible, licensable disease that I can do something which only actuates, thereby, avoiding the subsequent need for closed-loop control, and then get it licensed without the need for diversity if I can do 100 percent testing?

MR. STATTEL: What I would say is it depends. The answer to that, it depends on the specific design. The intended applicability is to ensure performance of the safety function. If the safety function is defined as just actuate, and it doesn't include the followup action in the safety analysis, then it wouldn't include it. If it does include that followup action, as was stated earlier with integrated systems, then I would expect that it would be included in this.

MR. EAGLE: Yes, for example, if your device was so simple that the only thing you had to do was take several inputs and do an output, then that probably could be 100 percent tested. But if that device has to feed into some other group of devices and has to have more complex type types, then it is probably unlikely you are going to be able to do 100 percent testing. And therefore, you would need to take a look at common cause failure.

DR. HECHT: Does the guidance here reflect concerns about corrupted input or spurious inputs or things like that as part of that?

MR. EAGLE: It says, "Every possible combination of inputs."

DR. HECHT: So, that would include corruption?

MR. EAGLE: That would include --

MR. STATTEL: This gets very difficult. This criteria gets very difficult to meet as soon as you --

(Laughter.)

MEMBER STETKAR: Once you look at that "every possible combination" phrase.

CHAIRMAN BROWN: Once you have more than one line of code, you're lost.

DR. HECHT: As long as that is understood, I'm --

CHAIRMAN BROWN: Yes, I think this is a throwaway.

MEMBER STETKAR: I wouldn't expect many people to invoke that.

MR. STATTEL: Even with the Wolf Creek application, which was a main steam and feedwater isolation function, it was receiving a digital input and simply sending a digital output to those valves. But even in that case, the 100 percent testability argument, actually, when you did the math, it became a lot of iterations of testing. And because of that, we --

CHAIRMAN BROWN: Well, you have got to test every possible form of that data that comes in under corruption and everything else.

MR. EAGLE: Sorry.

(Laughter.)

CHAIRMAN BROWN: No, that's okay. That's all right.

MR. EAGLE: Some of these are almost like apple pie and motherhood. So, we will move through these slides very quickly.

Another condition that came up was the

echelons of defense. As you know from 603, it talked about four items of what we call echelons of defense, the idea that the operator is our main control with his hands-on manual controls. If that fails to stop something, you have the reactor trip system. You have the engineering safety features that are supposed to automatically come in. A fourth line of defense is the monitoring indications. These were pointed out as actually being conceptual more than absolutely hard, fast divisions.

Combining maybe introduced new common cause failure concepts. Remember that, originally, you had the silos of the analog, each analog channel coming through for various types of parameters. If one of those failed, you had four different divisions, and you had one channel fail, but you still had the rest of that division intact.

Once you combine all those parameters together in some kind of digital system, now if you lose that digital system, you have lost that entire division. However, in a common cause failure, you could lose the entire four divisions. So, you do definitely have different types of interactions when you have common cause failure.

A D3 analysis, acceptable methods is done

through 6303. It is subject to a potential common cause failure. A diverse means needs to be provided.

CHAIRMAN BROWN: Before you leave this --

MR. EAGLE: Yes?

CHAIRMAN BROWN: Just from where I come, I got wrapped around the axle on this whole issue of combining into a single computer --

MR. EAGLE: Eight.

CHAIRMAN BROWN: -- both the ESFAS, EFS, EFAS, ESFA, however you want to call it, and the reactor trip system, and you all make this specific comment in here: NRC regulations do not require, nor does this guidance imply, that the echelons of defense must be, the RTS and ESFAS echelons must be independent or diverse from each other with respect to CCF.

What?

MR. STATTEL: That's just a true statement.

(Laughter.)

CHAIRMAN BROWN: Well, I love true statements, but, I mean, why would you ever accept a combined system? I mean, I just almost fall off the cliff thinking that you would ever accept a combined system where, instead of a reactor trip system, which

has got its four divisions, and an ESFAS system, where it has got its four divisions, they are separate, and now I am going to stuff them into one thing.

I have reduced my baskets. I have gone from eight baskets, if you want to call it that, down to four baskets. And the more you lump stuff into one area, the more likelihood you have of nailing yourself to the wall on some type of a failure that locks everything up.

MR. STATTEL: The reason it is written this way is to purposely not be prescriptive and drive design.

CHAIRMAN BROWN: Why not?

(Laughter.)

MR. STATTEL: Well, I mean --

CHAIRMAN BROWN: I think you are bending over backwards to the point of just saying, well, gee, we'll accept anything as long as it is not so ugly that I don't have to put a mask over it.

MR. STATTEL: Well, in the case of Oconee, they did combine echelons of defense. So, the same process --

CHAIRMAN BROWN: Yes, I know; that one slipped by me.

MR. STATTEL: However, when they performed

their diversity analysis, the postulated failure mode was a loss of all of those functions simultaneously in all four divisions. So, as long as they follow that analysis through, it is hard to come up with a regulatory means for denying the applicability.

CHAIRMAN BROWN: Well, why shouldn't I just have one division of something, put all the eggs in one basket? And therefore, I will define that as --

MR. STATTEL: It would have been a lot easier for us for sure.

(Laughter.)

CHAIRMAN BROWN: -- subject to CCF, and I will have a diverse, you know, so I will have two things instead of eight things. I mean, at some point, it is like the time difference between time available and time required. The fewer things you have to deal with, the more likely you are to screw stuff up.

MR. EAGLE: The counterargument to that, by the way, is the idea of digital equipment increasing the capability, better able to handle things, providing more efficiency --

CHAIRMAN BROWN: I am going to tell you, quite frankly, in 1978 I went out for my first

microprocessor-based system for an aircraft carrier. The vendor came in and said, "Gee, why do you have a microprocessor in every instrument? We can use, instead of 28, we can use four, and we can manage this entire protection system with four microprocessors," et cetera.

We looked at him and said, "You're nuts. We don't even know how to do anything in 1978, 1979, regarding safety system software," and threw him out of the office.

He never said a study. So, we had 28. It worked beautifully.

So, I mean, that whole idea, because of the capability, just does not hold water.

MEMBER SIEBER: They were all TRS80s.

CHAIRMAN BROWN: It was a Z80, as a matter of fact. Don't laugh.

MEMBER SIEBER: Right, I know.

CHAIRMAN BROWN: It was the only mill-qualified microprocessor in 1979.

MEMBER SIEBER: Pretty fast.

MR. STATTEL: The current state of affairs is we don't have a regulatory means for driving designs in that direction. That's the bottom line.

CHAIRMAN BROWN: All right. Go on.

DR. HECHT: But don't you still have the independence requirement for the diversity --

MR. EAGLE: Oh, yes, the four divisions.

MR. STATTEL: We do, and we do review these designs that combine these echelons to those requirements.

CHAIRMAN BROWN: Yes, I understand that.

We've got to get on. Let's go on. I have vented my spleen.

MR. EAGLE: This reemphasizes, Mr. Brown, the fact that we do need the common cause failure, the diverse means, because of the possibility of losing all those.

Problem statement 7 was clarification on whether a CCF is classified as a single failure in design-basis event evaluations. Again, CCF is not classified as a single failure, as defined in Reg Guide 1.53. It is considered beyond-design-basis.

Digital reactor protection systems, however, should be protected against common cause failure. That is basically the bottom-line theme throughout BTP 7, Revision 6.

Postulated common cause failures need not be considered as a single failure in design-basis evaluations. Analysis of common cause failures

coincident with the design-basis events can use realistic assumptions. And again, we define realistic assumptions.

And there was one additional one. We have actually already brought this up, but there was an additional item that came up. And this was where that there was actually possibility of two manual initiation systems.

Now IEEE 603 states basically that you are required to have a manual ability to initiate the automatic reactor protection system. But it doesn't say, other than saying you need a minimum number of components and this type of thing from the control room, it doesn't state that you have to be completely, that you can't go through the automatic system. So, if you do go through the automatic system, then there is a possibility you will need -- that system could be subject to a common cause failure and, therefore, would require a diverse means to initiate the manual actuations or manual initiations. Therefore, you would have two systems.

So, what would be the criteria you would need so we could only have one system? So, the two could be combined under these circumstances: the reactor manual protection activation system is

independent and diverse from the actual automatic reactor protection system. It has to be safety-related and not subject to the same potential common cause failure as the automated reactor protection system.

I believe that is what we discussed here shortly before.

CHAIRMAN BROWN: Okay. Yes. That just says, whatever it is, if your manual means goes through the processor, the computers, then you have got to have an independent, separate, manual actuation system. I mean, it may be an automated system, but it is a separately automated system. It is not necessarily analog.

MR. EAGLE: Well, now this is the manual system. In other words, right, if you have got those two buttons that scram the plant --

CHAIRMAN BROWN: Yes, I understand, but you have got the one that goes to the automated system, and the other one you haven't defined -- as long as it is independent --

MR. EAGLE: Right.

CHAIRMAN BROWN: -- from the primary safety system and it's diverse. It doesn't mean, because I haven't seen -- maybe I've missed them -- it

doesn't say it can't be software-based as long as it is suitably diverse from the primary software-based system. Is that --

MR. EAGLE: Correct.

CHAIRMAN BROWN: You haven't precluded that?

MR. EAGLE: Right.

MR. STATTEL: Depending on the design --

CHAIRMAN BROWN: Yes, okay. I just want to make sure I understood that nuance in terms of how you all were thinking about it.

MR. EAGLE: Yes, we used one example of saying one possibility would be like a hardwired system. It is just an example.

CHAIRMAN BROWN: Yes.

MR. EAGLE: But it could also be software, too.

Also, we received a considerable number of public comments, approximately 70. Ninety percent of them came from NEI. They are included in various information that was made available to the Committee. And we would like to point out some of the more notable ones.

In some instances, comments led to additional clarification for clearer understanding and

improvement.

Staff agreed with some comments in principle, but not with the specific rewording recommendations. Staff addressed them based on principle or accepted portion.

The staff agreed that not all reactor protection system safety functions may be disabled by a common cause failure, but pointed out that assuming all reactor protection system functions are disabled is a worst-case bounding condition.

Based on digital operating experience, several comments challenged why CCF was considered beyond-design-bases. And until there is a revision of the Commission policy, Revision 6 states that CCF is beyond-design-basis.

A comment stated that the intent of BTP 7-19 is not to protect the digital safety systems, but to protect the plant. The staff accepted the comment and addressed it accordingly.

The staff accepted a comment expressing concern that, after actuation of the ESF functions from the main control room, the need may exist for some use of local controls later. And for instance, just one example might be like beyond 72 hours, although maybe it might be shorter times and maybe

other special circumstances.

Comments challenged the concept that diverse means had to be both independent and diverse. We have discussed this. The staff prepared a paragraph discussing independence. That was in under, we talked about that one on page 7 concerning point 3.

Also, there were several notable clarifications in BTP 7-19, Revision 6, that were of interest. Based on the ACRS letter on Reg Guide 1.62, "Manual Initiation of Protective Actions," "system level" was changed to "system or division level," depending on the design.

IEEE 603 requires manual initiation of automated functions. There is no requirement the manual initiation be independent from the automated actuation. If subject to the same postulated common cause failure as automated functions, then an additional diverse means for manual initiation is needed. We, of course, talked about that as part of the extra item.

The use of the term "diverse backup method" was replaced with simply the "diverse means" to mach with the Four-Point D3 Policy and because some current nuclear power plants use the term in their main system called "primary" and "backup".

Again, the 100 percent testing definition was copied directly from ISG-04. A common cause failure 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 ISG-04.

Since single failures concurrent with a common cause failure are not required to be postulated and normal equipment alignment is assumed, diverse actuation of one division is sufficient, provided that one division is in service. That is somewhat of a caveat and oftentimes leads to a more complex system of the diverse, perhaps with several different subdivisions involved in the diverse method.

CHAIRMAN BROWN: Don't bother with 39 and 40.

MR. EAGLE: Okay. Okay.

CHAIRMAN BROWN: They are just a summary.

MR. EAGLE: Yes. Okay.

CHAIRMAN BROWN: I just wanted to do two things. First, relative to the comment on the independence issue, where you pointed me back to concerning point 3 on page 7 --

MR. EAGLE: Yes. Right.

CHAIRMAN BROWN: -- and a couple of the statements from industry on items 6, 7, 8, and 9, which we discussed earlier.

I see the words in concerning point 3. I went and read them as we were talking here. Yet, if I go back and I read the industry comments, they make very clear statements which seem to be inconsistent a little bit with -- I'm not saying what you don't have in concerning point 3 isn't there. To me, that's fairly clear. But, yet, they make statements there's no requirement for independence between automatic and manual functions. Okay? And then, they go on to say there's no need for independence to cope with common cause failures.

And you agreed with both of those. All four times you agreed with it, as they made that point repeatedly.

So, they deleted all those words of independence. I see this. I see your all's words about agreeing with that. And then, I look at the words over here where you have assuaged me somewhat relative to the thing by saying, really, you've got to have independence from your manual means --

MR. EAGLE: Right.

CHAIRMAN BROWN: -- one way or another

from your automatic systems. Forget about what you call it; you've got to have an independent operation. But, yet, they are saying you don't need independence.

So, I don't know whether comments and resolution of comments can come back to bite you sometimes, but that --

MR. EAGLE: Basically --

CHAIRMAN BROWN: Go ahead.

MR. EAGLE: Yes, basically, we were in agreement that, when you say "independence" and "diverse", that we agreed that basically both "and's" together, that they didn't necessarily have to be both independent and diverse, that diverse was obviously the main point. And that when they took over the independence as a separate look-see or a separate requirement, it covered the independence.

CHAIRMAN BROWN: But if I have an automatic system that is my primary system, and I am going to have a diverse, I am required to have a diverse system, doesn't it, by definition, have to be independent from the primary system?

MR. EAGLE: Basically, obviously, it is independent.

CHAIRMAN BROWN: But that's not -- that seems to be --

MR. STATTEL: Well, I think it was more of a clarification. If you read the original words --

CHAIRMAN BROWN: In?

MR. STATTEL: -- in what they were commenting on --

CHAIRMAN BROWN: Yes, I didn't see the originals.

MR. STATTEL: Right. The originals, based on what they were commenting on, it could be interpreted to literally impose requirements that didn't exist with regard to independence of the system, particularly when you were using a safety system to implement your diverse function, right? So, it was really more of a literal interpretation, and we provided the clarification and gave that dividing point between safety and non-safety.

CHAIRMAN BROWN: Okay. Let me phrase this another way. I have got four divisions of automated microprocessor, computer-based divisions.

MR. STATTEL: Yes, yes.

CHAIRMAN BROWN: And I have got a diverse manual system that is within that. In other words, it doesn't get compromised by CCF.

MR. STATTEL: Okay.

CHAIRMAN BROWN: Okay? Doesn't that imply

in some way that it is independent of the computer-based functionality of each division, within each division?

MR. STATTEL: Yes, it is implied in an automatic system and in a manual system, usually it implies independence. They're different systems.

CHAIRMAN BROWN: There is no need for independence to cope with CCF; that is a direct statement by industry four times. Okay?

MR. STATTEL: Honestly, I think it may be taken out of context a little bit.

CHAIRMAN BROWN: I'm just reading the words as you all phrased them in the --

MR. STATTEL: Well, right, but I think you really have to look at the original wording of the BTP.

CHAIRMAN BROWN: All right. I'll stop right there. I just want to make sure that the independence issue is of primary interest to me all the way along.

MR. EAGLE: Right. We basically agreed with industry that the idea of independence and diverse did not have to be linked together. Actually, the diversity by itself, and then the independence examination by itself --

CHAIRMAN BROWN: I, quite frankly, can't see how you can have one without the other.

MR. EAGLE: It depends on where it is.

CHAIRMAN BROWN: But I'm not real smart.

MR. EAGLE: But their claim was that, if you have, for instance, if you have four divisions of diversity, and they could be actually included in the safety divisions, but they would be there without being independent --

MR. STATTEL: Right, without being electrically independent.

MR. EAGLE: -- electrically independent, they could be in the same division. But they would be independent of each other, the four --

CHAIRMAN BROWN: When you say "electrically independent," okay, let's stop right there.

MR. STATTEL: Powered by the same source. They have the same power.

CHAIRMAN BROWN: I might work on that one a little bit.

MR. STATTEL: Well, they were; they are. They are.

CHAIRMAN BROWN: No, I understand that.

MR. STATTEL: So, I mean, that is

literally where the interpretation issues came up on those comments. Because the wording was originally written --

CHAIRMAN BROWN: Hold it. But if the power source cannot be compromised by the CCF --

MR. STATTEL: See, you're talking four divisions here.

CHAIRMAN BROWN: I understand.

MR. STATTEL: There's four divisions of the safety, and there's four divisions of the diverse --

CHAIRMAN BROWN: I'm just saying, but if they're all the same and they can't be compromised by the power supplies themselves feeding the diverse system, can't be compromised by the CCF, then, in fact, it can be considered to be independent from CCF. In other words, you have used independence to cope for CCF.

MR. STATTEL: But, I mean, if you make a statement that they have to have a different power source --

CHAIRMAN BROWN: I'm not saying that.

MR. STATTEL: But, I mean, if you made that statement -- this is akin to what was in the original wording -- if you make a statement that the

diverse system has to be independently powered by a different source, then that precludes me from implementing that within the safety systems because there are only four safety divisions.

CHAIRMAN BROWN: I got that.

MR. STATTEL: So, I have to use the same power source, right? So, we didn't want to --

CHAIRMAN BROWN: No, you don't have to. You can put separate power sources within each division to power that particular part of it. So, there is no preclusion of that. It just a matter of evaluating the whole system.

MR. EAGLE: I believe when designs are doing that, they have dual power supplies inside each division.

CHAIRMAN BROWN: Well, you could have two pairs of dual power supplies.

(Laughter.)

All right. Let me just finish up. I wanted to see if there are any open items here. I am not going to work on this one anymore, but John brought up the issue of the words on time available/time required. And I think you agreed to try to come up with a --

MR. STATTEL: We will look at his quote.

He gave us a quote.

CHAIRMAN BROWN: Yes, and see how that fits into the context.

MR. STATTEL: Right.

CHAIRMAN BROWN: I'm looking at my other notes. Where are the other notes?

The manual control and override. John had to leave for another meeting. So, I didn't see that as being open at this point, by the time we finished. I don't know how anybody else looked at that. There's a number of nuances that we went through in the discussion.

But, Dennis, do you? Or, Jack, do you?

MS. ANTONESCU: ISG-05.

CHAIRMAN BROWN: Doesn't some of that get covered by 18-A, when we get to that, in terms of manual operations? So, I didn't see that we needed to take that. Okay.

And I guess on, let's see, the spurious actuation ones, John still wanted to ruminate on that. How do you propose we address that? I mean, I presume this will be -- are we going to set this up for a full Committee meeting? We hadn't really talked about that yet. They're about to issue this.

MEMBER BLEY: Were you expecting a letter

on this?

CHAIRMAN BROWN: I don't think they were, but you can answer that yourself.

MEMBER SIEBER: We decide whether they get a letter or not.

MEMBER BLEY: Well, I know, but sometimes they --

CHAIRMAN BROWN: But were you all expecting a letter on this?

MR. JUNG: Not necessary. Revision 1 has been reviewed by ACRS. It is the last step. Another letter will just --

CHAIRMAN BROWN: Revision 1 of?

MR. JUNG: ISG-02. A lot of these subjects we discussed --

CHAIRMAN BROWN: Oh, yes. Yes, I went through them one-by-one on these. They did crank them all in.

MEMBER BLEY: I don't remember what we said then on spurious actuations. I think John probably said something. I mean, he may want to get a letter out on that because he sees that as a key issue.

MEMBER SIEBER: Well, the argument was in fire protection spurious actuations was a big deal.

Here they say don't worry about them. So, you have got to decide, am I going to worry about them because it's a big deal or I'm not going to worry about them because I don't have to?

CHAIRMAN BROWN: Well, the statement was just a base statement. It just said there's less concern, period, and there was no presentation of a set of considerations as to why it was considered of lesser severity.

MEMBER SIEBER: Well, you could make the distinction that fire is a separate element as opposed to all the other kinds of requirements.

MEMBER BLEY: No, he was just using that as an example, though.

MEMBER SIEBER: Yes.

MEMBER BLEY: If you anchor it in regulation in one place, why not the other? The underlying question was, if you put a new system in and were looking at common cause failure, why ought you not look at significant events that could be there? We heard the staff argument that they think that is covered in the normal design review, and that wasn't clear to all of us. So, I don't know where that sits.

CHAIRMAN BROWN: The spurious actuations

issue?

MEMBER BLEY: Yes. I don't know where John sits on that.

CHAIRMAN BROWN: Okay.

MEMBER BLEY: You know, you are probably not going to close it in the sense you are trying to close things. I think that will continue as a concern. What the Committee does about that, the Committee will have to decide.

CHAIRMAN BROWN: Yes. Okay. Well, I guess, right now, from a standpoint of what we expect back, it would be just the one item. And I will try to get with John.

Did you have something, Jack? I'm sorry, I didn't go around the table to see if you --

MEMBER SIEBER: Yes, well, this is a way to do it.

(Laughter.)

But, in any event, one of the things that sort of troubles me is all of this seems to be directed toward actuations of safety systems. In other words, you close a circuit breaker someplace and everything starts and happens automatically. And if it doesn't, some operator can go and flip a switch and make it happen.

On the other hand, there is a whole series of safety systems, and the aux feed is one of them, where you require modulating control. In other words, you have to use a three-element control system in order to control the regulating valves or, if they are electric-driven, aux feed pumps, or the turbine throttle valve for steam-driven aux feed pumps.

That requires manual operator action on a continuous basis. He doesn't run and flip a switch and say, "I did my job." He has to pay attention to what is going on.

Now the question is, are we just talking about actuating safety systems or are we talking about operating safety systems, once they are actuated, to maintain the right parameters? And the impression I got was we don't consider these auxiliary control systems that operate regulating valves, and so forth, as part of the actuation system. And therefore, it is not covered by this.

CHAIRMAN BROWN: Well, I guess I tried to think about that, as John was going through it. And if you went back and looked at the concerning point 4, there were two specific statements in there where it stated that you had to manage the plant-critical safety functions, one.

MEMBER SIEBER: Right.

CHAIRMAN BROWN: And then, the last paragraph explicitly states, once manual actuation is performed from the MCR using these displays and controls, controls outside the MCR for long-term management of these plant-critical safety systems may be used when supported by HFE analyses.

So, that is how I walked away from what you have to do downstream. You have got to look at that after you have actuated it. And if you need to modulate stuff, then you have got to know that you have got the analyses that says I can go do that within the context --

MEMBER SIEBER: Well, we tried to do that. It's very difficult.

CHAIRMAN BROWN: I'm not disagreeing. I have watched people try to control steam generators during a rapid ship transient maneuver where it's really hard.

MEMBER SIEBER: Yes. The other thing is you let it flood and let the relief valves take care of it, but I don't particularly like to rely on relief valves opening and closing as a way to regulate pressure or heat removal or anything else. Sooner or later, one of them is going to stick.

MR. STATTEL: I don't disagree that an HFE analysis should be performed for those situations.

MEMBER SIEBER: I know you don't.

MR. STATTEL: I'm not seeing the connection to where the BTP 19 would drive performance of that analysis, because those are things that are required outside of the scope of a common cause failure.

MEMBER SIEBER: Well, and I agree with that. The regulations, the way they are written, don't encompass that aspect of it. On the other hand, from a practical standpoint, from the operator's standpoint, you have to deal with it. No place do we deal with it that I know of.

MR. EAGLE: To follow up on that, I just want to reemphasize that the --

MEMBER SIEBER: So, yes, I understand how the regulations are put together and what you are trying to do.

MR. EAGLE: Right.

MEMBER SIEBER: I just think there is an outlier.

MR. EAGLE: I just want to reemphasize that one point. Remember, what we are looking at is the common cause failure of the automated system, the

automated reactor protection system. And once you have that failure, then you need to provide a diverse means that will accomplish that same function. Okay?

We also stated that, if you are already doing something manually and you have a common cause failure, you are still expected to be doing it manually. You just may have to do some different equipment.

So, remember, the BTP 7-19 is still focused mainly on the failure of the automatic reactor protection system.

MEMBER SIEBER: Right.

MR. EAGLE: So, you're right about getting into manual stuff. Once you get over there, anything falling through that needs to be manual, that may be outside of the scope of the --

MEMBER SIEBER: That's right.

MR. EAGLE: -- key idea of replacing the automatic system.

MEMBER SIEBER: Yes, it's still a problem, but it's probably outside the scope of this.

CHAIRMAN BROWN: Okay. I'm not going to be able to resolve this here. So, you should just be aware that these two items, that we still need to resolve what we are going to do, and that would be on

the follow-on operations and the spurious actuation. Since John had to leave to go to another meeting, we will probably have to independently come to that conclusion.

Myron, did you have any comment?

DR. HECHT: Possibly a third one, and that is on page 35.

CHAIRMAN BROWN: Slide 35?

DR. HECHT: Yes, slide 35. Excuse me. In response to a public comment, "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."

And I am just wondering if that is always the case.

MR. EAGLE: Well, the idea was, if you lose everything, in other words, you just assume that the entire automatic reactor protection system has disappeared, then it is hard to imagine not that being pretty close to a bounding condition.

The public comments pointed out that you may have a failure in your reactor, in some part of this calculational system, but it may not fail other parts. And that may be true. We couldn't disagree with that.

But if you just assume that whatever failure takes out everything, then your diverse system has to be able to replace the functionality or the safety function that was lost for that particular event.

MR. STATTEL: I can only speak for the analyses that have been performed. And we have used those bounding assumptions.

DR. HECHT: Well, I know that that is an assumption. But is there a partial failure mode of -- let's extend it to more than the RPS or I guess several critical functions that are listed in 603. I don't remember them all.

Is it possible that two systems fighting with each other, when one system has a partial failure mode, could be worse than if the primary system totally fails? And shouldn't that be shown as part of an analysis?

MR. STATTEL: I would expect --

DR. HECHT: It might be a trivial one, but --

MR. STATTEL: I would expect those types of failure modes to be identified in the failure modes and effects analysis, and, also, to be included in the hazards analysis, which is part of the design process.

So, we do review those documents as well.

MR. JUNG: Myron, for new reactors we get into that question and we work with them. But if you look at the diverse means that we looked at, they are looking at plant condition diverse ways. So, a reactor level, water level, is changing either through partial or not. Actually, diverse means actually don't know exactly what caused the primary system. So, some of the partial situations we looked at, we couldn't come up with a good reason why failure to actuate cannot be a bounding case.

For example, certain water flow coming in from two pumps instead of two pumps and one pump comes along type of things. We are assuming that already two pumps are not doing anything. So, if you have one pump providing water, what we can see is maybe there is additional time available for the backup diverse means to kick in a little bit later. So, maybe more time.

We couldn't come up with a scenario where there is some more urgent need that is beyond the bounding. So, we couldn't come with a really good reason for it.

MEMBER BLEY: I think the only thing that comes to mind is, if somehow one of these partial

failure modes isn't recognized as failure, such that the diverse system gets actuated. And I can't give you -- I haven't dug deeply on that, but there might be some partial failure that looks like the system worked.

So, if the diverse system worked, I think you would be all right. But if it doesn't know it has got to work, that would seem to be one that could get you into lots of unanalyzed conditions. I don't know if you guys --

CHAIRMAN BROWN: You are talking about it disguising the need to actuate a diverse system in one way, shape, or form?

MEMBER BLEY: Somehow.

CHAIRMAN BROWN: Yes.

MEMBER BLEY: Yes, such that it --

CHAIRMAN BROWN: Whether manually or --

MEMBER BLEY: Such that it is close enough to good that the system doesn't realize it ought to start.

CHAIRMAN BROWN: Operators don't run them or --

MEMBER BLEY: But, then, you can rely on the operators. So, I would agree, you would probably have more time then, if that happens.

MR. STATTEL: But, even in those cases, there are instructions for the operators, and there are PAMS variables. There are Reg Guide 1.97 variables that are provided to the operators to confirm that the water is getting to where it needs to go.

MEMBER BLEY: That's true. That's true.

MR. EAGLE: Another thing that might be pointed out, I think Rich pointed out, was a lot of times, the way it is set up, like if you have a parameter, you know, the automatic system, the reactor protection system would kick in at this point. But if it doesn't kick in, right below it may be a parameter that is feeding directly to the diverse system, and that would be, if it doesn't do the first one, then the second one catches it.

MEMBER BLEY: The only thing I would suggest there is, when situations get real complex, which this might be, we have seen incidents in the last couple of years where it is real hard for operators to figure them out. So, that would be the one spot, but I don't think that is a big deal.

CHAIRMAN BROWN: Okay.

MEMBER BLEY: Anyway, we've got another meeting, Charlie.

CHAIRMAN BROWN: I know. I'm going to close this off right now.

We will try to get back to you. Well, not try; we will get back to you in one way, shape, or form as to the next step on this. We need to resolve whether with a full Committee meeting or whether we are going to write on it or not, based on a couple of these concerns.

MR. JUNG: I think you ought to leave it up to the ACRS to decide that.

CHAIRMAN BROWN: Yes, we won't dally on it. Okay? I mean, obviously, we are not going to do anything this week.

MR. JUNG: Understand.

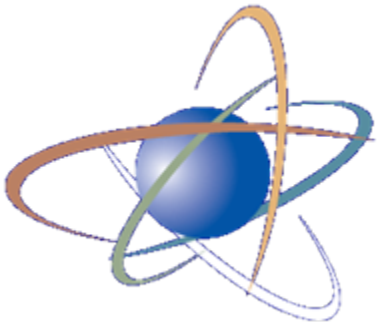
MEMBER BLEY: But we have a meeting, a full Committee meeting, this week to talk about. We need to talk about it

CHAIRMAN BROWN: Yes. Yes, we've got time to discuss it.

All right. The meeting is adjourned.

Thank you very much, gentlemen.

(Whereupon, at 12:23 p.m., the meeting was adjourned.)



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

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 priories
  - 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, ***IF*** 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?