Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, February 26, 2009

Work Order No.: NRC-2691 Pages 1-335

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

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

MEETING

+ + + + +

THURSDAY, FEBRUARY 26, 2009

+ + + + +

ROCKVILLE, MD

The Subcommittee convened in Room T2B3 in the Headquarters of the Nuclear Regulatory Commission, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Dr George Apostolakis, Chair, presiding.

SUBCOMMITTEE MEMBERS PRESENT:

GEORGE E. APOSTOLAKIS, Chair

MARIO V. BONACA

JOHN W. STETKAR

DENNIS C. BLEY

JOHN D. SIEBER

OTTO L. MAYNARD

CHARLES H. BROWN, JR.

CONSULTANTS TO THE SUBCOMMITTEE PRESENT:

MYRON HECHT

SERGIO GUARRO

NRC STAFF PRESENT:

CHRISTINA ANTONESCU, Designated Federal Official

JOHN GROBE

STEWART BAILEY

STEVE ARNDT

DAVID DESAULNIERS

DEBORAH HERMANN

SCOTT MORRIS

PAT HILAND

RUSS SYDNOR

EUGENE EAGLE

ED MILLER

LOIS JAMES

BILL KEMPER

JERRY WERMIEL

KARL STURZEBECHER

ERIC LEE

MICHAEL WATERMAN

DAN SANTOS

ALSO PRESENT:

JOE NASER

JIM RILEY

PHIL CRAIG

TED QUINN

RICHARD WOOD

BRUCE GEDDES

RAY TOROK

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

P R O C E E D I N G S

(8:30 a.m.)

OPENING REMARKS

CHAIR APOSTOLAKIS: The meeting will now come to order.

This is a meeting of the Digital Instrumentation and Control System Subcommittee of the Advisory Committee on Reactor Safeguards.

I am George Apostolakis, the chairman of the subcommittee.

ACRS members in attendance are Mario Bonaca, Dennis Bley, John Stetkar, Jack Sieber, Charley Brown, and Otto Maynard.

Sergio Guarro and Myron Hecht are also attending as consultants to the subcommittee.

Christina Antonescu of the ACRS staff is the Designated Federal Official for this meeting.

The purpose of this meeting is to discuss interim staff guidance documents under development by the staff for reviewing digital I&C applications, and for addressing criteria for crediting manual action.

We will also hear about research efforts on diversity strategies for nuclear power plant I&C, and the regulatory guide on cyber security.

The briefing on the NEI/EPRI reports on operating experience and diverse actuation system risks and benefits previously scheduled for Friday has been postponed to a later date at the request of the staff.

A portion of the meeting may be closed to discuss safeguards and security information.

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. We have received no written comments. We have received a request for time to make oral statements from member of the public regarding today's meeting.

A transcript of the meeting is being kept, and it 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 first identify

themselves and speak with sufficient clarity and volume so that they may be readily heard.

We will now proceed with the meeting, and I call upon Mr. Jack Grobe of the NRC staff to begin.

OVERVIEW OF DIGITAL I&C STEERING COMMITTEE AND TASK WORKING GROUP ACTIVITIES

MR. GROBE: Thank you very much.

My name is Jack Grobe. I'm associate director for engineering and safety systems in NRR.

With me for the introductory comments this morning is Stu Bailey. Stu didn't get enough pain and agony from working on instrumentation and control for a year, and he decided to transition over to GSI-191. So this will be his last ACRS meeting, subcommittee meeting on digital. But you may see him sometime in the future on sumps.

I appreciation the opportunity to present for a day and a half, which is an outstanding amount of the subcommittee's time. We have a variety of topics that we are going to discuss associated with digital I&C. We look forward to the subcommittee's feedback on two particular issues. One is the interim staff guidance revision on operator manual actions. That is done; that will be presented today. As well as the regulatory guide on cyber security to support the new security rulemaking.

Stu and I will provide some background information and status information that sets the foundation for the remainder of the presentations.

There will be two issues that will be presented next time the subcommittee meets, which I think is in June; is that correct?

CHAIR APOSTOLAKIS: Don't know.

MR. GROBE: Well, whenever is the next meeting, there are two issues that we want to make sure are on the agenda. One would be the research plan. Research is in the midst of finalizing with input from all the program offices the next five-year research plan. And it will build on the last five-year plan which expires I think in 2010, and go 2010 to 2015. And so that's something we want to make sure is on the agenda next time.

And then the second issue, as Stu goes through the status presentation, there are two aspects, one of diversity and defense in depth, and the other of risk, that continue to be matters of angst on the part of industry. They would like to see us go further.

We signed out a letter in November addressing both those issues, indicating that we didn't have sufficient technical foundation to go further in those areas.

EPRI has finalized some reports which we have not had an opportunity yet to discuss with them in those two areas. So we requested that the subcommittee not entertain dialogue with EPRI until we had an opportunity to meet with them to discuss those reports and further understand that. So that will be on the agenda next time also.

CHAIR APOSTOLAKIS: Okay, so the way I understand it you would be prepared to have a subcommittee meeting in June sometime?

MR. GROBE: Right.

CHAIR APOSTOLAKIS: Okay, let's make a note of that. We'll see if we can arrange it.

MR. GROBE: Okay, let's go to the next slide. Just a little bit of background to make sure we're on the same foundation. The Commission met in November of 2006. It's hard to believe that was - it's now 2009.

The first meeting of the Digital Instrumentation Control Steering Committee was December of 2006. It was officially chartered in January of 2007 by the executive director. The steering committee established seven task working groups; they are listed here in the slide. The industry established counterpart groups to both the steering committee as well as the task working groups, and there have been over 100 public meetings over the past two years to first address - to find the questions that we needed to address, and then discuss them and resolve those issues. Go to the next slide.

All of the interim staff guidance regarding technical issues for reactors have been resolved, and those issues are as described in the project plan. Later in these introductory remarks we are going to be talking about some going forward issues that we have now identified that also need to be addressed.

The licensing process is well underway. We are meeting publicly very two weeks with the industry to finalize the licensing process guidance for operating reactors; and also the fuel facility guidance, got a little bit of a late start, but that has been working very well and we expect that to be completed this year as well.

The next steps in all of these areas will be to finalize the official regulatory documents, whether that is a revision to a reg guide, or a standard review plan, whatever is appropriate; and that is all described in the project plan.

What I'd like to do now is have Stu go through each of the TWGs and what the status is of the various activities that they have going on.

MR. BAILEY: Hi, I'm Stuart Bailey. Good morning.

My job really is to coordinate all the activities that are going on under the steering committee, and that includes coordinating the work of the seven task working groups. I'll try not to use too many acronyms here, but let me just go through briefly the status of the task working groups, the path forward, and hopefully that can add some context to the other presentations that you will be hearing today.

Task Working Group One is on cyber security, and this arose out of perceived differences in the guidance between NEI 04-04 which the staff had endorsed, and Reg Guide 1.152, which had been updated in `06. And this Task Working Group did a gap analysis between those two documents; realized that there really were no conflicts. There was some difference in scope, and a little bit of overlap.

The eventual fallout here - I shouldn't use that term I suppose - is NEI updated NEI 04-04, and the interim staff guidance document included a cross-referenced matrix so that a licensee could either use any NEI 04-04 Rev. 2 or Reg Guide 1.152 in developing their application.

So ACRS has seen this. Their letter was dated on April 29, 2008, providing positive comments on this.

Our next steps are to update Standard Review Plan Chapter 13;, and Reg Guide 1.152, both following the rulemaking; and then also to issue Reg Guide 5.71. This is formerly draft guide 50.22, and that is the presentation that you will be hearing later today.

CHAIR APOSTOLAKIS: Would you remind me what the two guides do, 1.152 and 5.71?

MR. BAILEY: 1.152 is really a broader document, but it includes information on cyber security assessments. NEI 04-04 is NEI's documentation on cyber security.

CHAIR APOSTOLAKIS: What's 5.71? It does the same thing I think.

MR. MORRIS: I'm Scott Morris. I'm the deputy director for reactor security at NSIR. Very quickly, Reg Guide 1.152 applies only to safety related systems. In the revision to 1.152 in 2006 added a section to the reg guide that talked about lifecycle, how to maintain security throughout the lifecycle, from design to implementation through retirement.

NEI 04-04 is a programmatic document on how to institute a cyber security program at a nuclear reactor site. Reg. Guide 5.71 which we will talk about at length this afternoon is the staff's guidance for implementing the new cyber security regulations in Part 73, and effectively will - it's a program management document, but it covers all of the aspects of NEI 04-04 and Reg Guide 1.152, and it is our intent to revise -152 after this security reg guide is issued to essentially remove the cyber security portions. But we will get into that in some detail this afternoon.

CHAIR APOSTOLAKIS: But right now there is considerable overlap.

MR. MORRIS: A little, yes.

CHAIR APOSTOLAKIS: 1.152 is subsumed -

MR. MORRIS: Reg Guide 5.71 covers - the cyber security rule covers not only safety related systems but also security related systems and any systems that are required for effective emergency response activities, whereas Reg Guide 1.152 is strictly a safety related reg guide.

CHAIR APOSTOLAKIS: Thank you.

MR. BAILEY: Okay, Task Working Group 2 dealt with the issue of diversity and defense in depth. If you recall the SRM/SECY 93-087 provided the Commission's policy on diversity and defense in depth. In a nutshell it said to evaluate diversity and defense in depth for digital systems that were vulnerable to common cause failures, make sure that they were adequately addressed.

The guidance was for licensees to review all events in plant safety analysis, Chapter 15; to identify for any vulnerabilities using realistic methods, since it was considered beyond design basis; and then provide a diverse means, make sure there were diverse means to maintain safety.

The task working group really had a six-part problem statement dealing with various aspects of diversity and defense in depth. Interim staff guidance was developed and issued in December of 2007. It was presented to the ACRS. The ACRS wrote its letter on October 16th of 2007.

There were two things continued on out of this. The interim staff guidance that was developed was rather high level on when you would be able to consider that common cause failure was - needed to be considered, or whether there was insufficient diversity in a system in order to accommodate common cause failures.

The staff has worked further on that issue, and that is the NUREG that will be presented later today. It is looking at the design features, or the built in design of a system, and when does that provide additional assurance of resistance to common cause failures.

Also if you remember in Staff Working Group 2 that the staff had put forth as a criterion for adding a diverse actuation system, the industry's desire was to credit manual operator action, and the staff's position was that that gets difficult to demonstrate if the operator diagnosis and action time is less than 30 minutes.

So the criteria in the interim staff guidance is that if the operator is actually required in greater than 30 minutes that that was acceptable; and in less than 30 minutes a diverse actuation system should be considered.

The ACRS letter recommended that additional guidance be put in there for evaluating the ability to take operator action in less than 30 minutes. The update to ISG-5 that you will hear later today, Interim Staff Guidance number five is that guidance for manual operator actions.

Next one. Task Working Group 3 is for risk informing digital I&C. This Task Working Group had a three-part problem statement. The first was how probabilistic risk assessments that were required by Part 52 for new reactors would be addressed.

The second problem statement was how to use risk insights.

And the third was the state of the art PRA methods.

Interim Staff Guidance No. 3 was issued in August of 2008, providing guidance for the risk assessments for new reactor applications.

The issues on risk informing and state of the art have been deferred at this time to the research plan.

The ACRS provided a letter on ISG -

CHAIR APOSTOLAKIS: That's fine, keep going.

MR. GROBE: I was going to say this later, but I'll do it now. The Commission's policy for diverse actuation systems is of significant interest to the industry. The current policy is that if you are susceptible to common cause failure you have to have a diverse actuation system. And there is a lot of flexibility in that diverse actuation system. It doesn't have to be analog. It doesn't have to be safety related. A lot of flexibility. It just has to be diverse.

Other regulators around the world have addressed the issue of common cause failure in different ways. One country required complete diverse, independent diverse actuation system, and of course that gives you tremendous margin to compensate for potential design errors by either the software design error or the hardware design.

That doesn't meet our expectations in the United States for minimal regulatory burden. And we are being much more precise on when a diverse actuation system is needed. The difficulty is that to allow the staff to make a decision of reasonable assurance of safety we have to have sufficient technical basis to evaluate and resolve these issues. The diversity attributes that Mike Waterman is going to be talking about is research that the NRC initiated and Oak Ridge supported that research to try to get more insight on how we can use hardware diversity attributes in determining at a more precise level when a system is susceptible to common cause failure.

The industry would prefer that we move forward on that. As far as I know, they are not doing research in this area; we are. And as soon as we have enough information we will move forward. We are committed to doing that.

Similarly in the risk area, which Stu is just now getting to, the industry would like us to risk inform the requirements to being susceptible to common cause failures, and requiring a DAS, a diverse actuation system.

We have had many discussions with the subcommittee on risk, and clearly we are not at a position yet where we have a solid foundation to be able to utilize risk analysis of the digital systems in making regulatory decisions. It's another area that we are going to be doing a lot of work on, and I would encourage the industry to also engage in this work. And research is working with EPRI on a memorandum of understanding. We will get into that at our next meeting.

So these are areas where the industry would like us to move forward, and we are moving forward. And the area where we are moving forward is establishing the technical foundation to be able to move forward to further refine our regulatory requirements.

Thanks for listening.

CHAIR APOSTOLAKIS: This is an area of course where the subcommittee - in which the subcommittee has great interest. And I would encourage you to request frequent subcommittee meetings to discuss the work as it progresses. Because it is too late after you guys have invested a lot of time and effort. So we will get some exchange of ideas.

Now ISG-3 was revised to incorporate the ACRS comments. Do we have an opportunity to look at it again?

MR. GROBE: Go ahead, Steve. Introduce yourself.

MR. ARNDT: Steven Arndt, NRR. When we incorporated into the Standard Review Plan, come back to the ACRS.

MR. GROBE: That will be the next opportunity on all of these issues, when they get incorporated into the Standard Review Plan or the regulatory guides.

But I believe after we receive comments from the ACRS we went through a rather substantial revision of that interim staff guide. That specifically focused on new reactor risk analysis. And I think we sent that back to the subcommittee.

CHAIR APOSTOLAKIS: I have not seen the revision.

MR. BAILEY: I thought we shared that to you before the Commission meeting.

MR. GROBE: We will make sure that you have that.

CHAIR APOSTOLAKIS: Oh, you mean you just sent it in? I'm talking about the meeting. Meetings are great.

MR. GROBE: We appreciate that, and we will make sure that that is considered in the next agenda.

CHAIR APOSTOLAKIS: Very good, thank you. The reason I am asking is sometimes the revisions and so on are based on our comments, and we don't really know that. We don't know how the revision was done.

MR. BAILEY: Okay, thank you.

MEMBER BROWN: ISG-3, the purpose of it is to provide some guidance relative to risk informing decision processes for -

MR. GROBE: It actually didn't do that. ISG - the ISG, for new reactors there is a specific requirement that all new reactors have to have probabilistic risk analysis. In the area of digital that was somewhat problematic. There wasn't any consistent industry accepted guidance on how to do risk analysis of digital systems.

So ISG-3 is a review guideline for the staff of the specific attributes to look for in evaluating the adequacy of the licensee's PRA of digital systems for new reactors.

Of course when we provide review guidance to our staff, that provides some oversight to the industry on what our expectations in that area are.

So it's a very detailed guidance document to focus the staff on how to review a PRA for digital systems for new reactors, and make the reasonable assurance conclusion.

MEMBER BROWN: But if you haven't come to a decision as to how you can use risk - PRAs for risk-informed decision making, so you issue your guidance for the staff to review it. That presumes then the licensee is going to be submitting something, making decisions on the digital I&C application for common cause failure or for whatever issues come up.

But yet you said the research is not complete, and we don't have a good basis for it. Why aren't you - I - maybe I'm dense, but I kind of got a disconnect.

MR. GROBE: I am absolutely confident that that is not the case. Steve, did you want to comment?

MR. ARNDT: Yes, it's a little difficult to understand unless you have followed the evolution of the various regulatory documents.

The evaluation criteria for the different regulatory uses of risk are different. That's the real threshold here. In the Part 52 they are looking for outliers and systems and the design aspect of the system; it would be something that you would want to review to ensure that it does not provide an outlier or does not conform with the policy statement of the Commission safety goals. It's a much higher threshold.

Risk inform a current licensing process, or risk inform a particular application, the threshold for data, for system completeness, for analysis, is a much higher threshold. We don't think we know how to do that yet. We don't have the technical basis.

CHAIR APOSTOLAKIS: The way I understand this is, the licensee or the applicant has to submit a PRA for a new design. And the new design contains digital I&C. What is the staff to do? That doesn't mean they have to quantify the probabilities of digital stuff going wrong. But they have to have some guidance. What for example if the PRA says, and all the digital systems are perfect. That's one approach. Is the staff going to accept that? Are they going to do something else?

So the title, I agree with Charley, is not quite risk informing the digital I&C. It's really guidance on how to treat digital I&C in a PRA context; something like that.

MEMBER BROWN: I asked the question for two reasons. One is, I took a look at this, and then I also looked at ISG-6, which we are going to be talking about later, which is licensing, what information do they have to submit with the digital I&C, because if you look at the other documents so far, we say you got to meet certain requirements, but yet, how you demonstrate that you do that is sparse to say the least.

MR. GROBE: There is no risk analysis in that.

MEMBER BROWN: I understand that. I saw that.

MR. GROBE: One of the reasons for that is that that's for operating reactors.

MEMBER BROWN: I remember that also. But

conceptually the thought process can apply to new reactors as well. Just because it's new does not mean that there aren't certain types of information that are required to show that the system is going to perform as expected.

So I understand the difference between two two, but you really can't disconnect information in terms of the details, so that you can understand what the system is going to do.

We can go on. I just was hesitant when you say, we don't have the techniques yet. We don't have the depth. So they submit a PRA. They've got some risk analysis associated with their I&C, how do you look at that? If you are not going to accept decision processes based on the PRA, you are going to look at it in a more traditional manner. I can only think that is what you would have to do. Am I wrong in thinking that?

MR. GROBE: It's not - I don't know what you mean by a traditional way. But it's more the black box approach.

CHAIR APOSTOLAKIS: Well, it's what you mentioned, Jack, you know, about diversity and defense in depth. I think that falls in that traditional way, without quantifying the probability of it.

MR. BAILEY: Exactly.

CHAIR APOSTOLAKIS: Maybe you guys can change the title in the future.

MR. BAILEY: Well, that was the title on the Task Working Group, and I will have to review the title that we ended up on the interim staff guidance. Because the interim staff guidance as you can see really answered the first of the three problem statements.

CHAIR APOSTOLAKIS: Actually what you said makes perfect sense. The interim staff guidance is of more limited scope. Maybe the scope of the working group is broader.

MR. BAILEY: It was intended to be broader.

CHAIR APOSTOLAKIS: But real life intervened, right?

MR. BAILEY: That's right.

(Laughter.)

MR. BAILEY: Okay, Task Working Group 4, Task Working Group 4 dealt with highly integrated control room, the issue one communications. There are two issues on going to the highly integrated control room that I'm sure you've seen, particularly for the advanced reactors.

The guidance here is to provide guidance and information and inter-divisional interdependence. Staff realized really that there could be benefits to this inter-divisional communication, these cross-divisional communications. However there is still the requirement to provide - preserve the independence of those redundant systems.

So the interim staff guidance was issued in September of 2007, and it provided guidance on the communications between safety channels and non-safety channels; also guidance on command prioritization, which was when a piece of equipment is receiving commands from several different masters so to speak, say a safety system a control system, and an operator. And then also guidance on use of the multi-divisional control and display stations.

The ACRS has reviewed this interim staff guidance also and provided its letter on October 16th, 2007. Our next steps are to update that standard review plan, Chapter 7, and then also Reg Guide 1.52. It's envisioned that some of these criteria would also make their way into IEEE 7-432.

MR. HECHT: Is there any formal definition for HICR as opposed to a traditional control room? In other words, we have to draw a line other than saying, year of implementation, is there any specific definition?

MR. BAILEY: I have not run into one. And so the communications here start to apply whenever you have a lot of interface between the safety related digital systems and other digital systems.

MR. GROBE: Steve, do you have anything to add on that?

MR. ARNDT: There may be one, Myron, but I don't know that there is. We didn't define it in that way. We defined it as issues that will come up as you design integrated control rooms. And the guidance that is provided here, and other guidance that is out there is basically saying, if you design a system that looks like this, i.e. one that has potential communications between divisions or potential communications between safety and non-safety, you either can't do it or if you are going to do it you need to do it in this way. These are the criteria that make it permissible.

So whether it's a single system, or the entire gutting of the whole thing, these are the criteria the staff would consider acceptable for doing it that way.

So we haven't defined a threshold

associated with that.

MEMBER BROWN: Does this particular ISG, is it intended - highly integrated control rooms, you look at the existing plants, they are obviously the existing control rooms which are somewhat like all the other existing control rooms. And if they upgrade their systems, do the new plants do that? The stuff I've seen to date, have they gotten the entire control room as well? I'd forgotten that.

MR. GROBE: The vast majority of the digital upgrades in current control rooms has been on balance plant systems, feedwater, turbine control, things of that nature.

MEMBER BROWN: I understand that, but on reactor protection, there are some coming along?

MR. GROBE: That's correct. And the panels have been modified in the cases of the feedwater and turbine controls. I guess I'd like somebody from NRR to talk about what the Oconee control room is going to look like. Steve, you're up again.

MEMBER BROWN: Again, it comes into the level of interchannel communication.

MR. GROBE: You're talking only physically?

MEMBER BROWN: Do these only apply - that's what I didn't get out of looking at some of this stuff, these ISGs you developed, were they only for new reactors?

MR. GROBE: No.

MEMBER BROWN: I was springboarding off your previous comment that ISG-6 was only new reactors.

MR. GROBE: No, ISG-6 is operating reactors. We are getting a little confused here.

MEMBER BROWN: Okay, you're right.

MR. GROBE: We are talking about ISG-4, which is communications.

MEMBER BROWN: I understand.

MR. GROBE: That applies equally to operating reactors and new reactors and has been used extensively for both.

MEMBER BROWN: Okay, that's fine. Do you want to sell it?

MR. GROBE: The only difference would be the communication within the video display units. There won't be as strong a dependence on video display units in the operating reactors as there is in the new reactors. So that would be the only difference in communications.

But beyond the panels, the communications issues are essentially identical in operating reactors and new reactors.

MR. BAILEY: Okay, let's go on to Task Working Group No. 5, also highly integrated control rooms and human factors issues.

Here the problem statements address the minimum inventory of indications and controls needed by the operators. Computerized procedures: there were questions related to safety parameter display systems.

The graded approach to human factors, and then manual operator actions for diversity and defensive depth.

Interim staff guidance on issues one and two was issued in September of 2007. A minimum inventory, that was really done more on a functional basis, what operators would need to perform their procedures, verify safety functions had been performed, et cetera; that these would be available to the operator.

Number two computerized, really this is a discussion on level of automation, and making sure that the operator was always in control and knowledgeable of what was going on in the plant.

Safety parameter display system, the 10 CFR Part 50 specifies the term, console, which most people in new reactors do not intend to have a console per se, so we are pursuing rulemaking on that.

Graded approach was determined not to be needed after that was delved into some more.

CHAIR APOSTOLAKIS: What was it mean, the graded approach?

MR. BAILEY: The graded approach - did you want to help me on that a little bit, Dave?

CHAIR APOSTOLAKIS: Identify yourself and speak with sufficient clarity and volume.

MR. DESAULNIERS: David Desaulniers with the Office of New Reactors.

And I apologize to introduce myself only to say to Stu, I can't help you a whole lot. Unfortunately, that issue was withdrawn prior to my joining the TWG. So maybe we can - do we have any other members of the TWG?

CHAIR APOSTOLAKIS: I'm just curious what graded means. I probably saw it at one time. Can someone enlighten us? It's not that important. Yes, please.

MS. HERMANN: Deborah Hermann, NRO. Graded approach basically means your solutions are commensurate with the risk. High risk you put more into the solution; low risk, it's graded. Your solution, your protective measures are proportional to risk.

CHAIR APOSTOLAKIS: Well, this is not unique to these problems.

MR. BAILEY: Well, you are correct. But I think what they were looking for, if I can recall back, is different levels of review, different requirements for the computerized procedures based on the risk significance of what was going on.

And I believe that the work on computerized procedures made that unnecessary.

MR. NASER: Joe Naser of EPRI from the TWG-5. Actually it was far broader than just computerized procedures. And the idea was, as was already stated, that there are different levels of risk, depending on what you are doing. And the other comment that was also made is also correct, we are looking for some commensurate amount of review, and what you had to do to get qualified depending on that risk level.

And again, it was systems, it was procedures; so it was broader.

MR. GROBE: Thanks.

MR. BAILEY: Okay, and as we stated, you will be hearing more on item #5, which is the operator actions, later today.

Task Working Group No. 6, Tasking Working Group No. 6 addressed licensing process issues. It focused primarily on operating reactors.

The questions that were brought about, the level of detail in the submittal, the applicability of the standard review plan, chapter seven, process protocols and licensing criteria.

In terms of the level of detail, as you are aware, the staff reviews very much the licensee's process for developing a digital system, and this calls into question a little bit the type and level of detail that licensees provide.

Also there was a desire by licensees in the industry to have staff reviews correspond better with the lifecycle development of a digital I&C system. So these issues are being addressed in Task Working Group No. 6.

The interim staff guidance is under development, and you will be hearing a presentation on that later.

CHAIR APOSTOLAKIS: What is the size of these groups? When you say, TWG-6, are we talking about two people, four people?

MR. BAILEY: Currently on TWG-6, we have I'd say four main people in house, and support by a number of other people, working out the details of what we are doing. Industry has - they have probably three primary contacts, and then they have the support of all their other contacts as well.

CHAIR APOSTOLAKIS: And let's say there are four, these four are NRR, or is it research and NRR?

MR. BAILEY: For the licensing process it is primarily NRR. If you look at the other task working groups dealing with the technical issues have been across the research, NRO, NRR, NSIR -

MR. GROBE: NRO is also involving in vetting this.

CHAIR APOSTOLAKIS: Sure.

MR. BAILEY: Correct. Task Working Group No. 7 is for fuel cycle facilities. Many of these problem statements were originally in the other task working groups, but there was sufficient difference in the licensing criteria, while the technology is not necessarily that different, the licensing criteria and how these would fit in to the items relied upon for safety was sufficiently different from the Part 50 process that it was determined that it was more effective to break the fuel cycle facilities into a separate task working group.

So if you look at the problem statements, they are similar to the problem statements in the other task working groups. They did get a later start, and they worked rapidly. We are looking at having interim staff guidance available for public comment in the April or May timeframe, and should be able to speak to you about that in the next subcommittee meeting.

CHAIR APOSTOLAKIS: So this subcommittee is going to review this?

MS. ANTONESCU: No, not at this time.

MR. BAILEY: Not today.

CHAIR APOSTOLAKIS: Oh, I know, but another time?

MR. BAILEY: Yes.

MS. ANTONESCU: I think the question is when.

MR. BAILEY: Oh, okay, we are trying to have these ready in sufficient time so you can review these at the next subcommittee meeting. June or July, whenever.

CHAIR APOSTOLAKIS: June for this?

MR. BAILEY: That is correct.

Okay, the long term documentation here is of course we are completing the interim staff guidance. There will be some update to NUREG-1520, which is standard review plan for fuel cycle facilities. And also looking at a new NUREG. If you are familiar with NUREG- 1520, it's at a very high level; it doesn't get into the level of detail that these interim staff guidance would do. So the staff is looking at putting this more in depth level of guidance into a separate NUREG.

MR. GROBE: Okay. I wanted to get into a little bit of where we were at right now in real space of applying all of this guidance, but also, where we are headed with the steering committee.

Technical consistency was an issue of great concern to the EDO and the office directors when we split NRR and new reactors. There was a lot of debate as to whether or not there should be one technical support group for both offices, or two. The decision was we'd have two.

So we established very close connectivity between the technical staffs in every area, and they were working very closely in digital instrumentation control to ensure that the way in which we solve problems on both sides is appropriately consistent. In some cases there would be significant differences because of the differences in design.

But in many areas of digital I&C, they need to be consistent, and while the process, the Part 52 process, is different, the basis for reasonable assurance needs to be consistent between the two models.

There has been extensive work going on on essentially every new reactor design. The NRR staff has been involved in accordance with the procedure we have in supporting new reactors. Likewise as we go forward with an operating reactor design that is applicable to new reactors, new reactors has been involved in that.

The two major licensing actions going on right now affecting operating reactors involve Wolf Creek and Oconee, very different applications. Wolf Creek is a narrowly focused solution for one signal, and that is the main steam and feedwater isolation signal. The staff has gotten extensive use both in operating reactors and new reactors of interim staff guidance Nos. 2 and 4, diversity and communications.

The staff review of both Wolf Creek and Oconee has not only been in office, but we have been out to the vendors on multiple occasions, and much to the staff's pleasure and sometimes dismay, the vendor for the Oconee system is in Germany.

So there have been multiple - we have been burning the frequent flier miles over to Germany for doing the field audits.

The Wolf Creek review is complete. It's in final review process now with the Office of General Counsel and others, and we expect it to be issued in April.

The applicability of this device, the field programmable gate array, is very broad. And it's a small solution to digital upgrades that can be applied across many different functions. So it's a different solution than Oconee.

Oconee is a more commonly understood microprocessor-based extensively applied solution. It's much more complex. It involves much more capital expenditure of course; a much more complex design and review on our staff's part. That review is also well underway. There are no outstanding issues that don't have solution paths. We are expecting later this summer that that review will be completed and issued in the early fall.

Again as I mentioned there have been extensive site audits as well as vendor audits to make sure that that design is well understood.

One of the difficulties in both of these reviews was clearly defining the expectations in a predictable way of what information is necessary to do the review, and when - at what period of time it was necessary for the staff to have access to that documentation.

And that was the purpose of ISG-6. The licensing process in the staff guidance. It clearly defines at what stage what types of documents are necessary, because the design is not complete when they are submitted to the staff. The - neither of these were good test cases for that interim staff guidance. Oconee provided us extensive documentation right from the get-go which we would not typically expect. And that's because their design process spanned 3-400 years. We would expect the next application, which hopefully is going to come in later this year, or early next year, will be an excellent test case for the new interim staff guide. And it would follow a more predictable process.

MEMBER SIEBER: Could you or somebody give us an example one or two of what the six open items for Tony was, so we can make a judgment as to what level of detail you are dealing with?

MR. ARNDT: Open items that have been opened and then closed, and some of which are still open, the amount and type of validation and verification of the software; the tools used in the validation and verification of the software; the way in which interchannel communication was done; cyber security solutions; a number of others.

MEMBER SIEBER: Okay, that gives me some ideas what your scope is. Thank you.

(Noise interference.)

MR. GROBE: It must be his magnetic personality. Go ahead, Pat.

MR. HILAND: I'm not going to talk if he's satisfied. I've learned.

No, I believe what you are referring to is the initial application for Oconee came in prior to our preparation of what we now call our acceptance review. And in that initial application we sent a letter out that identified six areas that were - I'll use a shorthand language - show stoppers. And that was my intent. I'm Pat Hiland, I'm the director of engineering in the division for NRR.

What we wanted to do was up front before we expended the licensee's resources and our resources was to make sure that there were resolutions that were agreed upon for those six show stoppers.

So that was the first audit that we did at the Oconee facility. That is a public document. That trip report is available.

And although those six issues have not yet reached fruition, we clearly have agreed upon what is the path to be an acceptable document.

MEMBER SIEBER: That is a trip report and not an inspection?

MR. HILAND: That is correct; it's a trip report.

MEMBER SIEBER: Maybe some time offline you can give ma reference?

MR. HILAND: Absolutely.

MEMBER SIEBER: I'd like to read it.

MEMBER BROWN: Am I getting the implication that the ISG-6 is not complete, but that's already available to the industry to see what you are expecting and what you are anticipating to do?

MR. GROBE: The answer is yes and now.

MEMBER BROWN: You said somebody was coming with a test cases. And yet these two were not good test cases, because they were more well defined in the Wolf Creek, and you got tons of information on the Oconee.

I'll make a comment on that. Because one of the issues was inter-channel inter-division communications, which was not very clear with the Oconee information, and we brought that issue up in discussion when they were here.

So I'm just trying to figure out - I'm new, so the ISGs, you're working on them and developing them. Are they already out there in use? I get the implication from reading that they are already -

MR. GROBE: The ISGs that address technical issues are in use. That would be two, three, four, and five.

MEMBER BROWN: Okay, even though they are not official reg guides or whatever, they are out there -

MR. GROBE: They are official interim staff guidance. And those - that guidance will be incorporated appropriately into the reg guides and standard review plans.

MEMBER BROWN: Okay, but now, because they are not official, they are official interim guidance, but there could be changes -

MR. GROBE: Absolutely. As a matter of fact I think we have identified some appropriate changes to ISG-2 and 4.

MEMBER BROWN: So industry understands

that, okay.

MR. GROBE: Now with respect to ISG-6, I believe if you look at our website, there is a draft that was prepared a year ago. It's on the website. It might have been pulled down? It was pulled down?

ISG-6 has gone through a tortured lifecycle. The earlier draft that was published publicly was extensive, and it was more information that you needed at each step of the process. It scared the industry, and what we decided to do was not to work further on that ISG while we were doing the Wolf Creek and Oconee reviews, and use those reviews to inform exactly what information is critical to our reviews.

The current draft has been shared with the industry. I don't believe it's up on the website.

MR. BAILEY: No, it's not at that point yet.

MR. GROBE: It's not at the website, but the industry has - we have been meeting with them every two weeks on this ISG. So there is extensive dialogue between us and the industry on what the expectations will be.

We expect in about 2-1/2 months or 3 months to have that ISG out for public comment, and I would hope, and I've heard some rumblings of who that next utility would be to take the opportunity to move forward in digital. I would hope that that would happen this fall, and they can pilot the ISG.

So it's extensively discussed. There is going to be - my goodness, it is extensively discussed. There is an international conference in April. There is a workshop that we are planning I think it's in March, am I correct?

MR. GROBE: March or April.

MR. GROBE: March of April. There is going to be extensive discussions at the RIC, Regulatory Information Conference in March, as well as at the Amelia Island conference, industry working conference, in July or August.

So these are all industrywide opportunities where we are going to be sharing exactly what's going on in the digital arena, including licensing process, as well as the working - you know, roll-up-your-sleeves working level staff that are meeting every two weeks.

The industry has extensive knowledge and awareness of what's going on, and input into our thinking on that ISG.

MEMBER SIEBER: We have a draft ISG-6 that was sent to us?

MEMBER BROWN: Yes, I know. We are going to be looking at that later, they are going to talk about it in more detail later.

The only comment I would make is, you commented that it was de-scoped is the way I would phrase it. You reduced the size of the information and stuff you were requesting.

MR. GROBE: I live to refer to it as improved precision.

MEMBER BROWN: We can argue about semantics sometime. But I am just encouraging you to be careful on cutting back what I call the functional level of detail, not the detail detail, but the functional, where that tells you or shows you how they act actually going to meet the regulations and requirements that are published in standards, et cetera.

MR. GROBE: Let me just leave an open opportunity, that the level of effort we have had dozens of FTE of work over the last two years, probably scores of FTE of work over the last two years that have gone into this area of digital I&C. And you folks touch it every several months, three or four months.

There is an extensive amount of knowledge in each of these areas that any time either a small group briefing of a couple of members or if there is something you want at a subcommittee meeting, the feedback that we get from the committee is very valuable. So it's - and your challenge is huge, because there are literally thousands of hours of work that go into each one of these activities.

We'd be glad to meet with you separately, or make sure that the agenda is full with all these various topics.

So we are here to support your informed consideration of all this stuff.

MEMBER BROWN: Maybe we'll get some later.

MR. GROBE: Good, we'll look forward to it.

CHAIR APOSTOLAKIS: Okay, let's move on. Are you happy?

MEMBER BROWN: Yes, I am.

MR. GROBE: There's a couple of issues. We are getting ready to put the project plan out of business. As I mentioned all of the technical ISGs are issued. We are going to have a licensing process and full cycle ISGs out in the next couple of months. The staff is already working on converting this interim staff guidance into our formal infrastructure documents.

As soon as those formal infrastructure documents are drafted, the steering committee has concluded that the TWGs can stop, can die, can sunset - die, that's not a good word - but they can be sunsetted. We will no longer need the additional crutch of a task working group. We can go back into our normal regulatory processes of publishing reg guides for public comment or standard review plan, whatever it might be.

The - however, as one would usually expect, we are identifying a number of issues that need continuing work. One of them is a unique characteristic of Part 52. Part 52 is a very different licensing process than Part 50. One of the unique characteristics is the utilization of what's called a design acceptance criteria within the context of inspection, test, analysis and acceptance criteria; commonly referred to as ITAAC.

The design acceptance criteria facilities the staff making a reasonable assurance of safety judgment by putting out detailed design criteria where the design has not yet been reviewed by the staff, but the reasonable assurance of termination is based on the criteria that are in the design acceptance criteria.

That is something new for us, something new for the industry. We are struggling a bit with that. So Office of New Reactors right now has underway some effort to define an interim staff guide on exactly what a design acceptance criteria should look like to support a reasonable assurance determination by the staff.

The second area is operational, making digital systems operational for the operating areas. Within the next 24 - I'm sorry, George?

CHAIR APOSTOLAKIS: But is a TWG-8?

MR. GROBE: No, no. That is where I'm going. Give me a second.

CHAIR APOSTOLAKIS: Okay.

MR. GROBE: We want to get rid of the TWGs. The TWGs were essentially a belt-and-suspenders method to get us through this transition process. What we would like to do is get everything back in the normal management processes for the agency.

The second area of further work that we have identified has to do with making digital systems operational if you operate reactors. There is all of a sudden a number of interesting challenges that come up that we hadn't thought of because we were working on design and licensing.

As soon as you start thinking about operations, you got to think about maintaining the design and licensing basis under 50.59. Handling maintenance act type of use under 50.65(a)(4), the maintenance rule. Risk informed licensing actions, how do you deal with that in the context of digital systems. Risk-informed tech specs, risk-informed allowed outage times. The - and then within the agency we need to be able to deal with inspection findings on a digital system. So we need a significance determination process for digital systems.

The - and the licensees are going to have toe report under 50.73 events associated with the digital system. Those event reports are risk informed, so how - we have - and this is just an early list - I believe that it is fairly comprehensive of the types of challenges that the industry and the NRC are going to fact, once we make these systems operational.

I think Oconee has it scheduled in their outage about two years from now; Wolf Creek will be earlier than that. But we have to solve these problems.

From an operational perspective there is going to be another group that is focusing on these questions, and how to deal with these in an operating context.

What we want to do is sunset the belt-and-suspenders approach of the steering committee and task working groups and put this back into our normal processes.

We believe we have matured in the digital area far enough, and we have been dialoguing with the industry on this, that that is a reasonable thing to do; that is the next step.

So we are not going to create TWGs for operational considerations of DAC, excuse me, design acceptance criteria. Those are going to be handled through normal interactions.

The steering committee will stay in existence I would expect for another year just to ensure that there is continuing effective integration among the various offices on digital issues, as well as effective integration and coordination between all of our external stakeholders.

But by the end of this year we should see all the TWGs go away as functional entities, because we made substantial progress.

MEMBER BLEY: Jack that was really interesting. It raised a couple of questions for me.

The first one is, I heard you say you are going to have an ISG on how to essentially write a DAC. Is there going to be a reg guide and some associated ISG or SRP on how to meet and review specific DAC?

MR. GROBE: Interesting question. The way the Part 52 process works, the license is issued. Of course the utility once they have the license doesn't need to build the plant; they can build it whenever they want. But once it's built, and the licensee indicates that the ITAC had been met, then we do some inspection with them. And Loren Plisco is a second deputy regional administrator in region two. His only responsibility is to develop that back end piece for the new reactors for how to resolve the ITAC, and he has a fairly significant staff that is working on it in conjunction with new reactors.

So that is something - those procedures have to be reviewed -

MEMBER BLEY: This is for all DAC, not just INC?

MR. GROBE: Yes. The first two areas that are -

MEMBER BLEY: Who did you say that was?

MR. GROBE: Loren Plisco is the deputy regional administrator. Glen Gracy is the division director in NRO that is developing the construction inspection program.

MEMBER BLEY: My other question - I'd like to learn more about that - you talked about setting up the process for LERs for these systems. I wonder if the existing guidance on when you have to file an LER is applicable to these new integrated systems. And if not, if you are working on what the requirements for reporting ought to be, it seems because we don't - we certainly hope we don't see any large scale common cause failures or things of that sort, we would sure like to get a handle on things that are going wrong that could be precursors to those kinds of problems.

Are you working on this? Have you thought about it?

MR. GROBE: You are getting George's attention. This is going to be wonderful, because as we put these systems into operation, the nuclear plants not only in the United States but around the world, we are going to get good data on failure modes and root causes.

MEMBER BLEY: If they get reported.

MR. GROBE: They will get reported. In the nuclear industry they will get reported.

The challenge that we faced, and we discussed this with the subcommittee previously, is that in other industries we don't get good information on what was the root cause and failure mode; we just know that the system failed.

On the nuclear side we are looking forward to putting these systems in place, so we can get some real useful information about root causes and failure modes.

We are hoping that none of these requirements need to be revised; we just need to implement guidance so that the industry and the staff understand what the expectations would be under these requirements for a digital system.

MEMBER BLEY: Okay, I'd be willing to learn more about that. In mechanical systems anything that causes a trip will get a report, but you've got to take out, as I recall, both trains of a mechanical system to generate an LER, and that would be equivalent to one of these big common cause failures. So what kind of reporting criteria are going to ensure that we get to see these - I'm calling them precursors, but the very thing you were talking about.

MR. GROBE: This is not going to be ready for your next meeting; this will be two meetings out, something like that.

MEMBER BLEY: Okay, but the work is going on to define those?

MR. GROBE: It's just beginning.

MEMBER BLEY: Or you said you might not need to redefine?

MR. GROBE: I don't think we are going to need to change the rules. I think we are going to need to provide some implementing guidance.

MEMBER BLEY: That is going to be of high interest.

MR. GROBE: Again, that is speculation at this point, because we haven't studied it well. But I would think this is probably six or eight months out.

CHAIR APOSTOLAKIS: That's fine.

MEMBER SIEBER: Maybe I could comment a little bit on this. A couple of years ago they tried to review what the staff had done as far as licensing of digital systems. At that time there were 38 licensing processes that occurred, most of which were in the feedwater control, turbine control kinds of systems. There were no integrated control rooms.

And if you look at the NEI report on failures which uses info data and NRC data, you find that there have been 300 - 400 events, 300 events, something like that, about half of which were covered by LERs.

If you read through the actual event reports, the question really becomes, how detailed was the root cause analysis done by the licensee, and whether that was accepted or not or followed up by an inspection, by the staff. And right now there is not very much data on digital I&C, and the results seem to point to mechanical hardware failures, operator failures, things like that as opposed to common cause failures in digital systems.

On the other hand I know of some events which were safety related, and events that occurred that had LERs that aren't in the study that were common cause events, and so I think that report is sort of incomplete.

If you would base a regulatory system on 38 minor subsystems with a small amount of failure data, and say that I can have an integrated digital control room of some sort, I think that is sort of wishful thinking, because the experience base really isn't there.

The question becomes, in the process of implementing things like the economic change and there will be many others that will come in the future, because MR is sort of fading into the distance, and digital is more precise.

Do we have a good enough reporting system, do the licensees have a good enough root cause analysis, to be able to in a timely way get the regulations, the inspection procedures, the staff guidance and all these other systems that we have for licensed plants up to the scope of what we are trying to do in the process of an evolving concept of the industry.

And to me that is still an open question, as I think what the staff has done is good, but I don't think the data is sufficient to be able to hang our hat on any portion of it, and I think there is more work to do to make that happen.

MEMBER MAYNARD: I'm not excited about developing a bunch of new requirements. I think a lot depends on how much the industry does on their own through IMPO and other reporting systems to catch the lower item. We may have to change requirements if on a voluntary basis we don't have a way to get to some of that information. But I would think it would be in the industry's best interests to have a system that identifies and evaluates a number of these.

I can't wait a see a little bit on how some of those threshold levels change, too.

MR. GROBE: I think we can get into this in detail in the fall timeframe.

MEMBER BROWN: I did want to say one thing, because Jack is right from the standpoint of, if you look at the report, at least the one that was issued to us potentially for looking at it, was pretty sparse relative to data. And I got - I don't know, I had a ton of experience in the Naval nuclear program where for 22 years we collected failure data, and identifying root causes for failures of electronic or electrical systems is extremely difficult. People can replace cards, replace other assemblies, and you can replace two, three or four of those before you finally fix the system.

And the reporting systems you get identify all of them. Even if it's down to another piece part. Now do people after they've replaced four, and they finally get it fixed, do they go back and put the other ones back in again, put the old pieces back in to see if those are really okay?

The answer is no. So if somebody is going to - and that is one of my concerns with reducing some of the level of information we get, excuse me, to define whether the systems are okay. If you are going to depend on that coming in in the future, I think you are going to find that very difficult.

And that is just my personal opinion based on past experience. To say we don't have to know as much, we don't have to get as much information, because now we have this big database out there to define what causes this or what causes that, and therefore we can be more confident, I think that is going to be very, very difficult.

I'm not saying you shouldn't try. The point being that I wouldn't leap out of an often beaten path and into the briar patch before you have a very very good understanding of it, which I don't think you will ever really get, but that's a personal opinion.

MR. GROBE: Well, it's the first step I think to understanding how to truly risk analyze digital systems.

MEMBER BROWN: It applies to analog. There is really no difference whether you are doing analog or digital; all you have done is taken an amplifier and stuck a microcomputer in there; that's all you've done. All the rest of the stuff on the front end and back end is the same, and the way you talk to other things is a little different; but fundamentally the issues apply to both sides, both types of instrumentation controls, doesn't it?

MEMBER SIEBER: Actually, I don't see it quite that way.

MEMBER BROWN: So we have unanimity on this?

(Laughter.)

MEMBER SIEBER: On digital systems designers take advantage of the ability of computers to do complex functions which you can't do in mechanical or analog-type systems.

I guarantee that root cause analysis of failure is difficult in - among licensee root cause analysis, you are going to find a spectrum from extremely good to superficial. I think that that is where the staff needs to focus attention is to look at root cause when errors occur to make sure that they have truly identified what was wrong as opposed to picking the first thing that comes along.

MEMBER BROWN: I don't disagree with

that, that they will do more complex stuff. That is one of the advantages of a microprocessor-based technology, you can really monitor your plant in far more detail than you could with the analog system. So they are more complex from that standpoint.

CHAIR APOSTOLAKIS: Can we move on then?

MEMBER BROWN: Yes, that's okay.

MR. GROBE: Slide 14, let me just highlight one thing on this slide, so we can get on to actually getting the people who know what they are talking about up here and talk some technical detail.

I wanted to touch briefly on the international activities. We have been taking a leadership role that has been led by the Office of New Reactors in the MNDEP, that's the Multinational Design Evaluation Program. The - that's ongoing now in a very aggressive way. Digital is one of the areas we're focusing.

COMPSIS is an international reporting scheme. We have one country that just came forward and wants to utilize the ISGs and their complete review of the digital system for a new reactor, and we are working on a program where we are going to provide them training and coaching on the ISGs, and they are going to give us feedback on the review of their system.

Extensive interactions internationally, and maybe it might be appropriate at some point in the future to update you on all of those.

But with that, why don't I close, unless there are any final questions, and we'll get on to Dave Desaulniers and ISG-5.

MR. HECHT: Can I ask a question with request to COMPSIS, and it relates to previous discussions at the LARs.

MR. GROBE: You might want to get closer to the microphones.

MR. HECHT: I'm sorry. COMPSIS was a very involved, very structured and complex data reporting system. Is that being contemplated for use here? I mean it would be great from an analytical point of view if it had to be done, if I wanted to go home at 5:00 o'clock at the end of the shift I might think differently about it.

MEMBER BROWN: And what is it?

CHAIR APOSTOLAKIS: Who is running it?

MR. GROBE: Why don't we have research, they are the lead on COMPSIS?

MEMBER BROWN: What does the acronym mean?

MR. ARNDT: Computer systems important to safety.

CHAIR APOSTOLAKIS: Wow.

MR. ARNDT: I was the original chair.

MR. SYDNOR: I'm Russ Sydnor, branch chief in the office of research digital I&C branch.

We members of the OECDNEA COMPSIS Steering Committee.

COMPSIS is an international cooperative group to report digital I&C failures from all the - I wish it were all the nuclear countries, but about a dozen nuclear operating countries are reporting data into that.

The last four years they were setting up the database, establishing coding guidelines, things like that. There is some data entry in there; I don't think there is enough in there. We are trying to reinvigorate that.

Our representative will be attending the next steering committee in fact in about two weeks, and we are trying to gather new data out of the LAR database and get information from the utilities to improve, or to have more data in that database, and kind of lead by example and hope that the other countries will report more also.

MEMBER SIEBER: But is there any kind of report that looks at foreign operating experience in digital systems, the same as the NEI report where they generalize numbers of failures and break them down?

MR. SYDNOR: In our previous - I don't know if everyone recalls, there were some previous assessments that were done to support early steering committee activities, where the ACRS subcommittee asked us to consider operating experience in influencing some of these ISGs.

We looked at the COMPSIS data as part of that effort. So we are using it. Again, that data is limited, so that limits your use.

MR. HECHT: I was - my question was more related to the schema and to the forms that were being used than to the actual data in there. And so my question was, is - and I hear from your answer that there is no really a plan to require the COMPSIS reporting formats on the LERs here; is that correct?

MR. ARNDT: The LERs are governed by the 10 CFR 50 Part 73, and that actually was revised what, 10 years ago, something like that, 12, something like that. So there are a specific set of requirements associated with that in the 10 CFR.

The other industry databases, which are

voluntary industry databases, have additional information, the IMPO and the EPRI databases, and we have access to those, so we can glean additional information to support our side of the COMPSIS database through those kinds of informational guidelines as well as our own inspection reports.

MR. HECHT: But the point is, after the LER is submitted, then you have to kind of analyze it, and then recode it, and I guess reverse engineer it to a certain extent.

MR. SYDNOR: If we need additional information, we go ask the utility for their detailed root cause report. We've done that; we are doing that. And quite often there is additional details in those reports.

MR. GROBE: I think it'd be useful later this year to get a more holistic view of what we have been doing internationally.

MEMBER SIEBER: Yes, and the reason why I asked the original question is, if there is a foreign report on digital I&C failures that is publicly available, I'd like to read it. So if there is one, let me know; let me know how to get it.

MR. GROBE: We can get you a copy of our analysis, which was about a year old now I think.

MR. SYDNOR: The assessments were provided to the committee.

MR. GROBE: We can get another copy here.

MR. SYDNOR: But as far as COMPSIS itself, they have recently issued their first three-year operation report; that's available. We could make that available.

MEMBER SIEBER: Okay, if I could get it I'd like it.

MR. SYDNOR: Okay, thank you.

MR. SYDNOR: Thank you.

CHAIR APOSTOLAKIS: I think we are going to take a break now. I never scheduled two-hour sessions when I chair.

Reconvene at 10:00 o'clock.

(Whereupon at 9:45 a.m. the proceeding in the above-entitled matter went off the record and resumed at 10:01 a.m.)

CHAIR APOSTOLAKIS: Okay, we are back in session.

Next item is a revision of ISG-5, credit for manual operator action.

How do you pronounce your name again?

MR. DESAULNIERS: Desaulniers.

CHAIR APOSTOLAKIS: Desaulniers. It's

more difficult that Apostolakis.

(Laughter.)

Okay, David, please.

REVIEW OF ISG-5, "CREDIT FOR MANUAL OPERATOR ACTION"

MR. DESAULNIERS: Good morning, all. Chrstina stepped forward and noted that I'm perhaps a new face to some of you here. So before I begin the presentation I'll just take a moment to introduce myself.

My name is David Desaulniers. I'm not too particular about the pronunciation of the last name. And I'm with the Office of New Reactors, here today representing TWG-5.

I'm been with the NRC nearly 20 years now, and so it's somewhat amazing that this is my first time here before this body. Others will be asking what my secret was.

MEMBER MAYNARD: We'll try to make this a memorable occasion.

(Laughter.)

MR. DESAULNIERS: Thank you. Yes, the first time, I'll always remember it.

My time with NRC has been principally with NRR and human factors there. And just over a year ago I came over to NRO as the senior technical adviser for human factors in NRO.

And as part of those duties I have been the human factors technical adviser for TWG-5.

Not surprisingly my background, formal training, is in human factors. I hold a Ph.D. in engineering psychology, and worked for some time with Lockheed on manned space flight issues. I worked as a consultant doing accident analyses prior to coming to the NRC.

Okay, today what we'll be talking about is briefly TWG-5 and its activities, focusing really on the manual operator action, interim staff guidance. And we will provide some background to set up the discussion of the guidance document, and then we will address the path forward.

Our task working group is comprised of the individuals you see here on this slide: Michael Junge is our TWG manager. He is also the branch chief for operator licensing and human performance in the Office of New Reactors.

George Lapinsky was the principal author of the - of this section of the ISG. I've highlighted others here that have contributed substantially to this document. You can see here that we comprise individuals from across the agency - NRR, RES, NRO.

The members bring to this group a range of expertise. Again, this is the human factors working group, so we have representatives with human factors background as well as I&C, plant operations, and operator licensing, and plant simulation.

Stu Bailey already discussed some of the activities, or areas of focus for this TWG, so I won't dwell long on this slide here. As you can see in additional to manual operator actions we have been addressing some of these other issues.

I'll be talking today, or I'll be generally referring to the ISG, or ISG-05, specifically with respect to manual operator actions, but just for purposes of clarity, this ISG also addresses these other two topics of computer-based procedures and minimum inventory. Those topics were previously brought before the ACRS, and you had issued a letter endorsing those topic areas.

MEMBER STETKAR: Dave, let me ask, I may have missed it before so forgive me for that.

I read through the computer-based procedures area to refresh my mind on things, and it seems to endorse the possibility of strictly computer-based procedures, in the sense of - the words say, backup procedures can either be paper based or a safety related computer based system.

So does that imply that the staff will - does not require paper based backup procedures?

MR. DESAULNIERS: That's correct.

MEMBER STETKAR: Okay.

MEMBER BROWN: I had the same question.

MEMBER STETKAR: No, the staff does not require -

CHAIR APOSTOLAKIS: What is the deeper meaning of this? You guys are talking and smiling. What is the deeper meaning?

MEMBER STETKAR: The deeper meaning is that you don't have to have paper-based procedures any more. If electricity goes black in the pant, you may be smiling by your own guy instincts.

MEMBER SIEBER: The smile is they are going to have paper procedures.

MEMBER STETKAR: The smile is they are going to have them.

MEMBER MAYNARD: I think that it is a little bit of an overstatement. The backup would have to be available.

I agree with you. I think everybody will end up with paper backup procedures. But just because the complete loss of AC -

MEMBER STETKAR: No, I didn't say AC. I said power. That could be DC also.

MEMBER MAYNARD: Well, if the world turned black, though, you wouldn't be able to read the paper procedures.

(Laughter.)

MEMBER BROWN: John, there is another aspect to that also. You don't have to necessarily lose all power. It could be, you need to carry a procedure with you somewhere, and if you want to pick up your backup computer and walk over -

MEMBER STETKAR: No, no, no, that is actually covered for DAS.

MEMBER BROWN: Oh, it is? I didn't see it in there.

MEMBER STETKAR: Thanks. Go on, Dave, thanks. I just wanted to make sure I understood that correctly.

MR. HECHT: Can I ask a question about what - I'm hung up on definition. But if I am an operator, and I rely on a single indicator on my highly integrated control room screen to make a decision, is that a computer-based procedure? What is the distinction - how do we distinguish between a manual and a computer-based procedure given that we are seeing all of our indications on these HICR flat panel displays or whatever?

MR. DESAULNIERS: Your question was -

MR. HECHT: Basically, what is the dividing line between a computer-based procedure and a non-computer-based procedure, given that we have a highly integrated control room?

MR. DESAULNIERS: Well, we make a distinction between paper-based procedures, and then various levels of computer-based procedures in the document. So if your procedure is on paper, you are dealing with not a computer-based procedure in that case.

Now your computer-based procedure may be a simple replication of this paper on the screen. And so it has no automation capability, but is simply portrayed as a - just like looking up a Word document, that would be a computer-based procedure, one level of computer-based procedure.

Does that answer your question?

MEMBER SIEBER: and a higher level of computer-based procedure is one where you have a series of steps and the operator gives permission. And a computer-based procedure goes and executes those steps.

MR. DESAULNIERS: That would be a computer-based procedure with automation.

MEMBER SIEBER: And there are rules as to how to design that kind of a system too in here.

MEMBER BLEY: Myron, I think the difference is those of us who have been hanging around the power plants. The procedure is the step-by-step instruction to the operator. It's not a panel that lights up, and when this light lights up you push this button. It's the thing that goes with it that says, after you have done that, here are the other things to do. So it's actually vocal guidance of some - in some fashion to the operator.

MR. HECHT: So it's defined a priori.

MR. DESAULNIERS: This slide provides a little bit of background, although today I'll be talking about ISG-5, really the step off point for the development of guidance for manual operator action in ISG-5 goes back to ISG-2 which deals with a diversity and defense in depth.

That ISG, as you have heard previously, provided guidance, review guidance, relative to the diversity and defense in depth, or what I'll refer to here as D3 analysis for I&C systems.

As part of that guidance it did address

operator action, and you had heard previously it referred to operator action being acceptable beyond 30 minutes, which will be addressed here further in another slide.

That guidance, ISG-02 recognized that there would be a possibility of a common cause failure, of a reactor protection system. In such cases where there was such a vulnerability identified, you would use realistic assumptions to perform the analysis of the plant response, and identify backup by systems or actions necessary to accomplish the required safety functions.

MEMBER BONACA: What do you mean by realistic?

MR. DESAULNIERS: Realistic assumptions - the term here has been equated with, but is not quite appropriate with, best estimate analyses. That term is synonymous in this case, but is not - because it has a formal definition is not applicable to the range of conditions we are talking abou8t here. But it is generally what are the expected normal range of conditions. It's not requiring worst case analysis.

MEMBER BROWN: Doesn't that just mean the diverse system doesn't have to meet your full bore safety analysis protection basis or licensing basis?

It's just a backup. It will shut the plant down in a controlled manner. That's what I got out of some of the other discussions. Is that correct?

MR. DESAULNIERS: I think Steve Arndt would like to add to the response.

MR. ARNDT: Yes, that is correct. That is only a subset of it though. Wh en you do the analysis, you have to determine how much time you have. That is part of a thermo-hydraulic analysis and a human factor analysis and other things. That part is using realistic assumptions as opposed to conservative assumptions. The other part of it, as you articulated, is that you don't need a safety grid system.

MEMBER BROWN: Okay, you're saying part of it goes along - if you did a worst case analysis, somebody might only have 10 minutes to take some action, and in other cases they might have 30, just to pick two numbers, don't read anything into the numbers.

MR. ARNDT: Correct.

MEMBER BROWN: Oh, got it.

CHAIR APOSTOLAKIS: But this identification of the common cause failure, is that the postulated failure? Does it go down - I mean what level of detail is described? Because the documents I have seen really - I'm not sure they get down to the actual failure mode. Is that a misconception on my part? Because the analysis will have to know what kind of CCR we are talking about, right?

MR. ARNDT: Yes, the guidance in BTP-19 and in ISG-2 provides guidance on the kind of failures you need to take, and that is derived from the Commission policy on that.

We don't provide specific failure modes, that's part of the analysis of the system.

CHAIR APOSTOLAKIS: That's right.

MR. ARNDT: There is guidance out there in NUREG-6303 on how to do that.

CHAIR APOSTOLAKIS: I guess you don't have a specific example, do you? In your presentation do you a have an example?

MR. DESAULNIERS: No, I don't. This presentation will focus on given common cause failure condition, what need be done to analyze time available for operator action.

MEMBER BROWN: Well, the crediting you talked about, it specifically says it's for AOO - anticipated operational occurrences and postulated accidents that are concurrent with software common cause failures; very specific.

And my first question was, how do I know I had a software common control failure? I mean you don't have time for analysis; stuff is going on. So you have to take plant control actions of some kind. So you don't know what the cause is when the lights start going off and alarms going necessarily, but you do have to put the plant in a safe condition.

So but yet your ability to use operator actions is based on being able to determine - based on all the subsequent analysis in here, and the discussions you went through, based on being able to identify the specific CCF, and that it is a software failure. That's what it says.

MR. DESAULNIERS: No, this is the scope of actions that can be credited in the diversity and defense in depth analysis. But the approach of the operator is not dependent on operator diagnosis of a common cause failure. We are not postulating that in all cases. We are just at this point identifying what the scope of actions are that would be allowed.

MEMBER BROWN: Okay, well let me - it says, this is going to be used for evaluating manual operator action as a diverse means of coping with AOOs and Pas that are concurrent with a software common mode failure; very specific. That is why I asked the question. It's not generalized; it's very specific.

MR. DESAULNIERS: Steve, do you want to add?

MEMBER BROWN: I don't know who is going to go first.

MR. NASER: I'd like to - I think Dave was kind of leading into what I'm going to say. Sorry, Joe Naser of EPRI.

If we aren't assuming that the operator will know there is a common cause failure, in other words he can't magically know this is a common cause failure, what we are saying is, he is looking at process parameters and he is seeing things that are going out of the normal realm which indicates there is probably a common cause failure or something else bad happening that he needs to take a response to.

So it isn't that he can see that, a ha, I have a common cause failure; he sees process parameters are going out of ranges where they should not have gone, and that something like a common cause failure, or something very abnormal happened.

MEMBER BROWN: Of whatever kind of common cause failure?

MR. NASER: Yes.

MEMBER BROWN: Whether it is a computing platform that just went burp in all the systems, or whether it's a software, or it can hardware, software, anything. That's fine; I just wanted to know, because this does not say that right now, so it was very specific as to how you were going to evaluate the stuff and what the circumstances were. You're saying it's really more general than that, more generic I should say.

MR. NASER: That's correct, and you can look at of course with the different events, you will have an understanding of the types of parameters that might be going out. So but again it isn't a matter like - well, yes, Steve wants to add.

MR. ARNDT: Yes, let me put a point on it. The concern is, this is a guidance to the staff on how to review the design. Our guidance says that because we have concerns about potential common cause failure you need diversity.

If the design strategy is, the diversity is automatic, that is one solution. If the design strategy is, manual operator action, then you use this guidance and the review criteria is, you assume that you have a design basis event or an AOO with a common mode failure. And then look at whether or not you can respond in the appropriate amount of time.

MEMBER BONACA: Yes, I want to specify why I raised the question to start with. Mr. Grobe said before, when he was making his presentation, that the concern was common cause. But he also said that you could implement a fully diverse as an optimal system, alternative, automatic, as some foreign operations have done. However that this would be placing a high regulatory burden.

And that concerned me a little bit. But the question is is it technically feasible to go manual or not? You know burden or not.

MR. ARNDT: I am not going to address the interpretation of what Jack said. The criteria is in ISG-4 - I'm sorry, ISG-2, that explains the review criteria that we have. And it basically says you have to do one of four things. You have to have a system, a plant that is so robust that you don't have to take actions, and you won't violate the Part 100 rules; or you have to have a system that has internal redundancy to processors of one kind and to processors of another kind or some other solution; or if you don't have internal redundancy you can have an external diverse actuation system; or if you have sufficient time so that a manual operator action can be taken such that you do not surpass the Part 100 acceptance criteria.

So there are a diverse set of ways that a design can be resilient to a potential common cause failure.

MEMBER BONACA: But then when you say that you have realistic assumptions, dependent on how you calculate them you can get easily to 30 minutes.

MR. ARNDT: In many cases you can, and in some cases you can't.

CHAIR APOSTOLAKIS: And Steve, the thing that is not clear to me yet in this context is, can you do all these things without really specifying what kind of common cause failure it is? Can you do it strictly based on the consequences of the common cause failure, because I think that's what we're saying.

MR. ARNDT: That I s correct.

CHAIR APOSTOLAKIS: That things have failed, I don't care how, and I'm going to take action.

MR. ARNDT: That is exactly correct.

CHAIR APOSTOLAKIS: And the last point, could you please sit over there?

MR. ARNDT: If the committee would like me to, I can.

MR. EAGLE: Gene Eagle, INC-2. I was on

the ISG-2 committee. And this set the background for getting ready for ISG-4. There were assumptions that were made or looked at. And one of the things, going back to the specific items, we looked at this common cause failure and said that one possibility here is it could be something - if you think of hardware common cause failure, that is the kind of thing that would be very slow, aging, things like this; they didn't look at that. Normally if you had failures, they would be like individual items. And we covered that with diversity.

However, in the common cause area it more likely would be coming from software. Of course another thing we said is that these systems are very - that we looked at in quite a lot of detail, looked at quite a broad spectrum. And we suspected that most of the things you could imagine or think about would be covered, and that the operating procedures would be well ready to handle a lot of different things. The operators would be trained on the simulators with a lot of things. So whatever would get you in the common cause failure area is probably going to be something we don't expect.

So the actual details at that point - what we assume, then, that probably whatever would happen, you just have to assume for a moment that all these basic four divisions or computer aids that you have, the four divisions would suddenly not be available in some way. They may not be giving you information. They may go dead. Or they could be telling you everything was just fine when you might be having a LOCA. So this is the idea that the worst possible, maybe the worst case, something would not be there. So that would be the background for starting. And that was one of the reasons for taking my conservative approach of a 30 minute - it says that if you lose your automatic systems, then you have to have an automatic backup as far as diverse systems, a diverse automatic backup. You cannot take credit for manual action is it takes less than 30 minutes.

That was the background for ISG-2. Now if you want to use manual operation or manual diverse backup, then we move into the ISG-4. But the basic background here was, we don't know what could be causing it, but whatever gets us in a common cause failure is probably something we are not expecting.

One example of this is recently when they had somebody walk up and take a picture in the control room of one of the digital instruments. And all of a sudden the whole plant shut down. I mean the reactor actually SCRAMed. And of course they had signs that you weren't supposed to be using cameras. The operators had assumed this was because of security reasons. They did not realize the camera had an RF type bounce distance, and everybody said that they should have imagined, they should have understood this, but they didn't. So this was a complete surprise to the operator.

So this would be the kind of concept of a loss of a common cause failure; something the operator doesn't expect. And there is probably going to be a lot of confusion at this point. So one of the reasons for the 30 minutes was to take the pressure off the operator and give him a little more time for making decisions.

So this is the background in ISG-2 before we start moving it over to the next possibility where they really look at maybe more realistic assumptions.

CHAIR APOSTOLAKIS: Thank you for that. Sergio.

MR. GUARRO: I would like to ask just a question as to what is the definition of RPS safety functions in the plural? In other words where is the boundary between what is the initial function versus cascading functions? I'm trying to understand how narrow or broad this is?

MR. DESAULNIERS: Okay, well, again, that comes from ISGO-2. I don't know if Gene wants to pick up on that, if they specifically addressed that aspect of the bounding there for the safety functions.

MR. EAGLE: Repeat the question one more time, please.

MR. GUARRO: Well, translating, are we talking just the reactor shutdown or all the cascading functions that go from there on? And where is the boundary - at what point, because the chart says, D3 analysis. One or more reactor protection systems, safety functions in the plural. So I'm trying to understand, there is a precise definition of what these safety functions are. Or is it somewhat open ended?

MR. EAGLE: Well, the basic assumption here was that it would be quite possible that we could not completely identify what would be the effect of a common cause failure. Because when you look at it, it's not really - it doesn't look like a very high probability. With as much effort as we've put into the design of these things, with as much diversity, the defense in depth, the four channels, the idea was that we do not have a complete idea of what could happen. They would take out everything. And so it was left as kind of an undetermined state, that whatever it is it could be unknown.

But obviously the biggest thing is, when something happens, getting out of hand, the reactor should SCRAM and shut down, and be shut down in a controlled fashion, and be able to keep the core covered, and remove its heat removal and all the other safety functions.

CHAIR APOSTOLAKIS: So it's everything?

MR. GUARRO: It's everything that follows the shutdown.

MEMBER BLEY: Reactor protection, and engineered safeguards.

MEMBER SIEBER: There is a distinction between the two. Reactor protection system is everything that will trip the reactor. It's high flux, high temperature, low pressure - all those things.

The starting of pumps, safety injection pumps and all of that stuff, that has to do with recovery from a reactor protection system actuation, is engineered safety features. They make that distinction.

MR. GUARRO: That was my initial

definition, but I was trying to understand if that included both or not.

MR. ARNDT: It's those functions to bring the plant to a safe state.

CHAIR APOSTOLAKIS: it's both.

MR. GUARRO: it's both.

MR. EAGLE: We also note that we already have a diverse backup system for the reactor protection system and the ASTWS system.

One other final point, just to be on the background of ISG-2 before we went on to ISG-4 was, that this failure of an automatic system, we did point out that this was the replacement of the automatic system. If there were already means that were normally planned to be manual, they would be normally expected to continue to be manual.

I think one example is the switch over from the pumping systems to the recirc in the PWR.

CHAIR APOSTOLAKIS: Myron.

MR. HECHT: Yes, I just wanted to point out that I think the entire discussion starting with Charley's question about, why does it say software here, and then the response, which was, we don't know what the common cause failure is, is because we are dealing with this totally within a DI&C context. So I think there was an implicit assumption in the writing of this document - tell me if I'm wrong - but on page 14 of DISG-5 it says, it explicitly says it twice, it says software common cause failure.

And yet in the more general discussion we've said common cause failures from any means.

And so I guess maybe the problem is that we have convoluted common cause failures which could occur in a totally manual plant with I&C failures, and maybe that is a confusion. Have you recognized that and dealt with that?

MEMBER BROWN: I just want them, if it is more general, then the ISG ought to say, you shouldn't put software in front of all these CCFs all the way through, because it really -

MEMBER SIEBER: From the operator's viewpoint, as he goes through procedures and monitors his instruments, he is looking at various parameters and indications and says, this should have happened and it didn't. He doesn't have time to analyze whether it's a common cause failure or a failed transducer or the plant is screwing up.

So he will take his actions, and some of those actions will be appropriate to common cause failures. And what we are dealing with here is to decide whether an operator's manual action will provide D3 for that common cause failure.

So you are taking a little piece out of a big set of things that operators do in order to establish that point.

CHAIR APOSTOLAKIS: I could go through all this discussion, call it symptom based operator performance, and never mention CCF once.

MEMBER SIEBER: You could.

(Simultaneous speakers.)

MEMBER BLEY: Except that it has to work in the presence of - that is the -

MEMBER SIEBER: But the question is, how do we deal with common cause failures? And one of those solutions, secondary solutions, is operator action. And that is what the linkage is.

The subject is common cause failures. You claim credit for operator action. He's doing lots of things for lots of reasons. But will he solve the common cause failure problem or not? And that is the question.

MR. HECHT: But I think the presumption here is that we have an additional - that the DI&C systems make this a special class of common cause events, let me put it that way.

MEMBER SIEBER: That's correct.

MR. HECHT: And that's why I think it's a little bit confusing.

MEMBER SIEBER: Regardless of how improbable it is, we have an extra element because it's digital.

MR. HECHT: Correct.

MEMBER BROWN: Steve, one of the other things you said in there was, the operator actions to be assessed would be to determine level of redundancy as well as diversity. Someone threw the word, redundancy in there. I heard that when you were sitting back over here.

I don't know if you meant that or not. Because that is not in the context - I mean if somebody was thinking about using operator action to say, I don't need four channels, I only need three or two.

MR. ARNDT: If I said that, I didn't mean it in that context.

MEMBER BROWN: All right, that's fine. So you are back to the basic premise here, by diverse means or backup means, can we use an operator action as the diverse means, as opposed to either an automated or a manual diverse backup system, whatever.

Is that right?

CHAIR APOSTOLAKIS: Are operator manual actions an extra level of defense in depth?

MEMBER BROWN: Are they sufficient to be credited as defense in depth. In less than 30 minutes. Thirty minutes, it sounds like, if it takes longer than that, I think based on ISG-2, already been accepted; isn't that correct.

MR. DESAULNIERS: This perhaps could lead into the next slide here, is that what ISG-2 says with regard to the operator actions is that for those that would be required after the first 30 minutes, there would be - require an appropriate human factors engineering analysis - I'm sorry, there was another question.

MEMBER STETKAR: No, that's fine. Are you done? I do want to ask a question, only because I'm confused.

This is going to be a simple question, I hope a yes or no. Is pressurized water, auxiliary feedwater actuation, considered an SFAR function within the context of DAS?

MR. BAILEY: Yes.

MR. DESAULNIERS: I believe so, yes.

MEMBER STETKAR: I wanted them to say

that, though. Only because everything that I've seen --

(Simultaneous speakers.)

MR. BAILEY: Did we get the answer?

CHAIR APOSTOLAKIS: The answer was yes. But you had a comment after that?

MEMBER STETKAR: No, I don't. It will come later.

(Laughter.)

MEMBER STETKAR: I had a follow up if the answer was no.

CHAIR APOSTOLAKIS: I have a problem here. You have 37 slides. Are you going to use all 37? Because at this rate --

MR. DESAULNIERS: Not at this rate.

MEMBER BROWN: No, ISG-5 doesn't. It's just for the morning.

We've got an hour and 15 minutes here.

CHAIR APOSTOLAKIS: In any case, there is a lot of discussion, so maybe you can think about skipping some stuff.

Keep going.

MR. DESAULNIERS: Okay. So quickly over the background here I gave ISG-2 as the starting point. When that guidance was issued there was feedback from the industry as well as ACRS that there should be consideration of developing guidance for crediting actions in less than 30 minutes. The scope of the TWG-5 action plan was expanded to incorporate that.

We pursued regular public interactions with our counterparts, industry counterparts, with TWG-5. Those were occurring on a monthly basis. While we were doing that the industry was developing a white paper that provided guidance for that methodology which we were considering as staff was developing its position.

And ultimately we saw that we had enough information to go forward and develop the staff guidance documents.

CHAIR APOSTOLAKIS: So the next slide I guess addresses the last bullet?

MR. DESAULNIERS: The - oops.

MEMBER BROWN: This is Section 3 then?

CHAIR APOSTOLAKIS: Staff considered and incorporated as appropriate white paper methods; is that what the next slide is about?

MR. DESAULNIERS: Yes. The next paper summarizes the white paper methodology.

CHAIR APOSTOLAKIS: I would like to know

which method you figured should be incorporated as appropriate. I want an example in other words. I know this statement. We use it ourselves. But you seem to be confused. Let's go back to slide #1l. Let's go back to the last bullet of slide #11.

Staff considered and incorporated as appropriate white paper methods in developing an amendment.

Can you give me an example of that?

MR. DESAULNIERS: Of what methods that we have incorporated?

CHAIR APOSTOLAKIS: Yes.

MR. DESAULNIERS: Several of these slides will be addressing that.

CHAIR APOSTOLAKIS: Okay.

MR. DESAULNIERS: In order to describe the white paper method, I'm going to describe where we saw that we needed to address some of the concerns.

CHAIR APOSTOLAKIS: Wonderful. Wonderful.

MR. DESAULNIERS: And you will see where the similarities are.

CHAIR APOSTOLAKIS: Good point. Very good.

MR. DESAULNIERS: So quickly, the white

paper methodology was a four-phase methodology beginning with an analysis phase, which was to determine what is the time available for operator action based on thermal-hydraulic analysis of the plant response. And the time required for operator action was to be based on use of an ANSI standard, that's ANSI/ANS 58.8, which was developed to develop time response criteria for operator action for design basis events. And I'll talk about that document a little bit further in case others are not familiar with 58.8, the subsequent slide.

Following that analysis, where you have comparison of time available to time required, there would be a verification of that analysis basically done through a table top or walk through, talk through, type exercises, and then a validation as the third phase in using part task simulators, or limited scope simulators, to verify or excuse me validate the analysis phase.

And then the human performance monitoring piece was the long term implementation ensuring that these credited actions remain reliable throughout the life of the plant or however long it was to be credited.

MEMBER BROWN: What is the table top

exercise?

MR. DESAULNIERS: That is essentially individuals sitting at a table top, your relevant experts, dealing with system design information.

MEMBER BROWN: All right, so they are just kind of discussion?

MR. DESAULNIERS: Yes.

MEMBER BROWN: Well, table top discussion, but normally you will actually step through a scenario at the table rather than being out in the field doing it?

MR. DESAULNIERS: Right, you walk through the procedure or whatever the actions are, walk through, talk through process. It's just not real time. It's a non-real time discussion of the operations and an assessment then, judgment-based, on what it really takes to do it, sans any other particular information.

Now this next slide provides just the detail related to the calculation of time required. Again, one of the proposed methodologies in the industry white paper was to use 58.8 as the guidance document for determining time required.

That guidance essentially provides a methodology for breaking down an operator action into specific time intervals, such as the time for diagnosis, the time to select a response and then perform the manipulation.

And as noted here, it was developed as a means to establish minimum allowable response times for operator actions for design basis events.

It provides specific time values for those various task intervals. Some of those have multipliers associated with them depending on the number of manipulations or the diagnostic time would differ based on the expected frequency of the event.

MEMBER BLEY: Is there any allowance for the uncertainty the real world is going to introduce, that when you have a real event that it won't be exactly like the design basis event, some allowance for uncertainty and interfering actions that might capture the operators' attention? Or is it just a straight, how-long-does-it-take to do just what you have to do in the design basis accident?

MR. DESAULNIERS: Well, if you are speaking with respect to 58.8, I want to close this by saying, keep in mind one of the reasons we had a concern with regard to this methodology is, the NRC had ultimately decided not to endorse that methodology.

MEMBER BROWN: They did not endorse this? NRC did not?

MR. DESAULNIERS: No, there was a reg guide that - draft reg guide where the staff had considered endorsing this. In fact the ACRS had provided feedback, noting concerns that some of the times in 58.8 may not be appropriately conservative, may perhaps not address some of the concerns that you are raising, Dennis, as well as the availability of the data supporting 58.8 was not readily available to the staff, had not been peer reviewed. So there were concerns in that regard.

MEMBER BLEY: Nevertheless, this is what you have to use for these manual actions?

MR. DESAULNIERS: This is a methodology that was proposed, and we are noting this because of some of these concerns which I will go to on the next slide.

The - we had not endorsed this methodology. In addition the - as proposed in the industry white paper, there would have been some modifications of that methodology to try to apply it here to a digital interface in these control rooms.

That standard was developed principally for analog control rooms. So it was thought by some members that there needed to be some changes made in order to be able to apply it in this circumstance, combining multiple steps for instance, perhaps, manipulations that would have been done in an analog control room, and consider that a single step in a digital control.

There was also a proposal for a concept of what was referred to either as a unique prompting alarm, or earlier on it was referred to as a common cause failure alarm. And it would have been some unique prompt that would have indicated to the operators that something had gone wrong that essentially could not - those conditions could not exist absent a common cause failure, though it wouldn't actually diagnose the common cause failure.

And the staff again had some concern with regard to both - from the technology on the I&C end, whether that technology was something new, whether we really wanted to be endorsing that in the context of this guide, as well as the - from an operations and human factors perspective it was essentially relying on a situation where an operator would simply see this alarm and take immediate action without giving consideration, time, to evaluate the event, and just take prompt action simply based on that -

CHAIR APOSTOLAKIS: This seems to be crying for being risk informed. I mean if there is something uncertain in all that stuff, it's operator action.

MEMBER BROWN: It becomes worse as you go through.

CHAIR APOSTOLAKIS: I mean why did they persist on this deterministic evaluation? I mean it all seems to be deterministic?

MR. DESAULNIERS: This would have been deterministic - I don't consider the approach that the staff ultimately took as deterministic.

CHAIR APOSTOLAKIS: Okay.

MR. DESAULNIERS: And I'll just leave it as that as some of the examples of some of the concerns that we had, and I'll move on to the next slide, which will I guess roll up what I think perhaps two fo the significant concerns that the staff had with regard to the methodology as proposed in the white paper.

And that was that the process there really seemed to focus on the feasibility of the operator action, and that being simply ensuring that operator response or required time was less than the time available without an explicit treatment of the margin between those two values as well as the potential for operator error.

CHAIR APOSTOLAKIS: Didn't you guys submit a similar analysis in the context of fire years ago?

MR. DESAULNIERS: Yes.

CHAIR APOSTOLAKIS: And there was a margin there.

MR. DESAULNIERS: Yes, there was.

CHAIR APOSTOLAKIS: So this one did not include a margin? I think there was a margin of some factor.

MR. DESAULNIERS: And in late discussions of the industrywide paper, there was discussion of margin in the context of trying a fixed interval of margin or a margin that was based on some fraction of the overall time for operator action.

And that deterministic approach, we did not have a clear technical basis for picking some specific time value, whether it was a set number of seconds, minutes, or whatever, or some fraction. So we opted not to pursue that approach.

CHAIR APOSTOLAKIS: Are we beyond design basis here?

MR. DESAULNIERS: Yes, common cause

failure -

CHAIR APOSTOLAKIS: Okay.

MR. DESAULNIERS: So the other aspect here was that in the approach here with - as proposed in the white paper, it seemed as though the large measure of information with which the staff could really make a sound determination was weighted towards the validation portion which would not be occurring until there was a simulator available which would be late in the process for those being licensed under Part 52, so we are looking to move the information earlier into the review process.

MEMBER SIEBER: Now the validation portion is just to establish that the appropriate indications or controls are there, that the operator can work through the manual operating procedure to achieve the end goal of the failure caused by common cause failures, right? You do not set - look at the human factors issues of the operator should have acted and did not, the operator acted and should have not, the operator should have acted but did the wrong thing? That would tell you what the risk of that backup is, and I don't think I've seen that as an evaluation criterion as far as whether the manual backup should be allowed or not or credited or not. Is that correct?

MR. DESAULNIERS: I'm not sure I would break it out quite as you have described, because as we will be discussing here later on the integrated system validation, you will be wanting to take a look at actual real time performance of the operator and the as-built design considering some of these various operating conditions that may affect the reliability of that performance.

So you are looking to validate that you have adequately addressed some of these human factors considerations.

MEMBER SIEBER: I just had this feeling that there was something missing.

MR. DESAULNIERS: Well, see if it's missing by the time of the end of the presentation, then we'll see if we can come back to it.

MEMBER SIEBER: If you take 100 crews and put them through 100 different scenarios, you are not going to get a perfect score from every crew on every scenario. That should be a factor is all I'm saying.

MEMBER BROWN: You can't factor in the fact that the guy is getting a little hazy partway through his shift also. I mean how many people go through their shift, and they are always bright eyed and bushy tailed. We can't even do that here in these meetings, much less -

MEMBER BLEY: That is coming up next week.

CHAIR APOSTOLAKIS: Coming up next week.

MEMBER SIEBER: Well, in the simulator you go in there with the expectation that you are actually going to do something, as opposed to going on shift.

MEMBER BROWN: Exactly. And that is how you are figuring this is going to be an easy 100 percent power for eight hours, that's it.

CHAIR APOSTOLAKIS: Okay, maybe we will address that point.

MR. DESAULNIERS: I think perhaps we will when we go further into this we will address your question more fully.

And so I will begin now with an overview now of what is actually in the interim staff guidance for manual operator action.

That guidance is broken down into major sections of scope, staff position, and 4-phase methodology within that staff position.

The scope I am not going to linger on here, because I think we have discussed that significantly here. I will just note that we are talking about a guidance document that is applicable to both new and existing reactors.

The staff position section of the guidance document just highlights a couple of the fundamental assumptions going into maybe that underpin the review process, the expectation that these actions will be included in the emergency operating procedures, that we are talking about those actions limited to those that can be executed from within the main control room; that ultimately these actions need to be demonstrated to be both feasible and reliable; and that this methodology that we will be talking about can be integrated, and in fact should be integrated, as part of the overall human factors engineering program.

MEMBER BROWN: Doesn't the - I'm sorry, go ahead, John.

MEMBER STETKAR: Just to make sure I clearly understand it, this methodology that you are going to be walking through applies to all operator actions that the licensee includes credit for, right, regardless of the 30-minute time window, it applies to -

MR. DESAULNIERS: Less than or above, yes.

MEMBER STETKAR: Less than or above? Okay, thanks.

MEMBER BROWN: The statement about executed from within the main control room, based on the earlier discussion of a common cause failure, something - because that is the initiating context of this, if it wipes out your ability to control from the main control room, in other words, that was a discussion we had at the meeting last week. Now how can an operator action be used if you have a CCF that takes out all the main stuff in the control room?

(Simultaneous speakers.)

MR. DESAULNIERS: Well, the ISG-02 -

MEMBER BROWN: Without a diverse actuating system that you can walk over to.

MR. DESAULNIERS: - is that there needs to be diverse controls and indications that would continue to be available under common cause failure conditions. So that -

MEMBER BROWN: So you are not going to eliminate the backup automated system by being able to take credit for somebody's operation or execution in 15 minutes base 30?

MR. DESAULNIERS: Well, there is I think a difference between the automated backup and having the instrumentation and controls available for manual action, is the way I would characterize it.

MEMBER SIEBER: Yes, last week we saw the diverse ways that it was done through that application.

MR. ARNDT: I think the point here is that the assumed failure going into this is you lose everything associated with that particular digital system. That may or may not include the indication, which may be a different system; it may or may not include the manual push buttons and things like that. If they happen to be on the same system, you'd have to take that hit, and you are probably not going to be able to do manual operator actions, because you don't have the indications.

MEMBER BROWN: Well, generally the indications come from the four - if you have four divisions of reactor protection systems in the plant monitoring, that's where the indications come from.

MR. DESAULNIERS: Yes, but they don't come through the same microprocessor necessarily, and you are taking the hit on the - the thing that is common and could fail because it's a digital system, in most of the designs, the indication is taken off in a different place.

MEMBER BROWN: It certainly didn't look like that from the block diagrams we've seen, at least the three systems I've looked. There was a box with a microcomputer there, and a data bus that goes somewhere. So having it come out ahead was not clear at all.

MR. DESAULNIERS: I would simply say that as part of our ISG-5 we addressed that specific concern by ensuring that when the validation of this is performed, that the operators are only going to use instrumentation and controls that they can show will be available under the common cause failure condition.

MEMBER BROWN: Okay.

MR. EAGLE: I would like to add, we actually have a BTP Branch Technical Position 719, and point four under this talks about a completely independent set of controls, and indications, that are completely diverse from your main systems.

In fact these are the basically non-safety controls that the reactor operator uses to handle the plant just under normal circumstances.

CHAIR APOSTOLAKIS: Okay.

MR. DESAULNIERS: All right.

The four phases of the methodology as proposed by the staff and Dr. Apostolakis, this perhaps addresses the question you addressed earlier, where did we in fact follow on from the industry white paper.

You can see again that we have a four-phase process here as well, and it mirrors it fairly closely, though there will be some differences in detail. And in fact that's reflected in the names of some of those phases where we are emphasizing preliminary validation as opposed to verification of the second step as an example.

The objective of the analysis is consistent with what you saw for the white paper was, the estimated time available for operator action, and time required to perform that action; identify what the critical assumptions are, and the credible operator errors; and then establish what would be an acceptable margin.

Sir? Okay, I thought you were about to ask a question.

CHAIR APOSTOLAKIS: Well, I was told that there is at some point risk information. It's coming? I don't know what to say. It sounds to me it is still pretty deterministic.

MEMBER BROWN: No, if you look at the analysis of all their operator actions and everything, it's very subjective when they go through what they want people to look at. So that becomes - it seems to me it's got to get into some risk informed evaluations.

CHAIR APOSTOLAKIS: Where are there any probabilities anywhere. The word, probability, is it anywhere?

MR. DESAULNIERS: No.

CHAIR APOSTOLAKIS: Okay, now I know.

MEMBER BROWN: It's engineering judgments. With no numbers.

CHAIR APOSTOLAKIS: Why don't you finish this slide, and then we will - I don't know what we will do.

MR. DESAULNIERS: For the analysis, the time available was to use - and again we have discussed this a bit before - methods and realistic assumptions consistent with the Branch Technical Position 719.

MEMBER STETKAR: Let me just cut you off here, so that I can get the point in. It's something that we have been beating around a bit.

The methods and realistic assumptions in BTP 7-19 simply says, use best estimate methods. How - first of all I agree philosophically with this approach; it's wonderful. However, there is nothing in the ISG, there is nothing in the Branch Technical Position, there is nothing in anything that I can read that tells me that I should worry about uncertainty and quantify that uncertainty.

There are several sources of uncertainty. One source of uncertainty is the uncertainty in the time available. That is never mentioned anywhere. There is a huge uncertainty in the time available, because of variability in thermal hydraulics code for a given scenario; slight variations in scenarios within your scenario groups.

So there is uncertainty in the time available. There is huge uncertainty in the time required because of one thing that Dennis mentioned, again, variability of scenarios within a general class that people will look at, variability among crews responding to a particular scenario within that class; and if I'm on a particular crew, my own variability, the thing that Charley mentioned, some days I'm having a good day, some days I'm having a bad day. And my time required to successfully respond will depend on that.

How does the analysis methodology, and your review of those analyses account for those uncertainties? Because I read words like mean value, and I have a little example here if we want to get into detailed discussions where the mean value and the median value both satisfy the criterion, except there is a 35 percent probability that I won't satisfy the criterion, if you do the full convolution of the uncertainty distributions.

So how do you - how does the methodology account for those uncertainties, those realistic uncertainties? Using best estimate methods with realistic assumptions?

MR. DESAULNIERS: I will address the uncertainties associated with the determination of the time required for operator action, but prior to that, as you pointed out, there could be and likely is uncertainty associated with the time available.

Now that is something I'd like the representatives from ISG-2 to address, because that uncertainty with time available is there whether we are looking at time available for operator action or time available for plant response in an automated system.

And what we are basically saying -

MEMBER STETKAR: No, no, no. I'm not talking about margin of error on instrumentation. I'm talking about margin until for example the core uncovers or I get start a fuel damage, or I get a certain pressure or temperature. That's thermal hydraulic analysis; that's not margin of error on instrumentation that will actuate an automatic function.

MR. DESAULNIERS: I wasn't - I understood what you were saying. I wasn't making that distinction, but I think it's still applicable to ISG-02, and that diversity and defense in depth analysis if you are talking about an automated system versus a manual action.

And what we were doing here is just trying to stay consistent with the assumptions and processes that were used with ISG-02. Now that may be recognized as a shortcoming on both of these approaches, but it's -

MEMBER STETKAR: Also before - you said you were going to address the uncertainty and the time required. Recognize that a margin for error is not the same as uncertainty in my response time. I have - there are variabilities in the time required to perform a successful response because maybe I'm a slow reader, for example. Maybe my leg hurts today and I can't really get there within 30 seconds. And that is not compensated for necessarily in a margin to recover from an error in the fact that I selected the wrong switch and I want to recover from that error. So just keep that in mind.

MR. DESAULNIERS: Yes.

CHAIR APOSTOLAKIS: Why is this analysis realistic? Why isn't it conservative?

MR. DESAULNIERS: Because this is a beyond-design-basis event.

CHAIR APOSTOLAKIS: Yes, but still, to be realistic when you have operator actions is a little bit difficult to defend it seems to me.

MEMBER BLEY: You can I think with the uncertainty, if you quantify the uncertainties.

CHAIR APOSTOLAKIS: Well, okay, but they are not quantifying. It seems to me they could address these uncertainties and say, you know, being conservative we will go with this.

MEMBER MAYNARD: The best estimate is a conservative analysis. It's just not as conservative as an Appendix K analysis, but it's not just, you go through and you take your best shot at where you think the average might be or whatever. There are some built-in conservatisms in the best estimate. It's not as conservative as an Appendix K.

CHAIR APOSTOLAKIS: In this case I don't think it's well defined. You see when you are doing thermal-hydraulic analysis, maybe a best estimate is better defined. But here, I don't know what is a realistic or a best estimate.

MEMBER MAYNARD: Yes, and I think maybe for operator action.

(Simultaneous speakers.)

CHAIR APOSTOLAKIS: The thermal-hydraulic, I understand that.

MEMBER BROWN: But referring to John's comment, for manual operator action I would think you'd want whatever analysis you do to show that you don't uncover the core, with these - if you are going to take credit for it, you don't want the thing to melt. I mean am I wrong in that thought process? Isn't that the objective?

CHAIR APOSTOLAKIS: Is that the idea?

MR. ARNDT: There is a specific acceptance criteria on what level of damage you are permitted to have.

MEMBER BROWN: So it's not zero?

MR. ARNDT: No, you have to meet the Part 100 safety goals.

MEMBER BROWN: The BTP said -

MR. ARNDT: The criteria for this analysis was established by commission policy, what the level of -

MEMBER BROWN: You are saying I have to agree because we agreed -

MR. ARNDT: I'm saying I have to agree.

(Laughter.)

CHAIR APOSTOLAKIS: Are you familiar with the Halden experiments?

MR. ARNDT: Yes.

CHAIR APOSTOLAKIS: And they found significant variability in the time to respond? I mean every now and then you have four crews or five crews that do it within a minute or two, but then there is one crew that goes 11 minutes, I remember.

MEMBER BLEY: Doing exactly the same thing.

CHAIR APOSTOLAKIS: Doing exactly the same thing. I mean what did we learn from that? How does that inform what we are doing here?

MR. DESAULNIERS: Ultimately in the integrated system validation, that - the criteria there would be that that validation needs to be done, run by using all the crews available to confirm the operator response times, so you are going to have multiple crews performing these - performing these actions. And I believe that goes to some extent to address the question about, there will be variability amongst crews.

All crews will ultimately have to be able to perform the action, show that they can perform the action within the time available.

As well as, there is the potential for operator error, and that is where we get into the discussion of margin here. We did not opt to pick a deterministic margin value either as a set amount of time or fraction of time. Margin is based on an analysis of the actual actions that are required, a human reliability analysis of those actions, what are the credible errors, and ensuring that there would be adequate time to recover from a credible - whatever credible error requires the greatest amount of time to recover from, that is what we are recommending as the margin to deal with the potential that operator error will - I mean operator performance will not be perfect in these circumstances.

CHAIR APOSTOLAKIS: So you mentioned the word, validation. You will come back to it later, right?

MR. DESAULNIERS: I will discuss it in

detail.

CHAIR APOSTOLAKIS: Okay, let's move on.

MR. DESAULNIERS: Okay. This just quickly is for the analysis phase, similar to what we discussed in the industry white paper. There can be used table top methods. This is your initial cut at developing what is the time required for the operator action, ranging anywhere from doing operator interviews to using the ANSI standard.

We put a caution in the guidance with respect to using that 58.8 standard because of some of the limitations we have already described. It is what we consider an appropriate methodology for basically decomposing the task. But it is the number values in there, or the times, are not necessarily appropriate for this application. But again this is just the initial analysis, and these other methods are available.

CHAIR APOSTOLAKIS: Where in this set of bullets would you consider the possibility of expert opinion biases, optimistic estimates and so on?

MR. DESAULNIERS: Well, that would be addressed in the next phase, the preliminary validation. Yes, there is the potential for bias in these expert opinions, say from the operator interviews. And that is why we require that the preliminary validation have a certain level of independence in it so that you can potentially pick up on those biases and counter that through the preliminary validation phase.

We provide review criteria for the analysis that addresses these various topics. I'm not going to go into detail on the specific review criteria under each of these, but we do provide an example here on this next slide with respect to the estimated time responses of operators is sufficient to allow successful execution of applicable steps in the symptom function based EOPs, and there was discussion previously here with respect to having a symptom-based response.

Now there could be optimal recovery procedures that would bring to the operator to the appropriate endpoint more quickly, but we want adequate time such that if that approach is not viable or appropriate, that they can at least use the symptom-based procedures in order to be able to respond to the event.

Also the initial control room staffing size should be the minimum assumed in the tech specs, so there is some conservatism perhaps that normally you will have nominal staffing, but we want to ensure that these actions can be performed by the minimum staff available.

Now the next slide goes into the preliminary validation, and this is to be independent confirmation of the analysis. Now we recognize that there are some limitations on this independence in that this process is iterative, as applicants are developing their designs and there would be perhaps feedback.

But the point here is, you want an independent group of experts reviewing this analysis, coming in with different methodologies to try to provide some convergent validation on the analysis phase. So we are looking for them to use diverse methods, and use methods that are as realistic as the maturity of the design would allow.

The examples here, again, raise from table top analysis on through real-time validation using the part task simulator.

CHAIR APOSTOLAKIS: I'm wondering again, have you actually gone through this process using specific example case studies? Have you actually done it?

MR. DESAULNIERS: No, this process has

not been piloted.

CHAIR APOSTOLAKIS: So how do we know that there may not be issues? I don't know, it seems to me that all this is a group of people thinking what would make sense to do. Does it have any validation so to speak by trying to do it? I still don't know what kind of common cause failure we are talking about. Do you plan to do that? Or you will wait until the licensees start submitting applications?

MR. DESAULNIERS: There is no specific plan to pilot this guidance. I can only say that our experience from many of the methodologies here and concepts are not unlike what the NRC has been using more broadly as part of its human factors engineering program. So it's not considered as breaking completely new ground.

CHAIR APOSTOLAKIS: I guess my question is, does it make sense to ask for a pilot here? I mean a pilot program? That is usually the way the staff makes sure that whatever they have in mind makes sense in real life.

MR. DESAULNIERS: I can tell you that there was some discussion of trying to do a pilot as we were developing this guidance, but the need for getting guidance out ultimately overrode the time available for piloting this. So we wanted to get some available out on the street that was -

MEMBER MAYNARD: Well, you don't really have anything in front of you to pilot at this point, do you? Whoever comes in first needing the operator action credit or wanting it is going to basically be the first pilot, correct?

MR. DESAULNIERS: Yes, otherwise you'd have to be creating -

CHAIR APOSTOLAKIS: Hypotheticals.

MEMBER STETKAR: I think the thing we've got - EPRI is trying to - you know, that EPRI report that we are not getting to in this subcommittee meeting I think was essentially an attempt to do, not quite from the time comparison, but basically from that same basic philosophy to justify no automation of no particular functions in DAS.

So it's clear that the industry is working on it, not necessarily from a particular design, but there is apparently some dialog going on.

MR. DESAULNIERS: Okay. Similar to what we have provided for the analysis phase, here again are just the high level topic areas for preliminary validation. We have provided review criteria in each of these areas.

MEMBER BLEY: Just back to that last thing, how would this fit into say we've got a design cert out there already, and it has a lot of DAC in the I&C system, when they get to the COO stage and come in they will have to have their procedures. And those would include human actions. And I guess that is at the point that this would have to be applied; is that right? Or is it another phase?

MR. DESAULNIERS: Right, the COO will ultimately be implementing the integrated system validation phase as part of an ITAAC.

MEMBER BLEY: And somehow this stuff will be part of the ITAAC review?

MR. ARNDT: Yes, depending on the level of detail and the design cert versus the COL, they will have made a design decision on what they want to do.

Our review of that, depending on the detail, will include the analysis phase, and perhaps the preliminary validation phase. But the final validation, the integrated validation, will be part of the actual ITAAC validation for - the current generation plant for an update, the preliminary validation probably doesn't make any sense, because they already have a simulator. They can do the full integrated validation at that point.

MR. DESAULNIERS: And I think I failed to mention that that probably was part of the bullets that this preliminary validation really is not applicable to systems in place.

MEMBER BLEY: I'm sorry, it's not applicable to?

MR. DESAULNIERS: To currently operating plants that are just doing an upgrade.

MEMBER BLEY: But this will - I'm just trying to see hot this fits together. Because the whole process is a little unclear to me. From the stuff that was talked about earlier that you have going on in the region, and at NRO, to write essentially validation criteria for the DAC all have to use this to factor that into those validation criteria.

What I didn't hear earlier, is there a schedule for when some of that is going to be really put together? It sounds like it is work that is going on.

MS. HERMANN: Deborah Herman, NRO. Are you talking about the DAC ISG?

MR. DESAULNIERS: No.

MS. HERMANN: With the schedule for that?

MEMBER BLEY: Well, earlier there was DAC, ISG, and also validation criteria being developed by - out in the regions and at NRO, kind of parallel to that.

MR. HILAND: This is Pat Hiland. We don't have a schedule available right now to give you. That's Loren Plisco, the deputy regional administrator, in Region 2, and the work that he is doing to develop that. I don't have a schedule for you now. I'll check and give you that information.

MEMBER BLEY: Yes, if you would. If it's something within the next year, or is it - fairly soon I guess.

MR. HILAND: Right.

MEMBER BLEY: Okay.

MR. DESAULNIERS: Okay, the preliminary validation results again we are talking about in this case applicable to Part 52 applicants. The results would be documented in the D3 analysis, the diversity and defense in depth analysis, for review. Ultimately it should support high confidence at that point that ultimately these operator actions will prove out in the integrated system validation.

If there are unacceptable results, that being that the operator action time required is greater than the time available, that would require modification of the D3 coping strategy, and that could range from modifying the operator action to somehow streamline it, i.e. through a redesign of the procedures, or the interface, or change some aspect of operator training perhaps. Or that could go all the way to determining that those approaches would not be effective and automation - an automated DAS for that function would be necessary.

CHAIR APOSTOLAKIS: So what is the definition of validation here? Maybe I missed it. What do you mean by validation? Confirm operators are able to perform: how do you do that? A simulator?

MR. DESAULNIERS: And this will be the discussion of integrated system validation which will explain the methodology used there. So this is the ultimate validation of the action.

CHAIR APOSTOLAKIS: The applicant then will have to tell you, we ran this simulation exercises. This is what we observed, and here are the conclusions we drew from those?

MR. DESAULNIERS: Yes.

MEMBER BROWN: And for plants upgrading this is all that you would do? They wouldn't do the preliminary stuff; you stated that a minute ago but it's also in here, that they would skip right from the beginning to their own simulator, and then they would use strictly their simulator based -

CHAIR APOSTOLAKIS: So all the other stuff is for the new reactors.

MEMBER BROWN: New reactors, yes.

MR. DESAULNIERS: So the expectations for this -

MEMBER BROWN: I didn't say I agreed with that; I just said that's what --

MR. DESAULNIERS: Expectations would be that they would be using a plant reference simulator that is capable of realistically representing the normal operational occurrences and postulated accidents; that they validate the time required using both nominal and tech spec minimum crews. Again, this can be accomplished as part of the human factors engineering program.

CHAIR APOSTOLAKIS: Those are going to be some interesting cases. I remember again from Halden qualified crews did everything within six minutes with plus or minus a minute, and then a fifth crew took 11 minutes.

MR. DESAULNIERS: We will get to that in terms of the specific criteria for performance times.

CHAIR APOSTOLAKIS: Okay.

MEMBER STETKAR: I wanted to ask you, the one thing that if you could back up a slide, I don't remember which bullet it was, back up - there you go - these plant reference simulator, realistically capable of simulating the AOO or PA with the common cause failures.

That presumes a lot of knowledge on the part of the simulator developers that may not necessarily exist today, doesn't it? I'm thinking of near term things like Oconee for example would have to conform with this guidance. Does in real time does the Oconee simulator - I recognize that it realistically evaluates the AOOs and the Pas. What I'm worried about is this common cause failures of the digital I&C system which we don't necessarily know what they are going to look like, do we, the failure modes?

MEMBER SIEBER: Maybe I can help a little bit with that. The problem is, you have to identify in advance what the common cause failure is to simulate it. So the question is, are you smart enough to identify all these things in advance.

MEMBER STETKAR: That's my whole point.

MEMBER SIEBER: Once you tell me what it

is, I can sit down and figure out how to make the simulator do that. The question is, you can't tell me what to do.

MEMBER STETKAR: That's right. And what I'm talking about is realistically in real calendar time now, in terms of the resolution of simulators. And the common cause failure may not necessarily be, all the screens just go nice and clean and pretty and black. In fact that is probably not the common cause failure -

MEMBER SIEBER: It could end up just being misleading. Because calculated functions aren't going to get a zero or infinity.

MEMBER STETKAR: Hal could be trying to do things that you really didn't expect Hal to try to do.

MEMBER BROWN: Well, you could have a screen start blinking, and the other ones not blinking.

MEMBER STETKAR: It's not just blinking.

MEMBER BROWN: I'm just saying, that is an example.

MEMBER STETKAR: - drive the bus off the cliff rather than for example steering in the direction of the skid. My real question is in terms of promulgating these guidelines, I got hung up on these requirements that you have to have a plant-specific simulator that is capable of modeling those common cause failures.

If we as an industry don't even know what those failure modes are.

MEMBER SIEBER: I'm convinced that a good simulator operator can model them if you tell them what to do. The problem is, what do you tell them to do?

CHAIR APOSTOLAKIS: So let's now pretend we are members of the staff. In light of this poor state of knowledge, what would they do? They have to do something.

MEMBER SIEBER: And they are doing it.

CHAIR APOSTOLAKIS: And they are doing it. Okay.

MEMBER BROWN: I mean, default to 30 minutes.

CHAIR APOSTOLAKIS: Do what, I'm sorry?

MEMBER BROWN: Default to 30 minutes, I guess. That's at least the initial default position as opposed to - it's not like it's proposing something less than that. You're automatic - show me why you can even do it in 30 minutes.

CHAIR APOSTOLAKIS: I would like to have some defense in depth in the ISG itself, not - I mean in other words if this thing doesn't work what is going to save the day? Because the state of knowledge seems to be so poor that you guys are doing the best you can, I acknowledge that. But do we have a backup policy or something, provision, that if something weird happens, and the operators wonder, what do we do, how do we protect ourselves.

MEMBER MAYNARD: How many layers of defense in depth do we need? We are already talking about a beyond-design-basis event. We are talking about that. This is an interim staff guidance. As far as from a regulatory perspective, the regulator always has the ability to make changes if there are things that weren't considered taking place; there are processes for doing that.

You have to be careful how many layers of defense in depth that we require.

CHAIR APOSTOLAKIS: Yes, but this seems to be particularly - I mean -

MEMBER SIEBER: Well I'm not sure it's as bad as we picture it. Because this is a backup to a backup. We are asking for a backup to that backup. And you know how far do you go?

I think that you don't have to be able to identify the exact common cause failure to say, I failed these many things; can the operator deal with that?

MEMBER MAYNARD: The main thing we are looking at, and I know there are lots of ways things can affect it, but what you are really looking at situations in which the reactor protection system didn't do its job when it was supposed to, and the SFAS didn't do its job when it was supposed to.

And you know do you have the ability to recognize that? And I know you can come up with an infinite number of things that could happen. At some point you have to say, enough is enough, and this is a reasonable approach to testing and verifying this.

CHAIR APOSTOLAKIS: Or put another way, this is an action or event that would be required when something that is already very rare has happened. Is that the same thing? Already we are in very low probability.

MR. ARNDT: Let me try it this way. First of all this is a staff guidance. So the way we anticipate it being used - obviously it will be used in other ways - but the way we anticipate it being used is if the licensee chooses this design strategy, and they go down the path of doing a preliminary validation, when they come to integrated validation, we would expect to see in their analysis the use of a plant reference simulator that is capable of performing the transients with a reasonable realistic representation of CCF.

That is to say, if we saw just the screens going blank, that would be guidance to the staff that that is probably not sufficient. However if we saw a set of criteria that the plant and the I&C designers had thought through based on the failure modes and effects analysis that would be representative of the kinds of things, then we would say yes. That is what we are trying to articulate here.

MEMBER STETKAR: That is good, and I would hope that the ISG would perhaps articulate that a little bit more clearly. Because the thing I hung up on in practice was, if I'm an applicant coming in tomorrow, I'll use the word Oconee, coming in tomorrow, saying I have this strategy, and I have now performed my integrated system evaluation, my validation. Here is my analysis. Am I now going to be held hostage because the staff doesn't accept the fact that my simulator has enough capability to realistically represent those common cause failures, whatever that means.

So the thing you said about a reasonable event derived from engineering evaluations of FMEAs would help an awful lot there. Because the process is good. But that was one pitfall that I could see that would just hold it up in terms of the kind of a discussion we are just having here, incessant discussions about how many different failures and what sort of failure modes and what combinations of things constitute acceptability for that realistically representing the CCFs.

CHAIR APOSTOLAKIS: I think the situation here is that the details are not perfect, but the fact that they will have to go - both the applicant and the staff - will have to go through this process adds an extra layer of defense in depth which is not at the front line. I mean already many things must have happened for us to rely on this.

So from that perspective I think it is reasonable. I mean if I relied on this to save the day, then there would be thousands of questions about the common cause failures and what is the operators - what are they seeing and so on. But given its place in a risk-informed environment, I'm inclined to say this is valuable.

This is not the only thing I'm relying on. This is after many things have happened. And that is very critical here. So by asking the staff and the industry to go through this process, yes, we are benefitting. There is a benefit in doing that. That makes me feel a bit better. I know Charley doesn't feel better.

MEMBER SIEBER: That's right.

CHAIR APOSTOLAKIS: That's fine. That's why we are 15.

(Laughter.)

MEMBER MAYNARD: Any applicant that comes in wanting to credit operator actions within the first 30 minutes as their diverse actuation system it's not a guaranteed - it's a risky approach because it is going to require judgment in satisfying the staff in these criteria. So I think -

MEMBER STETKAR: But let me - something I asked earlier - even if someone wants to credit operator actions after 30 minutes, they have to go through this process; is that correct?

MR. DESAULNIERS: Yes.

MEMBER STETKAR: So the justification is just more onerous now if the time available is less than 30.

CHAIR APOSTOLAKIS: In fact this is independent of the 30 minutes.

MEMBER STETKAR: That is right. I wanted to make sure I understood that. Thirty minutes only appears once in the introduction.

CHAIR APOSTOLAKIS: Is the earlier statement that we don't credit anybody for less than 30 minutes still valid?

MR. DESAULNIERS: No.

CHAIR APOSTOLAKIS: This is replacing now that?

MR. ARNDT: In point of fact there are no absolutes. The interim staff guidance in ISG-2 is a guideline that says, if it's greater than 30 minutes we are not going to look at it quite so hard because we have a higher confidence it's probably right. If it's less, it doesn't say we are not going to allow it; it just means we are going to look at it a lot harder. You are going to need a lot more evidence.

CHAIR APOSTOLAKIS: But these are for beyond 30 minutes.

MEMBER SIEBER: And in fact today there are backup operator actions required at a couple of plants that are 10 minutes.

CHAIR APOSTOLAKIS: So should we flatter

ourselves and say that this is the staff's response to the ACRS comment that you should look more carefully into the 30 minutes?

MEMBER SIEBER: I think that's what I wrote down.

CHAIR APOSTOLAKIS: We did recommend that, and you are doing all this, so it seems to me that that is a good response. Can you finish in 25 minutes, David?

MR. DESAULNIERS: Yes.

CHAIR APOSTOLAKIS: You can, right? It's the rest of us.

MR. DESAULNIERS: I'm prepared to in the time required to come up with a margin --

CHAIR APOSTOLAKIS: That's your best estimate, I assume. Okay.

MR. DESAULNIERS: Okay. Here an overview again of the various review criteria topic areas. We were talking some about the simulator. I want to go on to provide an example of the performance time criteria, which I think will address, again, some of the concerns and discussion earlier in this meeting.

I'll just simplify this and say, for each event or each simulation, the mean performance time - no, I don't want to say simulation, I'll say event -

the mean performance time of the crew is less than or equal to the estimated time required derived from the analysis phase.

MEMBER SIEBER: So some crews will fail? Is that how I interpret that? Some crews will not make the time, right?

MR. DESAULNIERS: Yes. So the average time has to be less than the time - excuse me, I misspoke. Because this is relative to time required, okay. Not time available. Okay.

MEMBER STETKAR: That is some required without the margin.

MR. DESAULNIERS: Without the margin. So you've done an analysis. You've determined how much time in the analysis phase you thought was required. Now you are actually running crews, and you are looking at basically was my analysis on target? Did I bound the time required with - in my analysis? And in that case you are looking at - and so here you are using a mean for that case.

Whereas in the next circumstance here, the second bullet, you are looking at the performance time plus the margin, and you are looking at that relative time available and each crew needs to be successful in that case, because you are looking at time available plus margin.

CHAIR APOSTOLAKIS: Tell me why is I satisfy the second bullet I don't satisfy automatically the first? I'm a little confused here. The second one seems to be more demanding. So if I do that then it seems to me the mean performance time will be lower, won't it? Or is there something I don't see. You are asking that for each - right - each performance time - I mean the performance time for each crew, including margin, must be less than the time available. Then it seems to me the average will be.

MEMBER SIEBER: Yes, that's right. You could skip the first bullet.

CHAIR APOSTOLAKIS: Yes, that's what I'm saying.

MR. DESAULNIERS: The purpose of the first bullet is to ensure that there is a consideration back to the analysis to ensure that there was adequate consideration of the analysis phase. But there is not something that you missed, or that your analysis was off for some reason.

CHAIR APOSTOLAKIS: I don't see that. I think if you satisfy the second bullet, the first is automatically satisfied.

MEMBER SIEBER: That's right.

CHAIR APOSTOLAKIS: So I would delete it.

MEMBER SIEBER: It just says that -

CHAIR APOSTOLAKIS: Think about it. You don't have to make a decision right now. The staff never makes a decision at these meetings.

(Laughter.)

CHAIR APOSTOLAKIS: They take it into consideration, consult with senior management.

MEMBER SIEBER: That gets back to the question on slide 38 where you say, high confidence that they will do it. High confidence is in the margin.

MR. DESAULNIERS: The next slide just again is similar to the preliminary validation slide with regard to what you do -

MEMBER BROWN: One other question on this. If you've got the acceptance criteria that you are going to accept, forget the argument about which bullet it is, let's just assume it's the second bullet, the licensee doesn't know that - is that written down in this integrated system validation assessment?

MR. DESAULNIERS: That criteria, yes it is.

CHAIR APOSTOLAKIS: It's what?

MR. DESAULNIERS: It is in the ISG, the specific criteria I had on the slide here.

MEMBER BROWN: Oh, there it is. Okay, fine, go ahead. I quit. I just wanted to make sure they got it.

(Off record comments.)

MR. DESAULNIERS: Again unacceptable results would require modification of the D3 coping strategy, and I previously provided examples of what that could entail.

CHAIR APOSTOLAKIS: So David, let me understand something else. Put this thing in the big picture. Suppose they fail miserably. And you don't give any credit for human action. What is the consequence to the licensee? They have to put some automatic stuff?

MR. DESAULNIERS: Yes.

CHAIR APOSTOLAKIS: Wow.

MEMBER BROWN: How about more training?

MEMBER BLEY: The example was failed miserably and they can't do it. And so going back again, I will reiterate the range of what does it mean to modify the D3 coping strategy. They could go back and say, we are going to somehow streamline our procedures so that these actions can be implemented more quickly. They could do it by somehow modifying their interface in a way that would provide for more rapid operator response.

So those are alternatives I expect would be explored prior to just going back and saying, we are going to just automate.

CHAIR APOSTOLAKIS: So coming back to Mr. Maynard's comment earlier, how much defense in depth do you want, let's say this is the third level of defense in depth. We take it for granted that this level is needed. So if you don't meet it with operator actions you have to do something else. That is really the attitude we have, that something needs to be done at this level.

MEMBER MAYNARD: Well, they either have to meet this criteria or they have to put in an -

CHAIR APOSTOLAKIS: That is what I'm saying.

MEMBER BROWN: Okay, so we are assuming a third level reactor protection system, SS is number two; if that doesn't work, we can have operator action, or if they fail, they have the diverse -

CHAIR APOSTOLAKIS: Which themselves are redundant; let's not forget that.

Okay.

MR. DESAULNIERS: I'm going to touch on the long-term monitoring very briefly. That is just ensuring that these actions that are credited will remain feasible and reliable on the long term. So we want to ensure that nothing has changed in the design over time, or in the way operators are trained, that would compromise the ability to perform these actions.

CHAIR APOSTOLAKIS: What is the definition of reliable? I remember there was one in the fire case. We are in the deterministic world here. Why don't we just say physical? Reliable is a red flag. What - how do you convince yourself they are reliable.

MR. DESAULNIERS: The principle I think was where we were at the white paper when we had no margin between time available and time required.

CHAIR APOSTOLAKIS: I understand that.

MR. DESAULNIERS: And so no capability, so my definition in this context of this, reliable is that they continue to have the ability to respond.

CHAIR APOSTOLAKIS: I would say in this context if you have significant margin between the time available and the time required, then it stands to reason that this is a reliable action.

MR. ARNDT: Yes, it's a qualitative judgment.

CHAIR APOSTOLAKIS: Now of course what is a reasonable margin - but I understand. You have to make some decisions. Okay.

MR. DESAULNIERS: It's credible, maybe sets a lower threshold. I'm looking at this - we were looking at nonsafety-related equipment capable of sufficient quality to ensure it can perform under - that is the alternative if you compare it to that.

CHAIR APOSTOLAKIS: Okay, good.

MR. DESAULNIERS: Okay, again, these are the specific review criteria associated with long-term monitoring. There is nothing particularly special or magic with these criteria. It basically says you will have an effective corrective action program. You will have a means for identifying and tracking this long term.

MEMBER BROWN: There is one statement in your thing that says, accordingly the vendor licensee applicant should establish a strategy for long-term monitoring of operator ability to reliably perform the manual operator actions credited in a D3 analysis. So if you have determined that the operator action becomes the third level, no automated backup is required. That means you have to have a continuous validation program for - as a crew may change if you bring in a new individual, or - and that has to be ongoing.

MR. DESAULNIERS: One way this could be implemented is that this is reflected in the operator requalification, so that scenarios for operator requalification may include at some frequency common cause failure scenarios. Those would be evaluated, and if there were indications that they were not able to -

MEMBER BROWN: But then you have to maintain - it seems to me it is more than just a guy finishing a qualification card that he has been through a set of - you have to monitor and track response times to these scenarios, so that you can have a continuous track at all times that you still meet the - whatever that second bullet is.

So you've got to have a continuous ongoing track for 30 years of the - whatever the second bullet meant, and you have to have that documented and available for audit. That's the way I would read it.

MEMBER BLEY: It's the same as any other operator requal training.

MEMBER BROWN: It's a little more

extensive than that because there are numbers, there are timeframes involved other than guys finishing -- going through and being able to answer questions and turn the right switches and push the right buttons and it responds to certain indications.

MEMBER MAYNARD: But typically things like this, if there is a time requirement for your requal exams, that becomes one of the success criteria; success/failure criteria is whether or not you met the criteria. And then if you failed it's going to get documented.

MEMBER STETKAR: It's like emergency boration for an ATWS event if that is part of your training.

CHAIR APOSTOLAKIS: So this regulatory guide will come to us for review at some point, right?

MR. DESAULNIERS: That's part of the normal process.

CHAIR APOSTOLAKIS: This was just an informational meeting today?

MR. ARNDT: When we originally briefed you on this, the steering committee, three or four times ago, the committee asked us to come to you from time to time to provide information on the ISGs and the ISG development process, so you could provide input to the development for the ones that are still under development, and input for their final revision into the reg guides for the ones that were complete.

So this is -

MEMBER BROWN: They are expecting a response at the - from the April meeting.

MR. ARNDT: We would like you to provide your input as to whether or not you think this is adequate as a -

MEMBER BROWN: We're expecting a letter on this and ISG-6 in April, after the April meeting.

MR. ARNDT: - input as to what improvements we can make when we draft it into the guide.

MEMBER STETKAR: To kind of follow up on that, do you have a schedule for the reg guide yet?

MR. DESAULNIERS: No, the draft reg guide we are targeting for later this year, but there is no specific -

MEMBER STETKAR: Well, in particular, for example, because this would cover the Oconee upgrade, the Oconee upgrade will be done completely under the auspices of the ISG, or at least -

MR. DESAULNIERS: Not even under the auspices of the ISG, frankly, is that the ISG would have needed to have been out six months prior to that action.

CHAIR APOSTOLAKIS: In any case when the guide is drafted you will also come back?

MR. DESAULNIERS: Yes, as part of the regular guide process.

CHAIR APOSTOLAKIS: Are you done, David?

MR. DESAULNIERS: I am finished.

CHAIR APOSTOLAKIS: Any comments, questions from the members?

MEMBER MAYNARD: I do have a comment. For the record, our discussion may imply that operators are unreliable and make a lot of mistakes, by the way we were probing into this. I'd just like to go on the record and say that today's operators are well trained, and typically perform very good. While there can be variability in times, typically if there is a timeframe that they are aware of, they manage that. If there is not one, well then of course you will see a lot more variability in that.

And yes, operators can make mistakes. But also they have the ability to recover from that, which some automated systems and some other things do not have.

So I recognize it is an important aspect.

We do need to take variability into account, and we do need to make some assumptions if there is failure. But I just want to go on record as saying today's operators are highly qualified and perform very well.

MEMBER BONACA: Personally, I agree with you. My only thrust in the questions was regarding realistic analysis and trying to understand the basis for the judgment and what we can get from that realistic analysis, what kind of range. And I think we got sufficient information here to have some understanding that there is a focus on that.

CHAIR APOSTOLAKIS: Any other comments?

MEMBER BROWN: So if anybody has any observations they would like thought about, they ought to feed them to you for your letter in April.

(Laughter.)

CHAIR APOSTOLAKIS: This is your letter.

Does the staff want to say anything? Well, it looks like we are going to lunch. And we will come back at 1:00 o'clock.

(Whereupon, the proceeding in the above-entitled matter went off the record at 11:51 a.m. and resumed at 1:01 p.m.)

CHAIR APOSTOLAKIS: Okay, we are back in session. The next item is review of status of ISG-6 licensing process.

REVIEW OF STATUS OF ISG-6 LICENSING PROCESS

MS. JAMES: Good morning, or good afternoon. My name is Lois James, and I'm the lead for Task Working Group No. 6.

Up here at the table with me is Jerry Wermiel. He is our senior adviser for instrument controls and NRR; Bill Kemper, who is the branch chief for instrument controls and NRR; and Ed Miller who is the licensing specialist assigned to Task Working Group No. 6.

Since Ed and I have never actually been a presenter at your committees, either subcommittee or full committee, we are going to take a few minutes and introduce ourselves.

MR. MILLER: My name is Ed Miller. In addition to this responsibility I am currently the PM for Oyster Creek. I've been with the agency since 2001. Began in I&C review section in NRR, but I spent the last five years in licensing work on plant issues and policy and procedure development.

Prior to here I worked in student programs with the U.S. Geological Survey.

CHAIR APOSTOLAKIS: The U.S. Geological Survey? Doing what for them?

MR. MILLER: Actually I was doing lab work out at the Abderdeen Proving Grounds, headspace analysis for environmental recovery.

CHAIR APOSTOLAKIS: All right.

MS. JAMES: As I said, my name is Lois James. And I joined the NRC in 1997 as an engineering inspector in Region #1. I then proceeded to be the resident inspector at Indian Point from 2000 to 2003. Yes, I was there on 9/11, so that's yes.

Prior to joining the NRC I worked for Bechtel Power Corporation as a licensing and analytical engineer, and I also worked for DOE as an environmental contractor.

Now on to Task Working Group No. 6.

CHAIR APOSTOLAKIS: So you don't want us to introduce ourselves?

(Off record comments.)

MS. JAMES: Oh, I have your names. And I've actually done research.

We will be presenting an overview of the licensing process that we are working on for digital instrument control license amendments.

This is going to be based on LICI-101, which is our current general license amendment process. But we are adjusting it and highlighting for digital instrument controls.

We are going to be talking about the format of ISG interim staff guidance. We are going to talk about tiers of complexity to give us an idea of what the review is going to entail.

We are going to talk about the phases of the process. By the phases, we mean what information is going to be submitted when; what we are going to do at different points.

Areas of review: we are going to be talking about how we are going to bin all the different clauses and requirements into areas of review, thereby allowing us to use topics instead of clauses.

And then we are going to tell you what our path forward is, and what our schedule is, and throughout the whole entire thing we will be communicating with questions.

So the purpose of the ISG: we already have guidance regarding digital instrument controls in Chapter 7 of our NUREG standard review plan. That is our guidance. That lists all the clauses we need to review, all the clauses the licensee needs to submit to.

This licensing process is going to better define what information we want when; when we are going to be doing specific parts of the review; we are acknowledging the fact that digital amendments and projects do not proceed on the same flow as other amendments and processes.

Not all the information is available when they submit the amendment. Things happen at different points. Testing happens at different points. And that's what we are trying to incorporate into this licensing process.

A big part of this also is going to be knowledge management. We have a lot of new engineers and reviewers coming into the NRC. We have a lot of new engineers coming into industry. We are going to use this as an opportunity, especially using our areas of reviews, to educate and transfer the knowledge from generation to generation.

The last thing we are going to do is, we are going to learn a lot from the current reviews that are going on. We are going to learn a lot from Wolf Creek, and we are going to learn a lot from Oconee.

They were not pilots for this. We are going to use the lessons learned. We have learned a lot, and we are going to educate and inform this process.

The next slide is an overview. It contains items that are currently in our license amendment review process.

Our Phase 0: preapplication phase. During this phase we are going to be strongly encouraging public meetings, through which we are going to discuss the complex topics. We are going to discuss D3, we are going to discuss V&V plans, our intent is that we are going to take the public meetings a little bit further than we have in the past. The outcomes of public meetings are summaries. Our summaries are going to be more detailed. We are going to put in there, we agree in concept with where you are going with D3, for example. Based on what we have seen, we think you are on the right path. We are going to be using those words in an effort to induce regulatory uncertainty, to let the industry and licensing know that we are okay up to here. We need more information on this. And we are going to use those meeting summaries to inform our acceptance review.

Phase one starts when the license amendment comes in house, and the first thing we do is an acceptance review. We hope that the acceptance review will go simple, will go easy, because of the public meetings and the public meeting summaries that we have had. We will be able to checkoff a lot of the items, we're hoping, during the acceptance review, based on the meeting summaries that we have previously produced and made public.

Pages one and two are our detailed technical review. That is where we are going to issue our RAIs. We are going to talk about items of interest -

CHAIR APOSTOLAKIS: Excuse me. Are we talking about any licensing activity including existing reactors, or only new reactors?

MS. JAMES: Only operating reactors.

MR. WERMIEL: This is only talking about amendments submitted under 50.90.

CHAIR APOSTOLAKIS: So this is for existing reactors?

MS. JAMES: This is for existing reactors.

MR. WERMIEL: This is a process intended to smooth if you will an application for a digital modification to an operating plant in accordance with 50.90.

CHAIR APOSTOLAKIS: Thank you very much. That was very helpful. So for new reactors it's something else?

MS. JAMES: It's going to be something else.

MR. WERMIEL: It would be totally different, because new reactors have to deal with this DAC/ITAAC process which we don't have under Part 50.

MEMBER BLEY: But you don't always have a complete design that you are looking at.

MR. WERMIEL: Remember, what we have to do, the finding that has to be made under 50.90 is that there is reasonable assurance that the change to the license can be made. We have to have sufficient information to make that finding.

That finding is made in a very different manner under Part 52, and the COL application process. And this does not apply to that.

MS. JAMES: We do have someone from NRO working on our task working group. Because the level of detail is going to be similar. How we get the information, when we get the information, may be different -

MR. WERMIEL: And who does the review, also, that's a key point here, may be different under the Part 52 licensing process than who would do the review under the Part 50 licensing.

CHAIR APOSTOLAKIS: Can you continue?

Who is going to do what?

MR. WERMIEL: Implementation of DAC/ITAAC. I think it was mentioned this morning that it falls under the umbrella of Loren Plisco in his Region 2 group. There is no team like that in headquarters.

CHAIR APOSTOLAKIS: Okay. That's an interesting expression.

(Laughter.)

(Off record comments.)

CHAIR APOSTOLAKIS: Okay, Lois. Oh, I'm sorry.

MEMBER BROWN: Not all the new plants are DAC-ITAAC. USCPR is not doing DAC/ITAAC.

MR. WERMIEL: Right, it's their choice.

MEMBER BROWN: I brought it up only because the details - let me finish please - is that the license - the stuff you all talk about which you would like to see relative to information submitted for the existing plants is also applicable to a new plant. And I would state, maybe not everybody would agree, that even with DAC/ITAAC that level of information is also required in some form to be able to allow you to determine that the plant is really meeting the general requirements that are specified in all the other documents.

MR. WERMIEL: That's true.

MEMBER BROWN: So DAC, just somebody telling you, yes, we are going to go test it, so you don't need to see anything, is not necessarily sufficient.

MR. WERMIEL: No.

MEMBER BROWN: So that's why I was a little bit - one of my questions was, why is this some of the detail in the process here not also implicit, or would be incorporated for new reactors as well.

MR. WERMIEL: From the standpoint of information needs, and the overall determination based on that information, you are absolutely correct.

MEMBER BROWN: So when we see the DAC ISG that is supposedly in process, we should anticipate somebody from NRC, we should expect some good level of detailed information to support whatever that DAC/ITAAC ISG classifies? You are shaking your head.

MR. WERMIEL: I'm not saying the ISG.

(Simultaneous speakers.)

MEMBER BLEY: It's not what you're here to talk about. But we are interesting in it.

MEMBER BROWN: The only reason to bring it up is, I don't want somebody to say, this is not necessary. This is all OBE for new reactors. And I do not consider it in that -

MS. JAMES: No, and that's why really we had to make sure we had somebody from NRO who is working on that ISG.

MEMBER BROWN: Are they here today?

MS. JAMES: No. He's not here today. But he is part of our working group.

MEMBER BROWN: You can pass the conversation on.

MS. JAMES: Yes. But the individual who's been working with us is not here. I don't see him in the audience.

MEMBER MAYNARD: The same level of detail is going to be essentially needed, but at different times.

MS. JAMES: At different times.

MEMBER MAYNARD: If it's just the reactor, it'll be before it gets a license to be modified. I'm not sure that by the time the DAC gets approved that that level of detail will be there at the DAC process. It would have to be there before fuel loads.

MS. JAMES: How they close the DAC -

MEMBER BROWN: There is a disconnect there, because - in some minds. Maybe only mine.

That approving a DAC, which does not give you a definitive way of identifying and ensuring that all those - that level of detail is going to be satisfied. When you finally get it, if you get it right before fuel load, it's kind of too late, right? The plant is built; the stuff is designed; it's in place.

MR. HECHT: It makes it seem like a gamble.

MEMBER BROWN: It's not a gamble. Now many times is NRC going to say no when you get to that point if the plant is built, the I&C is installed, and now you say, oh, we don't like the way you do that.

I just wanted to throw that out on the table so I could create some consternation.

CHAIR APOSTOLAKIS: The remark has been made. It is recorded. But it is not the question for today.

Myron has a question.

MR. HECHT: I have a really simple question.

CHAIR APOSTOLAKIS: Then you shouldn't ask it.

(Laughter.)

MS. JAMES: I'm glad we're after lunch.

CHAIR APOSTOLAKIS: Okay, Myron, go

ahead.

MR. HECHT: My question was, what is the scope of this guidance, to provide control systems, reactor protection systems, as far as all of the above?

MS. JAMES: All of the above, digital instrument and control amendments.

MR. WERMIEL: It applies to instrumentation and control systems that necessitate the need for a modification to the plant by amendment. In other words if a licensee has decided to implement a digital mod, they go through the 50.59 process, and they decide based on application of the 50.59 criteria that they need a license amendment, then we are going to apply this process to the review of that amendment.

CHAIR APOSTOLAKIS: Myron, 50.59 is - oh you know what it is.

MS. JAMES: Okay, I was getting into phase two. Phase two is where we are going to wrap up the review of the information. We are going to be conducting audits to verify the information that we have seen, verify decisions that we are going to be making. And phase three begins when we issue the SE. That is when NRR's part essentially ends, and it goes into the licensee's implementation and the region inspecting the implementation, and then the maintenance and follow up after that.

MEMBER BROWN: This flow chart is simpler than the one you had in the ISG.

MS. JAMES: Yes.

MEMBER BROWN: And I presume that is just for presentation purposes?

MS. JAMES: Yes. Yes.

MEMBER BROWN: All the feedback loops and stuff like that, that makes it look like nobody is talking to anybody. And no feedback. But in fact there are all kinds of feedback loops in the thing. I just wanted to make sure that I knew that they hadn't changed.

MS. JAMES: Oh, no.

MEMBER BROWN: I'm done on that one.

MS. JAMES: The formatted ISG is going to explain the process overview which we just discussed. It's going to explain and encourage the preapplication meetings; describe what we intend to get out of them, and how we are going to document them. It's going to discuss our acceptance review. We'll be doing it in accordance with our office instruction, but it's going to be based on the meeting summaries.

It's going to talk about review areas. I briefly mentioned that earlier, where we want to group all the criteria that needs to be met into topical areas. So that will all be defined in the ISG.

Our appendices are going to - we envision them giving actual lists of what information is needed based on the tiers of complexity which will be the next thing I'll talk about. We'll go to the tiers of complexity.

During the application meetings we are going to be talking about the tiers of complexity. And what we mean here is, Tier 1, the licensee is referencing an approved topical report in whole, none or minimal changes, you are in Tier 1. NRC review is then minimal. We are essentially verifying that the application is within the topical report.

Tier 2 is when the amendment that is coming in is based on an approved topical, but deviations are being taken. So in that we are going to have to again look at the topic; we are going to have to make sure that what is being assumed is within scope; and then look at all the deviations that they are taking.

Yes.

MEMBER BROWN: Some of the topical

reports, at least in the INC area that I've seen - and if I'm wrong, Dennis or whoever, correct me - but they have been specific to a part of the system, not necessarily the system, like maybe the computer, just the platform, and didn't address necessarily the other lines that moved into that. So that would be looked at as an approved system, the platform. But the plants had different inputs possibly, has some different other auxiliary type systems feeding into it. So I was having a little bit of difficulty with how you don't really - you have not much review effort because it's using an approved platform or an approved system, whether it's a MELTAC or AREVA or Mitsubishi's, whatever they call that one, maybe that's the MELTAC. I can't remember all of them. So that one is a little confusing to me as to how you deal - you make it less, because it's using a preapproved, or one that's already been approved for another project when you've got all the stick-ons for different.

MR. KEMPER: Well, the level of review, let's take the Wolf Creek review for example, they submitted an FBGA platform that had never been reviewed by the staff for a specific application, main steam feedwater isolation, which is a function of their reactor protection system.

So in conjunction with approving that site specific application we also had to approve the platform. And basically we have done a review of the platform in a manner that could have been done earlier by virtue of a topical report that the staff could have reviewed some time ago.

But because it wasn't, we had to do all of it at the same time. So the level of review was considerably higher, because we had to look at the built in diversity of the platform, for example, because diversity, although it was required for the MSFIS application, it's being implemented by the design of the platform itself.

MEMBER BROWN: That is a safety system in that plant?

MR. KEMPER: Safety system, right. So if that had been done by a topical report review earlier, then the MSFIS review would have been far far easier, and it would have been quicker to accomplish.

So that is kind of an example, the MSFIS, the Wolf Creek application took us, well, pretty much two years to get through. I would say we would have expended half that time if we'd have had an approved platform, although I don't want to lead you to believe that just because a platform is approved these plant-specific applications are a piece of cake or a walk in the park; they are not. Because the difference is, you build on these boxes that have been approved. And what we do is, we review and approve an integrated topology using those devices that we have already approved on a generic application.

MEMBER BROWN: The interface may not always be the same between the specific plants. That is more the point. Therefore, at that plant form, it's how you deal with that that can make a big different.

MS. JAMES: But the review would be less because the platform was already approved. So we still - we always have to look at the interfaces, because that is going to be very site specific. But theoretically the overall review will be less, because we already have something preapproved on the books. That is part of it.

MR. KEMPER: The Oconee application, the Teleperm topical referenced this second min second max interchannel communication thing that we have talked to you all before. Unfortunately there was not enough specificity in the topical to explain exactly how that was going to be deployed. So now that we see the

Oconee License Amendment Request, we see that that involves actual interchannel communications. They could have implemented it a number of different ways, but we wouldn't know that until we actually get to site specific implementation of that.

So that's the difference. We approved the concept back in 2000, but now the implementation of that, and the compliance with 603 and 7-4.3.2, and the ISG had to be ensured while we actually reviewed the topical for Oconee - excuse me, the LAR for Oconee.

CHAIR APOSTOLAKIS: Jerry.

MR. WERMIEL: Yes, to some extent these are generalities. What we are tiering the review from the standpoint that we want to provide an assurance to licensees that where they have selected something that the staff has already reviewed and approved, we are not going to go back and revisit those aspects that were previously approved, and previously established to be acceptable.

Those things that have not been, that are still germane to the application of whatever modification they are making will of course have to be reviewed because they weren't part of what was originally approved.

So it's just I guess an understanding that where a licensee can take advantage of something that has already passed muster, the review effort will be much simpler and straight forward than if they are biting off something that we are not familiar with and have not seen before. That is all we meant here.

MEMBER BROWN: I just wanted some explanation of that.

CHAIR APOSTOLAKIS: This is true for regulatory guides too. I mean a licensee is free to choose another approach, and then the review is from scratch.

MR. WERMIEL: You're right.

CHAIR APOSTOLAKIS: Any prior approval by the agency is still valid.

MR. WERMIEL: That is correct. And we are not even intending necessarily to encourage say an applicant to adopt the Tier 1 approach.

All we are saying is, this is how we see it from the standpoint of what's to be expected.

MEMBER BROWN: No, that's fine. I got that part. It's just the boundaries around the thing that I wanted to get some feel from you and ask, that is one of the questions. For instance the interchannel communication, even if it's the same platform, may be different in one plant than in another because the data and the information you need to transfer is different and has a different character.

So you have to look at that piece of it is what you're telling me, even though the box is the same.

MR. WERMIEL: That's correct. It may also be that the licensee is adopting a previously approved platform, but the application that they intend for the system may be something that wasn't originally intended for this particular design. That would have to be addressed.

CHAIR APOSTOLAKIS: Myron.

MR. HECHT: What is the - do topical reports address software only upgrades?

MR. WERMIEL: Topical reports can address software upgrades; it can address hardware changes; it varies.

MR. HECHT: I would imagine that this is - I know that this is for existing systems, but as we move to more advanced control systems, for example, the computers are going to be getting more complicated, we are going to be getting infrastructures, operating systems for lack of a better term; and we might be upgrading those audit systems, and that will end up in the same dilemma we have in the past where if we don't keep up with the vendor, pretty soon we are going to be stuck with an unsupported operating system.

So I guess - and by the way that is not unique to the nuclear industry - do the tiers need to be adjusted, or do additional definitions have to be made for software on the upgrades?

MR. WERMIEL: When we approve a platform we approve the entire hardware and software system, the integrated system.

MR. HECHT: And by entire you mean a specific list of components.

MR. WERMIEL: Yes, exactly, hardware components, peripheral modules, depending on what they submit, all right. It varies from vendor to vendor, the operating software. And also sometimes they give us explanations of system deployments, which we don't approve that but we at least we can see how they intend to operate that.

Now each one of these platforms, the day we approve it they start modifying it just to keep up with technology and obsolescence and things like that.

So what we are trying to work through here is a way that the vendors will come back and submit a supplement to their topical report; it's what we would like as a staff. Unfortunately we have no control over that. But we lobby for this whenever the opportunity presents itself, vendors who will come back and resubmit that updated topical from time to time so that we can amend our SE to approve that.

If they don't do that, then they could still get that done via a license amendment request; and that is exactly what's happening right now with Oconee.

The Oconee mod is using a previously approved system, a Tier 2 piece of hardware, with deviations in both the hardware and the software. And also the programs that were approved for the original platform itself.

So in order to approve this LAR we had to ask the vendor to give us an explanation of all the changes that occurred, then we are going to have to go through that in order to ensure that those changes don't invalidate the conclusions of the SE that was issued initially.

MR. KEMPER: So if I'm a vendor like AREVA, and I want to sell my customers the new operating, I'm going to write you a topical report, get it approved, and then I'm going to go to my customers and say it looks like it's going to be a Tier 1 change, no problem. Is that what you envision happening?

MR. HECHT: if the results of that change would require a submittal to us to approve it, then that would represent a lesser regulatory burden on the licensee if they did it the way you propose; in other words come back to us and get it reviewed and approved independent of a license application. But they don't have to do that.

MR. KEMPER: But if the licensee is a little bit more creative and believes that they have the in house technical talent and they don't do it that way, that means basically that any change would probably be a Tier 2 for software only?

MR. HECHT: Well, they would have to put that through the 50.59 process, and if it screens in, they would have to make a submittal to us and we would review it based on their submittal.

CHAIR APOSTOLAKIS: We are falling a little behind here.

MS. JAMES: Yes.

One of the keys with the tiers of complexity is, we want to discuss that during Phase 0 which is the preapplication phase, or preapplication meetings. And that is one of the things we would love to agree upon between the licensee and us which tier they are in; therefore the licensee and the NRC both understand at least in general how long that amendment or how long the process would take; where they are as far as documentation; and that sort of thing.

As I said earlier, Phase 0 ends with the submittal of the license amendment request. So phase one, a little bit more information on phase one. The acceptance review will be done in accordance with LIC-109.

We hope that the acceptance review process will go smoothly because we've had all the preapplication meetings and summaries.

This is where we will start our in depth licensing and technical reviews. RAI process will start here. The communication and questions will start here.

Phase 1 does overlap into Phase 2, so we will be wrapping up our technical reviews in Phase 2. We will be performing the audits to verify the information we got; verify that the plans and the procedures are in place, and are being implemented in the manner we had believed they were going to be implemented.

And Phase 2 ends the NRC headquarters staff review. We issue an SE, and Phase 3 begins.

Phase 3 is the implementation. The licensee will go out and implement it in their sites, upgrade their procedures, upgrade whatever equipment they need to upgrade. The regions will then take over and perform the inspection of the implementation and the inspection during routine oversight of the site.

There already is an inspection procedure to review these implementations. It will be looked at again once we complete this staff guidance, interim staff guidance, to see if any adjustments or upgrade or revisions are needed.

Bill?

MR. KEMPER: Yes, I was going to say this is a departure from what we have historically done. Historically as part of the licensing process we have also reviewed all of these installation and start up activities as well as their training program; qualification of technicians; that sort of thing.

But we rethought this and realized that that is really not part of - that is not necessary for a license, the platform and the safety system itself; that is more of an operational issue. So that is why we relegated that to the regions, and their traditional inspection.

MEMBER MAYNARD: I have a question on that for the new plants. Even though the ITAACs and stuff, basically construction specs are being done out of Region 2, this seems to be back in the other process where each region would do their own thing, yet we are dealing with the new system.

What is being done to ensure some continuity, consistency between regions on how they review these?

MR. KEMPER: Well, I can just tell you right now, we are dealing with the Oconee application. We have been in direct communication with Region 2 almost every step of the way. We have invited them to participate in the audits that we have done. We share all the products that we produce from the audits and that sort of thing; any written product we give them. We have weekly phone calls with the licensee as a matter of fact, and the branch chief from Region 2 participates in that phone call.

We've also written this IP which Lois has got referenced down here, the inspection procedure, which will embed those requirements that need to be inspected into procedures that they can then go follow through on.

And I would expect that as we get closer to the actual implementation of the system, we will do some 101 interfacing and training of the regional personnel. And we probably even will augment the team with some headquarters folks from my branch.

MS. JAMES: Throughout both Phase 1 and 2 -

MEMBER BROWN: That just got me thinking about that. How do you - I guess you were addressing how you keep each region from establishing their own set of criteria, which will drive everybody nuts again.

(Simultaneous speakers.)

MR. WERMIEL: The whole purpose of the inspection procedure is to avoid that, the inspectors going off on their own. It provides the guidance for the inspectors.

MEMBER BROWN: But you all will provide that?

MR. KEMPER: Yes. The inspection procedure is maintained out of headquarters.

MEMBER BROWN: So that is how you are going to maintain that control?

MS. JAMES: Yes.

MR. KEMPER: To actually generate that

procedure.

MEMBER BROWN: Okay, so you will know the design of the new platform and its integration and all that type of stuff, and you will provide then so that somebody - we don't like the looks of that part of the system. And you say, the answer is, well, I'm sorry, that's been approved, unless there is some fatal flaw they find, that obviously everything is off the table.

MR. WERMIEL: That's the idea.

MEMBER BROWN: I'm sorry, I just needed a little expansion there.

MEMBER SIEBER: Is that IP already written?

MR. WERMIEL: Yes, it is.

MEMBER SIEBER: Can I get a copy of it?

MR. WERMIEL: Sure, absolutely.

MS. JAMES: One of the things I forgot to mention was, during Phase 1 and 2 with the audits, we are going to be documenting the audits and trip reports. And we also intend through those trip reports to again state what we have looked at; whether we are okay with where we are, the information we have. Intending to close some items, to indicate to industry that we have completed our - essentially completed our review of that area, and no more information is required.

We are also going to be expanding our use of the RAI process to do the same thing. Again we are trying to use the current process to give indications to the licensee and industry of where the review is; what we have completed our review of. We are trying to figure out how to reduce the uncertainty in the process.

MEMBER BLEY: Lois?

MS. JAMES: Yes.

MEMBER BLEY: What you just talked about in an earlier summary of those public meetings, are staff actually bound by what you say in those?

MS. JAMES: No, no.

MEMBER BLEY: It's just to get an idea of -

MS. JAMES: Yes, and we are going to have to use the words, as of this moment, based on this information; nothing is final until the SE comes out and is reviewed by OGC.

MR. WERMIEL: What we were told in no uncertain terms by NEI and licensees was that these modifications are costly. There is a lot of money involved, and a lot of time and effort involved in developing these designs and these modifications. And because it's money spent over a period of time, there needs to be a way, as we understand it from them, for them to be assured to some level that expending the next number of millions of dollars or whatever is warranted based on where they stand with the staff; and that they won't end up wasting their money and their time.

So we have developed into this process a way we hope of communicating I'll call it a warm fuzzy or enough of a positive feeling so if a licensee's uncertainty about the regulatory process itself isn't so great that they are not going to continue with the designed development as they intend.

This isn't something that is particularly typical of what the staff does in an amendment review, but we think it is necessary here for that reason.

MS. JAMES: Okay. I've mentioned the review areas before, and we are working very diligently within the task group and with our counterparts to come up with a list of review areas. We had issued a list in our meeting summary or our meeting notice from earlier in the week. We are revising it; we are working on it. Because it's in such a flux right now, we choose just to tell you that we are going to be working on this, and not provide the actual items on this slide.

We are going to learn a lot from - apply a lot of what we learn from Oconee and Wolf Creek to selecting the review areas.

MEMBER BLEY: Just because the industry representative don't have their own session debate, but they are on the working groups, I wonder if anyone from industry would feel like offering a comment on this sort of assurance process?

MR. RILEY: I'll take the bait on that one. I'm Jim Riley. I'm director of engineering at NEI. I think Jerry very accurately portrayed our concerns about the digital I&C licensing process, and our request to establish some level of assurance that the modification is going okay and will proceed through to completion so that we don't have ourselves too far out in front of it from a financial risk standpoint.

There are other things we suggested, and maybe we will continue to work on it. But the concept is absolutely on; I mean that is what we had asked for, and we appreciate the work of the staff to come up with something.

MEMBER MAYNARD: It looks like it doesn't provide a guarantee, but it would at least identify any fatal flaws or something that would be a real show stopper earlier in the -

MR. WERMIEL: That is the absolute intent. If the design that is proposed up front, for example, we learn about it in the preapplication meeting, just doesn't address defense depth and diversity appropriately, I think the licensee would want to know that. Because if they have to go back and redesign the system, or develop a conceptual approach to defense in depth and diversity that is costly, they may decide not to even go forward with the modification. They are going to want to know that, I think, before they start to spend money on a design that the staff would find unacceptable without considerable additional cost to the licensee.

MR. MILLER: Part of what we want to do too during those preapplication meetings is identify the aspects of what they discuss that really we think are critical to our decision so you know where the committee changes an item more or less.

MEMBER STETKAR: Jerry, I just had - you mentioned diversity in depth. I mentioned last year, a work in progress, but it's more in progress in that particular area, at least the couple of revs I've seen.

I just wanted to make sure that I've got it clear in my head again given the discussions this morning. In that particular area there is a list of information to be provided. I recognize it's going to change. But the things - a couple of things that caught my eye was, requirements for a list of all manual operator actions credited for diversity; and detailed justification for operator actions required in less than 30 minutes. The implication there being that you don't need to justify operator actions with time windows longer than 30 minutes.

ISG -

(Simultaneous speakers.)

MEMBER STETKAR: I just wanted to draw your attention to that and make sure that you are interested in some justification for operator actions with time windows longer than 30 minutes in this regime also.

(Simultaneous speakers.)

MR. KEMPER: No, that actually had been flushed out in - at the time, and that is already changed.

CHAIR APOSTOLAKIS: You guys agree.

MS. JAMES: We agree.

Our next - our next slide is our path forward. We are currently meeting with our industry counterparts, the fourth Tuesday of every month for a public meeting, and holding a status call on the second Tuesday of the month.

We are trying to get the one to four topic areas to move forward to get to our next slide, which is our deliverables. Our first major deliverable will be the draft ISG which is scheduled to come out this summer. And then after we resolve the comments, we will issue the final one in the fall.

I think Jack alluded to we are very hopeful that we will have a pilot application for this. We don't know what it's going to be just yet, but we are interested in it, and I believe we know industry is interested in it.

MR. WERMIEL: We are soliciting; actively soliciting.

MS. JAMES: So that is the end of our presentation.

In summary, we introduced the concept of tiers of complexity. We introduced the concept of phases, where we are going to look at different topics at different times.

We are really trying to be responsive to our stakeholders and the concerns that we need to give indications of where we are and how the review is proceeding. And our own technical reviewers, so that we need to review what we need to review to make our decision.

With that, do we have any further questions? Yes?

MEMBER BROWN: Again, under the depth of review area, you talked about diversity in digital -- this is the last paragraph in your section 1.D 1.1, as it presently reads. You talked about diversity in digital I&C as necessitated by a vulnerability to common cause failures (CCFs) in software. You are going to review the system modification to ensure sufficient diversity as provided to accomplish the required safety function.

Are you sending a message that you want different software from division to division? Because that is not the way the systems we've seen so far as set up. The MELTAC platform uses them, but it's all common, and so is the AREVA.

MR. WERMIEL: I would answer just basically, we are sending a message that where you have multiple channels driven by common software, there is a potential for an error in the software to cause those multiple channels to not operate effectively; and for that reason you need some diverse means for coping with that particular problem or that particular potential failure mechanism.

MEMBER BROWN: By that you mean another system?

MR. KEMPER: No, it could be any number of - it could be a diverse system, a DAS system. It could be diverse software. It could be any different attributes on the design of the system. In fact you all are going to here a presentation by Mike Waterman I believe later on today where he is going to talk about that in very much detail.

MEMBER BROWN: Well, part of that diversity in design is an asynchronous operation of these things with not always arriving at the same - and no instrument ever reads the same. So most generally software things that fail is a result of some data bits getting in some place that it doesn't want to swallow properly. Common software failures most of those times you have to assume they all arrive at the same time, and therefore nothing happens even though you -

(Simultaneous speakers.)

MR. KEMPER: If we could find the root cause for software common cause failures, we'd all be very happy. But mostly there is just not one. Every one you point out there is another five that -

MEMBER BROWN: - design means to try to say we will minimize the chance of their design approaches other than different software.

MR. KEMPER: And Mike is going to cover -

MEMBER BROWN: Different software is very expensive from a V&V standpoint to have to put in. So that's why I asked the question whether you were trying to force them into different software or not. And you are not.

MR. KEMPER: No, we're not. We are just saying, here is the issue that you have to be able to cope with in your system design.

MEMBER BROWN: You are not worried about hardware common cause failures.

MR. KEMPER: No, this is the agency policy on common cause failure is rooted in software common cause failures.

MEMBER BROWN: So we are not worried in these new designs whether you got common hardware failures or not.

(Simultaneous speakers.)

MR. WERMIEL: You qualify the digital hardware just like you qualify the analog hardware. It's qualified to survive in its environment, 6.03

specifies there will be sufficient redundancy to be able to deal with failures, et cetera.

MS. JAMES: Okay.

CHAIR APOSTOLAKIS: Any other comments from the members? Questions? Comments?

MEMBER BLEY: All that being said, if there are hardware failures associated with these digital systems, the approach that we have heard for dealing with it will work just as well.

MEMBER BROWN: Yes.

MEMBER BLEY: There is no - you don't need to say software.

MEMBER BROWN: Yes, I got it. And that's why I was just trying to draw them out; that's all. Just to make sure we are on the same page.

CHAIR APOSTOLAKIS: Okay, thank you very much.

We move on to our Regulatory Guide 571 on which we will be writing a letter next week.

So there will be a full presentation to the committee on this particular topic next week, and then in April there will be the other.

MEMBER BROWN: Say that again? I missed everything you said.

CHAIR APOSTOLAKIS: We will write a

letter that is a presentation to the full committee. Next week this topic that we are about to start will be presented to the full committee.

In April the corresponding topics on which we will write a letter will also be presented to the full committee.

(Off record comments.)

DG-5022 "CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES"

CHAIR APOSTOLAKIS: Okay, I see three persons. Who is driving the show?

MR. STURZEBECHER: I am. My name is Karl Sturzebecher. I am from the Office of Research, and the project manager for the Reg Guide 5.71, programs for nuclear facilities.

To my right is Eric Lee from NSIR on my project team. I have my project team with me here. Eric Lee from NSIR; Deborah Hermann from NRO; then I have our technical expert Phil Craig from Pacific Northwest National Labs; and Scott Morris is the deputy director of NSIR who is the sponsor for this particular project.

CHAIR APOSTOLAKIS: Okay.

MR. STURZEBECHER: This presentation will be on the development of the Reg Guide 5.71. And I'm going to go over briefly the introduction, the history and background of the guide; then the reg guide itself, and we will run through the stakeholder comments; and then our path forward.

CHAIR APOSTOLAKIS: Good. Everybody keeps telling me I have to write a letter. I will write a letter.

(Applause.)

CHAIR APOSTOLAKIS: Okay.

MR. STURZEBECHER: The project goal is to write this reg guide based on 10 CFR 73.54, which is the protection of digital computer communication systems and networks.

And based on our understanding of the cyber environment -

CHAIR APOSTOLAKIS: So let me understand here or betray ignorance, 73.54, has that been approved by the Commission?

MR. MORRIS: Yes, it has been approved. The rule is down with the Office of Management and Budget awaiting clearance approval. We expect that any day now, and once we get it back we will put it in the Federal Register.

CHAIR APOSTOLAKIS: I will follow Steve Arndt's earlier comment that I will also not question this, because we have been blessed.

(Off record comments.)

MR. STURZEBECHER: We developed this reg guide in reference to that, and the requirement is that the licensee provide assurance to protect the critical system functions.

And I'll just paragraph quickly through the rule, we are looking to distinguish what we want to protect, what we are protecting it from; provide that analysis; and then move that into a program.

CHAIR APOSTOLAKIS: I have a question here. I had it before too. It says, against cyber attacks up to and including the design basis - cyber attacks. This is kind of a fuzzy concept, isn't it? I mean in the regulatory guide do you specify any attacks?

MR. STURZEBECHER: Well, in the rule there is a breakdown in the type of attack, but the actual definition of what a cyber attack is is what you are referring to?

CHAIR APOSTOLAKIS: No, it refers to the consequences, the impact of the attack. It says, adversely impact the integrity or confidentiality of data or software, deny access to system services data, adverse - so it doesn't really say what the attack is.

MR. MORRIS: Let me help you out Karl.

MS. HERMANN: You do not want to define the attacks, because then the people would turn around and use them. Because the attacks can be any attempt to compromise the confidentiality, integrity or availability of the system. And you don't want to specify the attacks.

CHAIR APOSTOLAKIS: I guess this is a similar question we heard earlier today about common cause failures. I mean we are protecting against something that we really say we don't need to know what it is. We are looking at symptoms of an attack, and we are trying to do something about them; is that what it is?

MS. HERMANN: You postulate what the likely attacks are through the vulnerability assessment, and then you design accordingly to protect against them.

What we are not doing is specifying the specific attacks in the reg guide, because there are thousands of different types of attacks -

CHAIR APOSTOLAKIS: So who si doing this vulnerability assessment? Is it part of the guide here?

MS. HERMANN: The applicants are responsible for doing that.

CHAIR APOSTOLAKIS: Is it part of another regulatory guide, or this regulatory guide?

MS. HERMANN: It's in 47.

MR. STURZEBECHER: Yes, NUREG/CR-6847 provides the details on how you go about -

CHAIR APOSTOLAKIS: It's a NUREG?

MR. STURZEBECHER: That'S a NUREG.

CHAIR APOSTOLAKIS: It doesn't have regulatory authority. It's a NUREG.

MR. STURZEBECHER: It provides guidance to the licensee or applicant on how to distinguish that digital assets they have at their site; and then work out the risk from there. The risk of an attack is 24/7 anyway. But you have to gradate what you have at your site to know which item has the most risk and the most impact of causing a problem at your site.

MEMBER BLEY: And vulnerability assessments are a standard security engineering technique. It is common knowledge on how to do them. There are lots of national and international standards.

MEMBER BONACA: Which has less the number of goals, three I believe. One of them for example was physical availability.

MS. HERMANN: Confidentiality, integrity and availability.

MR. GUARRO: I think there is a little bit of a semantic - because here there is a sub-bullet two, type of attacks. That is not really a type of attack; it's a type of impact.

MR. LEE: Are we talking about full attacks?

CHAIR APOSTOLAKIS: On this slide now, which, number 12?

(Simultaneous speakers.)

MR. LEE: Sub bullet two of bullet A says type of attacks, and he is really describing the type of impacts an attack may have on your assets, which is a different thing.

MR. HECHT: those are the points that are enumerated actually in 73.54. That's how it's stated. It does not state it as a type of attack; it says a licensee - the licensee shall protect systems and networks identified in this section from cyber attacks that would - and then it gives that list.

MR. GUARRO: I'm not questioning 10 CFR. I am just saying that particular language.

MR. HECHT: It says - what I'm saying

is, you are saying that it says, or you are agreeing.

I would like to point out that in the back of the standard it does define cyber attack. I shouldn't say standard - the reg guide. My comment on that is, I was looking at that, if I can just paraphrase, originating from inside or outside, have internal/external components, physical or logical threats, directed or nondirected, conducted against threats having either malicious or nonmalicious intent, and have the potential to result in direct or indirect adverse consequences.

Well, if we say that there is one "or" between each of those, so we can say that there is two; I get 2^6 or 64 different kinds of attacks. I suspect that there are many more than that. And I didn't see in the - in RG-5.71 anywhere where it specifically says, define your threats. Even maybe it's there and I didn't see it.

MR. MORRIS: This is Scott Morris, the deputy director for reactor security at NSIR. The threat - to speak directly to the threat issue, the threat is defined in 10 CFR 73.1, design basis threat; which is publicly available language.

Behind that is what we - is a safeguards document known as the Adversary Characteristics Document, which specifically enumerates the details of each of the threat characteristics presented in the design basis threat; and the cyber attack is one of those.

So there is a whole separate document that talks about cyber attack. And it is not in this document in part because this document is, first of all it's not safeguards, and actually we are trying to move it to the public domain if we can.

So we are specifically not going to talk about threat in this document.

MR. HECHT: But don't you think you should make it clear that a threat assessment just like an AOO, a design basis event, is an important consideration when you do safety.

MR. MORRIS: Absolutely, sure.

MR. HECHT: Because one example that I see here is that the entire document seems to imply that the threat is from the outside. So for example because it talks a lot about integrity and protection, and it speaks about aligning the physical and cyber threats for example.

Well, when you align the physical and cyber security, that does two things . It enables you to reduce overlaps and conflicts. But the other thing is it does maintain that there is a common vulnerability that is introduced as well, or could be if it's not done right.

So for example there is not enough about partitioning that I saw in there, and there wasn't really enough about information security in the DOD sense that I saw. It might be there, and maybe it just has to be made more explicit.

MS. HERMANN: Well, Karl is going to get into that later, where we distinguish between features and attributes and why we did that.

MR. HECHT: One of the things that I might say is that one of the confusions that I had at least is that neither in this, in the rule nor in the book, in the reg guide, is cyber security defined. It's not in the definitions. I was very confused by what cyber security meant, because it could be - does it just refer to the systems and the networks. Does it refer to the systems and the network and the information? Does it refer to information which is descriptive information about the system, or only the information stored on the system.

MR. LEE: Yes, well we'll take that comment. One thing that I would like to respond to that is, the whole purpose of the 73.54 rule is because at nuclear power plants they are worrying about the control systems. The purpose of the 73.54 is to protect the safety, security, emergency preparedness functions of nuclear power plant, not to secure the information itself.

For us availability is more important than confidentiality, or the integrity.

MR. HECHT: Though integrity might be necessary to perform the projected function.

MR. LEE: Yes.

CHAIR APOSTOLAKIS: I think though this is a reasonable question. I mean there should be some definition or description if you will, what do you mean by cyber security. That is your question. It stands to reason.

And maybe the comment you made, too. It would be nice to see it explicitly in there. Is it explicit? I don't remember.

We're still on slide four.

MR. STURZEBECHER: All right, the next slide shows how once you - once the licensee builds this program there are certain focuses that this program works on. It's the training, the risk management and configuration control from a cyber perspective, a cyber security perspective.

And then they build a plan which will be presented to the NRC.

CHAIR APOSTOLAKIS: Before you go to that, I was intrigued by (c)(2), defense in depth strategies that ensure detection, response and recovery. My, my, you are talking about a big thing here. So they will have to demonstrate to you that even if they are attacked, and there is loss of whatever, there is denial of access to system and so on, they can recover from this. That is a lot of work, isn't it?

I mean it seems to me it's buried here as number two under ©) but it is probably a major study itself unless I'm missing something. You are employing the full concept of defense in depth in terms of prevention, mitigation. Has anybody done this anywhere? Is there an example that it can be done?

MS. HERMANN: It's very common. I mean that's how your defense systems work. That is how your intelligence systems work; your financial systems. Defense in depth is a common characteristic of -

CHAIR APOSTOLAKIS: Financial systems

you said?

MS. HERMANN: Yes.

CHAIR APOSTOLAKIS: That is a very unfortunate example.

(Laughter.)

CHAIR APOSTOLAKIS: I don't know, what do you think, Otto? Doesn't that sound like it's a big tall order? It depends on what you mean by recovery.

MEMBER MAYNARD: And I'm not sure that they mean by recovery that the computer systems have to do it. I take this basically you are taking a bigger picture look at the whole plant and recovery, that if you do have an attack that you can identify it, respond to that, and that depending on at what point you catch it you are able to recovery by keeping the plant safe. It's not necessary recovering the computer systems right away or whatever, but I think it's keeping the plant safe as opposed to keeping the computer system.

MS. HERMANN: It's very similar to the fail safe, fail secure concept. Occasionally you have to fail operational, but you are in a known safe secure state.

MR. STURZEBECHER: You can switch over to a second highway for communications. While the other highway is down you try to go through a respond and cover mode.

MR. LEE: The main purpose of that is to maintain the safety security emergency preparedness function at the nuclear power plant.

MR. STURZEBECHER: The overall function must stay - I mean you can get into forensics, and we went through a lot of research on that and came up with many features on that that we are going to talk about.

MEMBER BROWN: Reactor protection, I'm trying to get specific. You have done this at a very high level. And when I look at this I presume it means making sure you don't compromise any of the reactor protection systems and/or safeguard systems and/or communications and/or, and/or, and/or ad infinitum.

And in order to protect against some of these things which you enumerate in this paper requires some fairly complex programming and software in order to be able to identify, respond, firewall, block or whatever it takes.

And I'm not really interested in having that type of software incorporated into a reactor protection system, or SFAS software, from what I've seen so far you normally do that by isolation. If there is no communication path from the outside in, from the external site, or even from other locations outside the main control, where you have to tell it go to do something. Am I correct in that?

MS. HERMANN: We have a slide that actually illustrates that coming up later.

MEMBER BLEY: Do you draw any - it just strikes me that George's question before, it seems to me that it is essential that you need to be able to recover. But it strikes me that there is a very strong parallel with what we have heard about common cause. So anything you could do by a cyber attack one would hope would be included in the range of things that might fit in that common cause, and if you can recover from a common cause failure of the control system, it almost by definition says - I don't see a tie though, from what you folks were doing, and what the folks in the common cause area did. And it seems to me there was a pretty logical one there. I'm just curious about that.

MR. LEE: Here we are talking about the common vulnerabilities. This is the test that Karl is discussing in the later slides. We will go into a little more detail.

Here when we talk about defense in depth strategy, we are talking about to ensure that one type of vulnerability does not postulate all the failure all the way up to the dual systems that are necessary to maintain the safety, security, and emergency preparedness functions.

MEMBER BLEY: I understand that. But it strikes me that the way one could prove that you could survive those vulnerabilities is very close to the way you can prove you can survive the common cause failures within the digital systems. And it sounds as if you really haven't made that connection.

MR. MORRIS: If I could just try something again, Scott Morris, just take one giant step backwards for a minute.

The issue with security is is that it's not people making mistakes or random failures or coding errors; this is real bad people trying to make your life miserable.

MEMBER BLEY: I understand that, but all I'm suggesting is, can they do something beyond what -

MR. MORRIS: I understand. And the other problem with this is, these attacks can be launched from anywhere in the world in a millisecond.

So in the security world what we are really worried about is radiological sabotage. So the licensing standard in the regulations is high assurance; it's not reasonable assurance, it's high assurance of adequate protection against the threats defined in the design basis threat of radiological sabotage.

And that introduces a higher - not a higher calling, but a lot more caution when it comes to how we constructed the regulatory language and the defense in depth and some of the measures that we have included in the regulatory guide.

And I think it's important to just keep that in the back of your mind as you consider some of the things that are in here.

The other challenge we faced in the development of the reg guide is, we had to keep it high level such to allow for rapid you know evolving threats and evolving technologies that mitigate the threat.

So the rule and the reg guide are written at what I would call a very high programmatic level, from that perspective. And I just wanted to put that out there to let that soak in a little bit as we go forward.

And I think that Karl and Deborah and Eric will be able to demonstrate as they move through the reg guide sections to show you how that - they try to achieve that in the regulatory guide.

But this isn't the final answer. There is a lot more technical stuff behind this, just what is in this guidance, in order to - and to the earlier point about just defining cyber security, I think it is an excellent point. Because there is a lot of confusion about what is the difference between information security, cyber security, and how it relates to physical security. It can be quite confusing, particularly for someone who is not a practitioner. So I think it's a good point.

CHAIR APOSTOLAKIS: By the way did you give us a definition of cyber security? Or no you took a note to put it in the guide. What do you think it is? What is the definition that you are using?

MR. STURZEBECHER: The definition of cyber security is to keep a digital asset of your computer doing what it's supposed to be doing so you are sure that it keeps working running that software or whatever function it's doing for you, that you have total assurance that it is not being interrupted or attacked. That is - compromised.

CHAIR APOSTOLAKIS: Make sense, Myron?

MR. HECHT: Well, I would say that you can't have assurance that it is not being attacked. I would say that you have assurance that the protection is in place.

MR. STURZEBECHER: Well, you have to distinguish usability versus security, and how do you integrate security so it's usable, and the idea that that is another aspect of what we faced when we tried to make this reg guide.

So you are trying to provide some kind of security in the background that's always there.

(Simultaneous speakers.)

CHAIR APOSTOLAKIS: (D)(2), evaluate and monitor cyber risks, right?

MR. STURZEBECHER: Right, evaluate and monitor cyber risks, which -

CHAIR APOSTOLAKIS: Is it fair to say that if I do everything else, I have met that requirement? If I do (c) one, two, three and four, (d) one, two three, and (e) one two, I have evaluated and monitored cyber risks; is that what you mean?

Surely you don't mean to produce probabilities?

MR. STURZEBECHER: No.

CHAIR APOSTOLAKIS: No refers to which one?

MS. HERMANN: You evaluate your risks in order to determine what controls to implement as part of your program.

MR. HECHT: Do you mean maybe threats?

CHAIR APOSTOLAKIS: I don't know what that means. I mean if I do everything else, have I evaluated and monitored the risks?

MS. HERMANN: You've managed them.

MR. LEE: Well, if I could, I think one of the slides, this is the test, and Karl is going to explain the guidance on each of these sections that we are discussing in a little bit more detail.

What he meant is that the - as he mentioned earlier about the NUREG-6847, back in 2003, so about five or six years ago - five or six years ago NRC developed a cyber security self-assessment method to provide a licensee a way to assess the cyber vulnerabilities at their site, and also manage cyber risk at their facilities.

And we developed that using the baseline method, developed by PNNL. And we developed in cooperation with licensees and full pilot plants and

NEI.

CHAIR APOSTOLAKIS: You developed this?

MR. LEE: NRC did.

CHAIR APOSTOLAKIS: I'm saying, if I do everything else on the previous slide, I have done this.

MR. LEE: Well, when you are doing that, you would want to - because if you put every security control to protect against everything you will - may not be closely protected. So what you want to do is perform the risk - you identify the vulnerabilities associated with the critical system, in other words those systems that could adversely impact safety, security, emergency preparedness function of your nuclear power plant, you identify that, and you run through a - identify the vulnerabilities, and see what the susceptibilities to cyber attack, and you look at the consequences associated with that. Then you find what the risks are associated with the vulnerabilities -

CHAIR APOSTOLAKIS: What do you mean, risk?

MR. LEE: Security risk.

MS. HERMANN: The risk that a vulnerability will be exploited.

CHAIR APOSTOLAKIS: Again, if I do everything on this slide except (b)(2), have I met (b)(2)?

MEMBER BLEY: Let me try a slightly different approach from what I just heard you say.

You say that (d)(2) is the thing that you might look at as a cost-benefit analysis, is the way you figure out how much of those other things that are listed above that you would do. Is that what you mean by (d)(2)?

MR. LEE: Yes, sir. You try to find the - what the vulnerabilities are, and then you would mitigate against that; yes, sir.

MEMBER MAYNARD: I tend to agree with George. To me, that (b)(2) is really the kind of overall bullet, and these other things are kind of subsets or things you do to manage and evaluate the cyber risks.

CHAIR APOSTOLAKIS: Why do (c) one, two, three, four have done a hell of a lot. I can come before any committee and say, I have monitored cyber risks. Look what I have done. I have done defense in depth. I have mitigated adverse effects. What else do you want me to do?

I'm asking you, if I do all this stuff

except (d)(2), have I met (b)(2)?

MR. STURZEBECHER: You couldn't do (c) one through four, especially (c)(2) because you need to evaluate and manage the risk, and by evaluating we are referring back to the 6847 NUREG, that helps you lay out exactly what the assets are that you are trying to protect.

If you don't have a plan, the overall plan to protect and know what your risks are, then there is no way to apply (c) one through four pretty much.

CHAIR APOSTOLAKIS: You are saying no. The answer is now?

MR. LEE: Let me put it this way, the (c) (2) will help you implement the one, two and those other above controls that you are going to put in, how you are going to put in. It will be a way that will go to areas of defense - various layers of defense, and it depends on your analysis. You may want to put it in the center, like where you need it most protected. Or it depends on your analysis. You might put it in the second layer.

So this would help them through the other security measures that we have specified above.

MR. STURZEBECHER: (d)(2) gives you a

strategy, an awareness of what you have. And then you go forward. You may not, for (c)(2) you may not want to put in certain particular protection items.

CHAIR APOSTOLAKIS: Okay. Okay.

MR. GUARRO: Is it fair to say that (d)(2) gives you the balance between the elements one, two, three, four that you had to put in place in order to meet your intent of protection?

MS. HERMANN: It's a graded approach.

MEMBER BLEY: Let me take you back to how I think George started all this, which was what do you mean by managing the cyber risks? What do you mean by risks?

And I guess, what do you mean by risks? What part of vulnerabilities, consequences, likelihood of problems, likelihood of attack, what part of all those things goes into the evaluation of whether there are risks and how they stack up.

MS. HERMANN: Within security engineering, risk has a slightly different meaning that in safety engineering. And it ties back to the likelihood of a vulnerability being exploited.

All systems' implementations have vulnerabilities, but not all vulnerabilities are easy to exploit, and they require different levels of expertise, different levels of resources, different levels of opportunities.

MEMBER BLEY: That's kind of the probability of, given an attack, how likely is it that you reach some consequence?

MS. HERMANN: Right, because you need to keep in mind you have millions and millions of attacks, but they may not be successful.

An attack is an attempt. A security incident is something, there are consequences which could be anywhere from negligible to catastrophic.

CHAIR APOSTOLAKIS: There is some sort of evaluation of how likely they are, without really quantifying these. I mean it's just a subjective -

MEMBER BLEY: Some kind of at least ranking.

CHAIR APOSTOLAKIS: Yes, ranking.

MEMBER BLEY: And the extent of the consequences is factored in there, as well as the likelihood of succeeding.

MS. HERMANN: But the model is, it's called OMER, it's Opportunity Mode of Expertise and Resources. And you do metrics against that based on your vulnerability assessment, and then you do a before and after assessment.

MR. CRAIG: So I would like to comment because back in 2003, 2002, we completed a very extensive pilot study at four U.S. nuclear power facilities that basically tested the risk methodology and created the graded methodology of how to quantify what risk really is.

And so that program has been effective, and it has been practiced for many years. Recently that program was committed to by all the CNOs in the nuclear power industry through their NSIAC to the Commission. So the program has a lot of run time.

The answer is emphatically yes: it does. If you evaluate and effectively manage cyber risks it takes care of all of the sections (a) through (g). It stands alone in section (d) and specifically (d)(2), because there needed to be a point that the history was brought into the development of a program.

So where the industry via the NEI, tools and their exercises, have committed to the NUREG 6847, as a method to manage this risk environment, we needed to identify it to ensure that one of the three major components of a programmatic approach would include: training your personnel; managing your risk environment; and managing the modification of assets.

The management component of this is the constant introduction of new digital systems into legacy environments and the ability to look at the new systems and the new plants and how they are going to be managed as they come from the vendor through the applicant process and then to an eventual licensee.

So George, the answer is, absolutely yes. It stands alone, but it does represent a more holistic approach to the entire program.

CHAIR APOSTOLAKIS: Okay, let's move on to slide six. Thank you.

MR. CRAIG: Oh, I'm sorry, I'm Phil Craig from Pacific Northwest.

MR. STURZEBECHER: This is the last part of the rule.

CHAIR APOSTOLAKIS: Can we move on?

MR. STURZEBECHER: You look at cyber security back in a timeline.

CHAIR APOSTOLAKIS: Yes, there is a history. Let's move on.

MR. STURZEBECHER: All right. This is the actual development of 5.71. The project was initiated in September of 2007. By June 2008 we were able to release a draft for review. We had stakeholder comments by July, 2008. And this is the process we used, using on the left all the inputs, and the research we did came up with the DG-5022, which was rich and comprehensive with many features.

Then we began to boil down to the basic attributes for the reg guide, and the reason being is in features, there is no way you can dictate those that change - technology changes in time, and we were looking for the high level attributes that those features stepped into, like if you have private sniffers, or detection systems of some sort, that might be an attack mitigation attribute.

So the technology is changing for those features all the time. You don't want to tell the licensee exactly what to do, and set that kind of precedent. And it is also programmatic reg guides, as is the rule. So that is how that evolution - this is based on the quality functional deployment we used.

CHAIR APOSTOLAKIS: I don't see any foreign documents there. Does anybody else worry about these things, or is it just us?

MS. HERMANN: Actually, the NIST 800-53 is a merger of two IEC standards. They basically took IEC 15408 and IEC 17799 and merged it and called it NIST 800-53, so it does capture the international perspective.

CHAIR APOSTOLAKIS: That's a commission of some sort. How about the French or the Germans? What do they do?

MS. HERMANN: They use the IEC 15408.

MR. ARNDT: IEC is an international standards body, similar to the IEEE, but international.

MR. HECHT: But there is a problem in those standards. I think those are really more for IT class systems, aren't they?

MS. HERMANN: No. IEC 15408 has been used for a variety of different equipment. The first things that were actually certified under it were IT, because it was easier to start with something simple. But other systems have used certified as well in the defense community.

MR. HECHT: I'm sorry, I thought in the actual title it did speak about information technology.

MS. HERMANN: Right, but if you look at the information technology, it means any digital equipment. That standard.

MR. HECHT: It's been awhile since I've

read it. And as I recall they are very long. But doesn't that really refer to systems based pretty much on IP technology, in other words, TCP/IP and things like that?

MS. HERMANN: No, I actually published a book on this standard, which goes into quite a bit of detail on the different applications of the standard and the technology it's been applied to. And it's pretty broad.

CHAIR APOSTOLAKIS: She said no.

(Laughter.)

CHAIR APOSTOLAKIS: That's fine.

MR. HECHT: Just one final question.

CHAIR APOSTOLAKIS: Okay.

MR. HECHT: If we are talking about something for example like an Allen-Bradley data highway, that's going to be packet sniffers, I don't think, yes there are packets there, but we are not going to - it's not the same nature of the - of vulnerability. The threat is not the same.

MR. STURZEBECHER: As far as 485, the manufacturer has the layered type of architecture for the communications on that, and anything over 20 knows they have to use a product from Allen-Bradley, because if you start increasing the amount of traffic you may lose something between, if you are sending signals, especially a trip signal between two different - if you go over 20 is what the typical recommended number is, you need to have a program by Allen-Bradley that monitors that highway, and controls it.

As for what kind of security measures they have in it, I'm not sure.

MR. HECHT: Okay, I guess my point was, is that the nature of - you are not going to use a firewall from Cisco on that kind of a system.

MR. CRAIG: No, the technical challenge there is, you are hitting it right on the head. It's not those specific protocols themselves. It's the employment of those protocols, though, when they encapsulate it within the TCP environment. And where you do use common IT security technologies to bridge those protocols, we've got a good way to address it through the 800.53 standard and other IEC standards that are developed.

MR. HECHT: Well, it's getting a little bit deep.

CHAIR APOSTOLAKIS: Now, Carl, we are approaching 2:30. You tell me when to take a break. You feel the burden of responsibility.

(Laughter.)

(Off record comments.)

MR. STURZEBECHER: The next step we go through the guide.

CHAIR APOSTOLAKIS: So maybe it's now. Okay, thank you very much. We will be back at 2:45.

(Whereupon at 2:26 p.m. the proceeding in the above-entitled matter went off the record and resumed at 2:45 p.m.)

CHAIR APOSTOLAKIS: Okay. We are back in session.

MR. STURZEBECHER: Okay. I'm going to move into the actual guide now, and it has the introduction, and the first part of the regulatory position in two talks about the plans requirements that the licensee has to list when they provide to the NRC. And it follows the rule, 73.54.

The Cyber Security program in the guide, it suggests a graded approach, risk-informed, and also requires a life cycle look at digital assets.

CHAIR APOSTOLAKIS: Did you say risk-informed? Yes. What does that mean?

MS. HERMANN: Getting back to the graded approach, security risk.

CHAIR APOSTOLAKIS: But you are not using the terms the way the rest of the Agency is using it, but that's fine. Please, Karl.

MR. MORRIS: Karl is laughing, because I warned him not to laugh.

(Laughter.)

CHAIR APOSTOLAKIS: Well, look, I mean, you put this, "using the final safety analysis report a site-specific probabilistic risk assessment." How can they use the site-specific probabilistic risk assessment to analyze digital computers, when the PRAs themselves don't do that? Is it in terms of consequences, in terms of systems? The PRA may not have the digital systems, but it has the physical system, so is that really what you mean there, that they're looking at the consequences of losing control or whatever it is?

MEMBER STETKAR: How much have you really thought, since it's in your Reg Guide, and it's in the NUREG, it's not clear how much the people who wrote the NUREG thought about it. How much have you really thought about the difference between failure to do something that a system was supposed to do, like I have a LOCA. I don't start injection; compared to doing things that the system was never designed to do, but could get you in a lot of trouble if it does it? My analogy is the steering controls the side that they want to drive the bus off the bridge, not that they failed to keep driving the bus in a straight line, but they actively want to drive the bus off the bridge. They know the bridge is there, and they want to drive the bus off the bridge.

I will tell you that no PRAs or internal events at full power look at those things. Fire PRAs start to look at those things in terms of spurious signals. The things that we're talking about in terms of common cause evaluations for software start to talk about those things. Active faults that make systems do things that they were never intended to do, and human reliability is called errors of commission. I don't see anything in the guidance that tells people they should worry about that, because if I was one of these really bad people out there, what people tend to think about, I'd be thinking about doing those things.

MEMBER BLEY: Or not out there, in there.

MEMBER STETKAR: Out there, or in there. Well, certainly, if I was in there I'd be thinking about that, because I know it's easy to provide defenses against the other things. So I was curious how much you've thought about that when you talk about using a risk-informed approach to develop hierarchies for critical digital assets, and the effects if those digital assets were compromised. Because you might come up with a different ranking if you think about the problem differently.

MS. HERMANN: Well, I think what you're suggesting is during the vulnerability assessment do the equivalent of a HAZ OP study. And I agree, what you're looking for is the ability to enter an unknown or an undefined state, and the vulnerability assessment would look for those conditions and factor it into the controls.

MEMBER STETKAR: That's right. But those types of HAZ OP studies in terms of the -- create conditions that are -- instead of fail to perform a required action, perform spurious, undesired actions, are typically not evaluated in current risk assessment, so you couldn't gain much in the current risk assessments. The NUREG doesn't seem to speak about that. It talks about ranking things in terms of its importance for, basically, failure to perform required actions.

MS. HERMANN: That's, I guess, the subtle difference between safety and security, the safety you're looking at failure, errors, latent defects, et cetera that are accidental; whereas, in the security vulnerability analysis we're zeroing in on those, as well as attempts to force a deliberate. So if I go in and I find I can do these horrible things, I'm going to explode that vulnerability.

MEMBER STETKAR: That's exactly what I was asking for. I didn't see very much emphasis in the Reg Guide or the NUREG for addressing those types of vulnerabilities, if you want to call them that; that it tends to focus on the traditional analyses for failure to do something that it was supposed to do, rather than doing alternate type things.

MS. HERMANN: We can beef that up.

MEMBER STETKAR: Okay. I'm not proposing how to do it, it's just a sensitivity that since it does make reference to existing plant-specific PRAs, which look in great detail at failure to do something it was supposed to do, but don't yet do the other part of the problem. And it makes a lot of reference to Appendix C in the NUREG, which has some words in it that almost sound right, but the examples are all of the fails to do something it was supposed to do.

MS. HERMANN: We'll be glad to do that.

MEMBER STETKAR: If you're thinking

specifically from the security attack mode, you might want to think a little bit more about others.

MR. HECHT: I don't think a PRA has a probability of all four feedwater pumps going out on PWR.

MEMBER STETKAR: Yes, it does.

MR. HECHT: Oh, it does?

MEMBER STETKAR: Oh, it absolutely does. What it doesn't have is - and I don't want to get real specific about these - it doesn't have something that would make the feedwater system do something opposite to that at the same time other things are telling the operator something else is going on. The PRA has that kind of stuff in it.

You see it a lot these days, and there's little experience, unfortunately, when people start to talk about fire risk assessments, where fires in cabling or control systems can cause bizarre combinations of spurious signals; stuff starting when you don't want it to start, normal stuff that's closed, that you expect to remain closed, opening up suddenly for no reason, because fire doesn't know. And there can be strange combinations of those things that happen that are not really well thought about in terms of both the response of the machine, or the response of the human beings in there.

CHAIR APOSTOLAKIS: Okay?

MEMBER STETKAR: Thank you.

CHAIR APOSTOLAKIS: For the time being.

MR. STURZEBECHER: Okay. So now analyze a digital computer system or network, there's two options, and we've listed them here for using either 10 CFR 50.65 or again, the NUREG TR-68.47.

MR. HECHT: Can I just make a comment on Section 3.1. You've stated that you want to identify CDAs, and CDAs are defined as basically - let's see if I can find the definition here - "a digital device", "digital" is the important word - "a digital device or system that plays a role in the operation or maintenance of a critical system and can impact the proper function of that system."

What do you think, or where would it be covered if, for example, you need to have an HVAC system to keep something cool so that it will work, or that you have something to prevent an explosion, those support type things?

MR. CRAIG: In the rule, it specifically states, "including off-site communications and support systems and equipment", and those are those.

MR. HECHT: That's the rule, but is the

Reg Guide consistent with the rule in that respect?

MS. HERMANN: Yes, the environmental protections, operational environmental protections.

MR. HECHT: Which section is that?

MEMBER BROWN: Page 12, 3.4.2.3. I think we're talking about physical and operational environmental protections?

MR. HECHT: Yes.

MEMBER BROWN: Yes.

MR. HECHT: Thank you.

CHAIR APOSTOLAKIS: All right. He's there.

MR. HECHT: Kind of.

CHAIR APOSTOLAKIS: Okay.

MR. STURZEBECHER: The licensee is to establish, and implement, and maintain the Cyber Security program as listed here. They're also required to incorporate the Cyber Security program into the Physical Protection program, and the Reg Guide gives them the ability to use key personnel in that situation.

CHAIR APOSTOLAKIS: Well, see, this is now where I, again, I get a little bit confused. Essentially, you are repeating what the rule says. And you say the security organization is responsible, dah, dah, dah. You have to do this, you have to do that, but isn't the purpose of a guide actually telling them how to do it? There isn't much information in this guide as to how to actually do things. Now, is that deliberate, is it the nature of the beast we're dealing with here, that you really can't go into detail?

I mean, if I look at other guides, like the 1.174, it tells me you have to worry about these five principles, this is what we mean by defense-in-depth philosophy. They have a series of bullets. They give you numerical guidelines, how to compare Delta CDF. And here it just -- it's one after the other, identify and document the CDAs, using the final safety analysis reports do this and that. Why is the level so high in this guide without getting into here's how to do it?

MEMBER BLEY: Or is that covered somewhere else?

CHAIR APOSTOLAKIS: Or is it somewhere else? Absolutely. Yes. I mean, if it is -- yes, Deborah.

MS. HERMANN: The intent was to write a performance-based Reg Guide, because the technology changes so quickly, because the threat environment changes so quickly. It takes a long time to get a regulatory guide all the way through the process and out, and if we put in very prescriptive detailed do it this way, it would be obsolete before we got it published. So we went with a performance-based -

CHAIR APOSTOLAKIS: But performance -- that was another question I had, because I've seen those words here and there. And, again, performance-based guide means -- okay, let's say here. It says, "Security organization is responsible for protecting the facility from physical and cyber attacks." So the licensee comes back and says I have a security organization that is responsible for protecting the facility. All right. So you met this.

Then you're supposed to look at the site-specific PRA. I look at the site-specific PRA. Do they have to tell you what they did, and do your reviewers have guidance as to what they did makes sense, is it reasonable? I mean, yes, performance -- I appreciate performance-based guidance, but it has to be a little bit more -

MEMBER BROWN: They're all like that.

CHAIR APOSTOLAKIS: I know.

MEMBER BROWN: Immediate protection. It says, "An acceptable method to develop a media protection program includes the following attributes; develop a media protection policy that defines the purpose, scope, roles, and response" -

CHAIR APOSTOLAKIS: Right. That's why I -

MEMBER BROWN: "Develop procedures to facilitate and maintain it." It doesn't give specifics on what are acceptable methods for protection, locking them in a box, putting magnets beside them if you don't want -- whatever. Nothing in here for that.

MR. MORRIS: This is Scott Morris again. Let me try to take this one on. It's a good question.

Actually, the first iteration of the Reg Guide had all that in there, and we intentionally removed it, explicitly because of what Deborah said. However, what hasn't been said so far today is there is going to be between the issuance of the regulatory guide and the time when we're actually out there looking at these things, and inspecting it, there's a licensing effort that has to happen. And the rule requires that every reactor licensee and every COL applicant submit to us for review and approval a comprehensive Cyber Security Plan for their site.

And we are currently working with NEI and industry representatives to develop a generic Cyber Security Plan template that will, in fact, have some of these details that you're talking about in it. Bu tit's up to the licensee to tell us how they're going to meet each of these -- what are their policies, what are the specifics of their site-specific program? And they have to demonstrate that they've addressed each of these issues that we talk about in a performance-based way. So we're working to do -- there's a whole separate exercise that we're just now getting involved with the industry -

CHAIR APOSTOLAKIS: Isn't that the purpose of a regulatory guide? Why is that a separate exercise?

MEMBER BLEY: Usually, it gives the licensee an idea of if I do this in the following way, I meet your requirements. And this kind of just gives a catalogue of what needs to be there, and then they've got to review everything.

CHAIR APOSTOLAKIS: It's almost a copy of the rule.

MEMBER BLEY: Only lot's more detail.

MR. MORRIS: We could have done that, but as Deborah said, with the environment that we're in, by the time we issued it, it might -- the things that we say, one effective way to do that is lock it in a box and use magnets and all. And then somebody develops a different widget that that no longer applies to in the next six months.

CHAIR APOSTOLAKIS: But you could give examples, Scott, without saying -

MEMBER BLEY: And equivalents.

CHAIR APOSTOLAKIS: Yes. And if you say, for example, and you give five or six bullets, then you're sending a message that this is really the kind of thing we're talking about. You don't necessarily have to implement bullet number three, but if you leave it at that level, I mean, I was struck by it. I kept reading it, and I said I'm not learning anything here. All of it is in the rule.

MEMBER BLEY: Again, I'd be interested in hearing from the industry on this, if this is one they're happy with, they can live with well.

MS. HERMANN: They wanted the examples deleted.

CHAIR APOSTOLAKIS: Well, the industry, in general, is happy with -

MEMBER BLEY: Usually, they like to know if I do this, I can get through.

MR. STURZEBECHER: The first version that Scott is talking about was 120 pages, and literally when we went through the review, they wanted -- almost 50 percent of the comments were delete, move. They did not like the prescriptive nature -

CHAIR APOSTOLAKIS: Well, I don't know how it was presented, and why they said delete. But, I mean, the issue here is the regulatory guide is supposed to give some guidance, rather than say show me this without giving them any idea of how they will show it. How are your reviewers going to do it? Is the SRP - there will be an SRP? Is the SRP going to be more detailed?

MR. STURZEBECHER: Yes.

MS. HERMANN: Both in Chapter 7, and in Chapter 13.

CHAIR APOSTOLAKIS: Are we going to review the SRP?

MS. HERMANN: I would assume so.

CHAIR APOSTOLAKIS: Yes. I don't know.

MR. MORRIS: The other thing that Staff hasn't said is that there's a series of technical documents that are being built, more than likely NUREGs that will address exactly what you're referring to, this detail. I don't know if you want to comment on that, but just we were planning on a series of NUREGs that talk about the specifics.

MR. LEE: For each of these sections, because we took those detailed examples out, we plan to develop -- are in the process of putting a process so that we would develop a NUREG or a study to develop a detailed technical basis on each of these subject areas, and also provide some guidance or examples of how one might -- issues that needs to be addressed in order to achieve that high assurance.

MR. MORRIS: In effect, it's already been written. It's just a matter, we have to repackage it with an NRC header on it.

CHAIR APOSTOLAKIS: Why can't you make it part of the guide?

MR. MORRIS: Well, originally we did, and we got major push-back.

MEMBER BLEY: But it will be easier to change a NUREG later than it would be to -

MR. MORRIS: I mean, Dave Rahn in the back can tell you the angst that we went through for months on -

CHAIR APOSTOLAKIS: That's the second time somebody is using "angst". I know. Are you done, Scott? Mr. Riley.

MR. RILEY: Jim Riley at NEI. I'm going out on a limb a little bit here, because cyber security doesn't happen to be the issue that I'm responsible for. But I do understand that industry is in support of this approach that's being used.

I'd like to point out that it's my experience that there's always a gray area here on being over-prescriptive on the regulatory guides where it defines an approach that becomes kind of the de facto, accepted way to do things without some level of defense to do otherwise, and that discourages innovation, it discourages change. And I think the approach that's being described here, we believe, is taking a road that does a good job of providing the guidance in a way that's easier to change, and that allows more of an interaction to get to really where we all want to go. And I guess the Reg Guide, in our mind, is something that ought to define the goals and allow more latitude on the means to get there. And that's the performance-based approach that you were talking about, so what I understand is, in general, we are in agreement with the Staff on how this is being done.

CHAIR APOSTOLAKIS: The last thing this guide can be accused of is that it's overly prescriptive. There's a whole spectrum, Jim, and you know that.

MR. RILEY: Oh, there is.

CHAIR APOSTOLAKIS: So yes, it seems to me that without the guide and just the rule, you would achieve the same thing. The rule says the same thing.

MEMBER MAYNARD: It seems a little unusual to me that we're going to put more detail in the Standard Review Plan than we do in the Reg Guide. I don't have a major problem with -- there are pros and cons to having more specificity in the Reg Guide. Actually, I've always found it works to the regulator's advantage for it to be less specific than the other way. Because when you get very specific, if they want to do something different that calls out of that, it's difficult. It seems a little unusual to me that it doesn't have that much specificity in it.

I do understand that in the security area, there can be changes occurring and stuff, and it may be difficult to have a level of specificity that you'd like.

MEMBER SIEBER: Well, I can see why you would write a general rule like this, because the nature of cyber attacks changes every day. The problem that I see is, how does the Staff evaluate a given applicant's program precisely due to the fact that the threats change almost daily? My security system for my laptop gets updated every day, and there's new threats, new modes out there. So whatever you write in your security plan is going to be general, like the rule is, like the regulatory guide is, and the only way you're going to be able to judge whether it meets some standard, and I haven't figured out what that standard really is, is to go and look at the program as it exists at a given point in time. And the most you can say is this program is adequate for today.

MS. HERMANN: I think as maybe a point of comparison, there are four or five federal rules out in the area of cyber security. Our Reg Guide is very consistent with HIPAA Act, has almost the same structure, management controls, technical controls, operational controls, the level of detail and specificity is almost identical. And that program is working very well.

CHAIR APOSTOLAKIS: Still, that's outside our purview.

MS. HERMANN: Yes, just a point of

comparison.

CHAIR APOSTOLAKIS: But giving a few examples, it seems to me, would not tie you down, and would actually give -- would outline what we expect to see. You don't have to say do this. I appreciate that, but right now it seems to me the rule is good enough. I started reading the guide, and after a while I say well, gee, I've read this before. It works as the same thing, essentially.

MEMBER SIEBER: It's hard to argue with the generalities.

CHAIR APOSTOLAKIS: It is very hard, indeed.

MEMBER SIEBER: And I'm glad you're writing the letter instead of me.

(Laughter.)

MEMBER SIEBER: Because I wouldn't know what to do.

CHAIR APOSTOLAKIS: The recommendation to the Staff will be produce an acceptable guide. And I will not tell them what acceptable is.

(Laughter.)

(Off the record comments.)

MEMBER MAYNARD: Well, I think that in some areas perhaps a couple of examples could be an appropriate way to handle that, without saying that this is the criteria. This is what you've got to do.

CHAIR APOSTOLAKIS: That's right. That's exactly what I mean.

MEMBER MAYNARD: The level of effort that you're looking at.

CHAIR APOSTOLAKIS: Yes, I mean especially in light of the comments on probabilistic risk assessment, and the Staff has comments, and so on. Give me some idea what you expect. What are you going to do? I mean, if they just tell you oh, yes, I picked up the PRA and I looked at it. Well, that's performance-based. They actually performed. I have to know a little more.

MEMBER SIEBER: The other thing I don't understand is why you would use the PRA as a part of this. If I were a cyber saboteur, I would look at the PRA and know what to attack, perhaps, but to evaluate your security plan, the only thing you can do is mimic what the saboteur would do.

CHAIR APOSTOLAKIS: No, because they want to also do defense-in-depth in mitigation, and the PRA might help them there.

MEMBER SIEBER: You may have to attack at different levels.

CHAIR APOSTOLAKIS: No, that's for the attack. But, also, they have to demonstrate that they can mitigate attacks. The PRA may suggest ways of doing that. Right?

MEMBER SIEBER: Okay.

CHAIR APOSTOLAKIS: Where you now?

MEMBER MAYNARD: You use a PRA in a different manner for this. Typically, for a PRA, you're looking at the probability of something happening. I think for this you're looking at it for where are you vulnerability -- where are your single point events.

MEMBER STETKAR: That's the whole point, is the vulnerability assessment and the scenario assessment.

MEMBER SIEBER: Yes, because probabilities go out the window with intentional acts.

MEMBER STETKAR: That's right.

MEMBER SIEBER: It's the risk that lies beyond the intentional act.

CHAIR APOSTOLAKIS: They will look at the PRA without the -

MEMBER SIEBER: Yes.

CHAIR APOSTOLAKIS: Slide 15, where are

we at?

MR. STURZEBECHER: Move to fourteen.

CHAIR APOSTOLAKIS: Fourteen, you want to be on fourteen?

MR. STURZEBECHER: Yes. Cyber security controls, and use the same common framework that NIST approved. And it's management control, operation controls, and technical controls, segmentation there between the three levels when you're dealing with cyber security. We've got defense-in-depth.

MR. HECHT: Excuse me. In 3.4, you speak about system hardening. That was just another term I didn't quite understand.

MR. STURZEBECHER: It wasn't defined?

MR. HECHT: Yes.

MS. HERMANN: It's just under hardening in the glossary.

MR. HECHT: Yes, it says 3.4.2.1., System Hardening program.

MEMBER BROWN: Well, hardened is in the glossary. Not system hardening.

MR. HECHT: Yes. That definition of hardening I think had to deal an awful lot with protection.

MEMBER BROWN: Well, it says system

hardening, also, in there. Second sentence.

MR. HECHT: I guess I was confused. There seems to be an awful lot of overlap between access control, what was called protection, and what was called hardening.

MS. HERMANN: There is. Hardening is a more general category. Access control is one aspect of system hardening.

MR. HECHT: But the access control had its own category, didn't it, like in 3.4.1.3, as I recall? And you also had system protection, I think as a separate -- ahh, under "System and Information Integrity", that's where you have it. So I guess you have 3.4.2.1, you have 3.4.1.3, and you have 3.4.2.5.

MS. HERMANN: Again, because there's different aspects of hardening and access of control in those, whether you're just talking about technical controls, management control, or the operational control.

MR. HECHT: But those were all -

MS. HERMANN: There's different aspects of the given technique, depending on whether it's a management, operational, or technical. It's just way the security engineering is organized.

MR. HECHT: Okay. Well, I might suggest

that maybe some explanatory sentences distinguishing between the three of them might be helpful, so that it doesn't look like it's going to be -

MS. HERMANN: That's easy.

MR. STURZEBECHER: These are defense-in-depth protective strategies. There's an example here. We show a topology with the concentric rings. If I use an analogy to physical security, your level four would be the vital area, the most important area. Then you move down to level three, which is the protected area, the owner's area would be level two, and finally the outside, level one.

MR. HECHT: Now, I just wanted to point out there that in the text you speak about level three as being a area where you have data acquisition, and level four being an area that you have control. And it seemed to me that in that particular structure, you couldn't get the sensor data to the control system, so maybe that's not a good example. 3.5, yes.

MR. STURZEBECHER: Well, typically if you were to put a fax or something that's being data reflection, it takes the control system and goes out from there. You don't always feed back in.

MR. HECHT: But that would be like the

level three system being both control and data acquisition?

MR. STURZEBECHER: Just data acquisition. If I was to build a model, and that's exactly what they do in the fossil sites, they do that type of work, where the DCS sits in the middle, level four. You go out to the VACs or a data historian, and then the historian makes that connection at level two, because this is where you reach that mind set change between control thinking, where you're trying to limit the amount of traffic on a highway all the time because it's safety, you can't have main fuel trip, similar to what's going on with safety in a nuclear situation, being interrupted. It has to have a clean highway when you're running. If you go outside level two, that's where you get into the IT world, the business world, where the drive is to make connectivity, number one. It's very high pressed, and the IT folks don't have that perspective that that control piece of equipment is running, or that controller is running a piece of equipment. They don't think in those terms. Different mind sets.

MR. HECHT: Fair enough. So I have level - you're talking about level two now, which is basically the interface between the management and the people who do the work.

MR. STURZEBECHER: Right. That's where you go from three to two.

MR. HECHT: Okay. But, now, my question was from three to four, where basically flow is prohibited. And my reading of that part of the standard basically said that, for example, level three would be where you acquire data, and level four is where you do the control. And a strict reading of that would be that I could not take my sensor data to give it to my control system to make a decision.

MR. STURZEBECHER: The data in level four is available all throughout the DCS. Why would it -- it would pass it through at a lower level data point. It would not go out and then come back in.

MEMBER BROWN: I think the sensors are within level four. I understand what he's saying if you read the words.

MR. STURZEBECHER: Oh, the words. Okay.

MEMBER BROWN: Yes. I mean, you've implied that all data acquisition functions are allocated to level three, critical systems providing data acquisition functions. Well, those are sensors, plant sensors, detectors, all that other type stuff that's related to protection signals, that the protection functions have to process. Just an implication. I don't think that's what you meant.

MR. STURZEBECHER: Right.

MEMBER BROWN: You're looking more of the level four, you've got all your plant sensors, you've got your plant protection systems, you've got your SFAS, you've got your other critical controls. They're all self-encompassing. They can pass data out, and they can take their own control functions. That's the data that gets fed to the data acquisition system, and that's the type of data you're talking about. You don't want anything back.

MR. STURZEBECHER: Yes.

MEMBER BROWN: I think that's what they mean. That's not -

MR. HECHT: That's not what it says.

MEMBER BROWN: That's not exactly what it says. You've got a few fuzzy words relative to critical.

MS. HERMANN: Yes. I think the difference is the security boundaries are logical and not physical, and there's not a window between physical security boundaries and logical security boundaries.

MR. HECHT: You've got -

MEMBER BROWN: You just got me.

MR. HECHT: You've got to have -- the plant protection system has got to have sensor data.

MR. STURZEBECHER: Yes.

MR. HECHT: Level four has got to have sensor data. And I guess what you need to say is that level four can also include sensor data, not just level three.

MS. HERMANN: See, this is an example why we're not prescriptive in the Reg Guide.

MR. GUARRO: Yes. Well, this is an example why examples may be needed so that you tie this high level of conceptual model that you have to something that people that are dealing with hardware and computers can relate to. Because, otherwise, these type of misinterpretations, if misinterpretations are, would arise.

MR. HECHT: Of course, you can say that this is the one time we tried to provide an example, and look what happened.

MS. HERMANN: Right.

(Laughter.)

MR. GUARRO: Because it is true that if you -- you cannot be overly specific because the technology changes, the threats change, et cetera, et cetera. But if you limit yourself to classes that serve as examples of what you're talking about, then I think things don't change as fast, and so you can provide some model into which your prescriptions or guidance can be put in more concrete terms. I think that -

MEMBER BROWN: In the level four area you could have more specific examples. In the level two to three, two to one area, that's where most of your uncertainty comes, and one to zero. But in the level four, there's no communication from the outside world into those two areas; therefore, you can do it with barriers, except for one. There's a lot of examples that you can use, because they're not going to be changed. They're fixed based on the design of the equipment you've got there. From the level two, one, and zero, you're right on the money in terms of the ability to attack those, hackers, whoever want to.

CHAIR APOSTOLAKIS: And there could be a nice story describing these things. This is why we're giving you examples here, here is where you have more flexibility. That's the whole point.

Okay. Are we done with fifteen?

MR. STURZEBECHER: Yes.

CHAIR APOSTOLAKIS: Attack mitigation.

MR. STURZEBECHER: Attack mitigation.

CHAIR APOSTOLAKIS: This is a fun field, isn't it?

MR. STURZEBECHER: The licensee must -

(Off the record comments.)

CHAIR APOSTOLAKIS: I'm sorry. Go ahead.

MR. STURZEBECHER: The licensee must detect the cyber attack or prevent that cyber attack, and then deny its ability to succeed further, or respond. And you've got to respond by just restoring the affected system.

CHAIR APOSTOLAKIS: Same comments as before.

MR. HECHT: No. I would make a comment, and that is that sometimes forensic techniques are basically -- is what you do when you have an incident response in an IT system, is they tell you don't touch anything. Disconnect it from the network, and call the experts. And that's probably not appropriate for a plant I&C system.

MR. STURZEBECHER: Certain systems do particular things, the Westinghouse or the Ovation. When the highway goes down, it provides data for the computer specialist at that point to go ahead and review and see what's going on. As a forensic, they want to know why it went down before they put it back up. There are a lot of systems that don't always do that. Sometimes they auto boot, which is not a good thing, because you're not trying to do any kind of forensic at all. So it really depends what the vendor is, and who the licensee selects from there. I'm just saying for an example, from my experience.

MR. HECHT: I guess you say incident response, so I guess we aren't telling them that. It's just that that was the thing that flashed into my mind.

MEMBER MAYNARD: Is this limited to just cyber attacks of the intentional nature, where somebody is intentionally trying to break into the system and do something, or does it involve any cyber attack that may be incident nature? Being just total scope. I mean, there's things that you could classify as a cyber attack, but you may just totally burden yourself down with a lot of things. And, to me, the ones that are -- any of them are important to the extent that they may cause damage, but the ones I would think you're really trying to get to are those that are intentional here.

MR. STURZEBECHER: Yes. The obvious is the outside. Right?

MEMBER MAYNARD: To me, just the scope of how many of these and to what level are you going to get down to? You could tie up a whole bunch of people evaluating things forever that may or may not do -

MR. MORRIS: The problem is until you do the forensics, you don't know if it was a directed or non-directed attack in many cases, not all.

MEMBER MAYNARD: And it also depends - I've go back and re-read your definition of attack there. I think things are attacking my computer all the time when I -- I mean, there's just all kinds of things could be classified as an attack. Getting nervous on this one, just what is the scope of effort in this that's going to be required.

MEMBER BROWN: One of the -- just to springboard from that. When I look at your level concept, the concentric rings, there are some areas that, to me, would require far less effort, because you can develop protection, like the level four stuff. You don't allow outside access, so from external attack, you're clean. Now, if somebody wants to destroy something, or go after internally, there you can even be prescriptive. Those are systems that are designed. You have to have access to the software. You have to be able to go through a password, so those are people that have to sit down and concentrate, and pull up all the different things to get in in order to change the software, to say put a bug in, to tell the software not to shut down when the set point is tripped. That's very difficult to do, very, very difficult to do. Even for an operator to go try to do that, he has to have a very detailed knowledge of the code in order to know where in the lines of code to go do that, because you've got to be able to program the appropriate level. You're going to have to have your tools, hook up a laptop, do a bunch of things. You're not going to be able to do that with these systems. If we design systems like that, we're toast. You shouldn't be doing that.

So, to me, you can be -- and to go after Otto's thought process, there was a couple of levels in here where you don't want to have to expend tons of manpower. You want to concentrate on the areas where you really are going to take a hit, and that's in the level two, one, and zero levels, and at the four and three. And there's no differentiation in here relative to the ability to accept a proposal from a licensee that well, gee, we really think we don't need to do any more than this. The firewall, where it's a one-way transmission of data, that's good enough. And we're going to put a lock on the box that only the shift supervisor has in order to get into the computer, the main computer, main frame, the different boxes to change software. Okay? Normally, it's pretty hard to go change software without doing a lot of different things. It's very difficult.

MR. HECHT: That's why you have to have a threat assessment, because you say it's hard for some people.

MEMBER BROWN: Well, I don't know about these commercial programs. I can only refer to the military platforms that I'm familiar with.

MR. HECHT: But even so, somebody ultimately takes some device, connects it to do a software upgrade, or to do any change, somebody takes a device, connects it to a port on the operational system, hopefully when it's not operating, and presses a button and uploads something.

MEMBER BROWN: I think you would find that's not -- typically, it's not absolutely that simple to do that.

MR. HECHT: Well, you've got to be able to change the software. Right?

MEMBER BROWN: Yes, but that's being done just not one guy walking up there and doing it. You're going to have supervisors involved, you're going to have verification of software.

MR. HECHT: All right.

MEMBER BROWN: I still think there's a level. All I'm trying to do is trying to see how can you get some common sense into this thing to allow so that NRC is not insisting on kind of a one-size fits all up and down. If I'm going down the wrong tree, I'm just sensitive to Otto's comment, and based on past experience what we went through. I mean, the only way to change software in my systems back in the Navy, you had to take a prom out and put in a brand new one, and it had everything coded into it. And those were all verified. There was a little package. That was it. New systems allow laptops to do that. But still, you had to go through a certain process that made it difficult to do something bad.

MR. HECHT: The point is that that would be part of it, if you have a cyber security plan that says that an insider is part of your threat, then you have the administrative controls that go along with that, and the management controls.

MEMBER BROWN: And some other hardware

controls. That's why I say, I think it's easier to do when you're inside. It would be more than administrative.

MR. HECHT: I'm mouse-milking this right now. George, you can tell me to shut up, and we can move on, as long as Otto is satisfied with my additional comments.

CHAIR APOSTOLAKIS: I will never tell you to shut up.

MR. HECHT: Well, you could ask me to restrain my -

(Laughter.)

(Off the record comments.)

MEMBER SIEBER: I'll do it.

CHAIR APOSTOLAKIS: Okay.

MR. STURZEBECHER: The licensee is to develop policy and procedures to insure the continuity in functions are protected from cyber attacks. The cyber security training and awareness, you need to have the individual up-to-date training to handle any particular cyber security job function. 3.9, Cyber security assessment with risk management. This is where the licensee again needs to apply the NUREG CR68.47, which is currently employed by the industry now. Additions or modifications to digital assets, we're asking that to comply they need to update, and periodically review their configuration management program.

Policies and implementing procedures, the licensee needs to maintain policies as they relate to the rule. Cyber security program review, and that's every 24 months we're asking for that review. Records retention, that's the -- enable the inspectors and auditors to be able to evaluate incidences and events and that ends discussion in the Reg Guide.

I guess back to the transition here to our stakeholder comments, and I was pointing out from July of 2008 to this recent month, February, we've been working to achieve consensus with industry on refining the document. We used a stakeholder analysis document for evaluating -

MEMBER BROWN: Can I ask you one question?

MR. STURZEBECHER: Go ahead.

MEMBER BROWN: 3.10, addition and modification of digital assets. This is largely an internal -- how you manage configuration of the software and all the other stuff, application software, et cetera. And if you leave this as loose as this is, you've got how many different plants that you have to -- you could end up with 30 or 40 different methodologies of configuration management, which would be -- my point being, this is an area along the examples, there are some fairly - methodologies for configuration management. They could be utilized by all licensees in a hierarchy that will allow a consistent approach, make it easier and less resources on NRC's part. And it has nothing to do with rapidly changing technology or anything else. This is strictly administration, keeping track of software versions, where it resides, what boxes you put it in, how many people it takes to open up the box, whatever the case may be. Those are procedures.

MS. HERMANN: I think we agree with you, there are standard methodologies. There's all sorts of automated tools you can use to simplify the configuration management process. We don't have legal authority to tell them what tool to buy, or what method to implement, because that gets into their standard business practices.

MEMBER BROWN: That's a fuzzy answer.

MR. STURZEBECHER: Well, they are using IMPO-914. They are using that now throughout the industry to standardize the configuration management.

MEMBER BROWN: So somebody is telling them here's an acceptable method.

MS. HERMANN: Right. I mean -

MEMBER BROWN: Let me springboard on that, because we tell them how to do all kinds of other things. You will implement stuff per IEEE-603, 1991 or you will use this Reg Guide, and use this. You'll this standard for something, you do this all the time.

MS. HERMANN: Right. We have the IEEE standard for configuration management as part of the Chapter 7 review, but we can't say use Doors. That's a commercial product.

MEMBER BROWN: I didn't say that.

MS. HERMANN: Right.

MEMBER BROWN: But the methodologies, there's other ways to specify methodologies, as opposed to telling somebody to use a specific product, or software program. Doors is -- I don't even like to think about Doors.

MS. HERMANN: Antique.

MEMBER BROWN: It's not only antique, it's too cumbersome. You spend more manpower doing it than you get results out of it. Excuse me. I tried that years ago, rejected it in about a month. Okay. I quit. I throw my towel in. Nobody cares. Pardon? Dennis, help me out.

(Laughter.)

MEMBER BROWN: You guys are leaving me hanging out to dry. Let's get -- okay. Continue.

MR. STURZEBECHER: So the first set of comments, as I mentioned, were 208, and they were from participants, NERC, FERC, DHS, NIST, Joe Weiss, control system vendors, licensees, and NEI. We used this particular document to bend them and try to get understanding what is going on with the overall consensus, what they thought of DG-5022. And the next slide, you can see the breakdown where the higher number of scope moved the retyped statements. We worked through that, and our second meeting was on December 4th, where we moved the comments down to around 14, we had 12, there was 6, and two weeks ago we had completed comments.

MEMBER BLEY: The current draft we have has all these comments rolled into it.

MR. STURZEBECHER: Right.

MEMBER BLEY: There are only a few really technical ones it looks like.

CHAIR APOSTOLAKIS: Is that one of the

major comments from the stakeholders? Did you mention those?

MEMBER BLEY: At least the technical comments.

MR. STURZEBECHER: The major comments -- let me step back.

CHAIR APOSTOLAKIS: First of all, who were the stakeholders, NEI?

MR. STURZEBECHER: Yes. NEI, we had Stars. We had -

CHAIR APOSTOLAKIS: Stars?

MR. MORRIS: We had Westinghouse there.

CHAIR APOSTOLAKIS: The whole industry. Okay. So what does it say there, A, B, C? Do we have that?

MR. STURZEBECHER: No, that was the original document which has changed. The red-line was -

CHAIR APOSTOLAKIS: Oh, these are the numbers.

MR. STURZEBECHER: Those are the numbers, right.

CHAIR APOSTOLAKIS: So we are agreeing the Cyber Security Plans needs to be clearer. But I guess what clearer means is subject to interpretation. They wanted less, we want more. Guides should leverage existing NRC. What does that mean?

MR. STURZEBECHER: Well, we should leverage other Reg Guides.

CHAIR APOSTOLAKIS: Have you gone over this slide?

MR. STURZEBECHER: No. Just flip that. I was saying we went from 14 comments. These are the highlights from those second set of comments after we worked on a guide. They were asking us to leverage more with other programs and processes that exist in regulations.

CHAIR APOSTOLAKIS: Can you give me an example of what that means?

MEMBER MAYNARD: The way I interpret that one is they're saying rather than come up with a bunch of new requirements where we have existing requirements, let's see which ones of those that we can use.

MR. MORRIS: Correct. An example would be 50.59 design controls, changes to systems, structures, and components.

CHAIR APOSTOLAKIS: So you did this.

MR. LEE: Yes. And configuration

management was another one. They wanted to use a process or procedures.

MEMBER BROWN: Which ones?

MR. LEE: Configuration management.

MEMBER BROWN: Yes. Was there a standard they wanted to use?

MR. LEE: They want to use the existing process for the safety systems, and they changed the NEI configuration within the nuclear power plant. And they want to follow the similar process, but for the cyber security aspects, what they want to do is they're going to -- whenever they change anything - first of all, when they perform the vulnerability assessment, they identify all the potential vulnerabilities. That would include any type of connections associated with the particular critical systems. So whenever they change anything, meaning any kind of connections or systems, they're going to do a full evaluation following the 68.47 process. And then they identified the vulnerabilities and see what those risks can -- cyber risks to that can adversely impact cyber security, I mean, safety and security functions. So they'll follow the process to address the security aspects before they actually implement, so they want to follow -- incorporate that into their HSN program, configuration management program.

CHAIR APOSTOLAKIS: This is interesting. Industry format moves all detailed sections to appendix, but there is no appendix. Is there?

MR. STURZEBECHER: No.

CHAIR APOSTOLAKIS: There will be one?

MR. STURZEBECHER: Yes, there will be a separate NUREG. They literally wanted a lot of the prescriptive details moved into the appendix.

CHAIR APOSTOLAKIS: You just disagreed?

MR. STURZEBECHER: They disagreed, yes.

CHAIR APOSTOLAKIS: So you eliminated them completely.

MR. STURZEBECHER: No, we did not. Well, we took the features that they were talking about and went to attribute levels, and that's how we tried to find consensus with this.

CHAIR APOSTOLAKIS: Can you remind me again this NUREG, when is it coming out?

MR. STURZEBECHER: We have a series that we're working on.

MR. MORRIS: Right now, it's hard to pin it down, but our goal is to have most of it done by this calendar year. We've already got all the information. It's just a matter of packaging it in a way that looks like an NRC document, as opposed to the sort of mish-mash of different things, things that we had stripped out of the original version of the Reg Guide, information available from other government entities, like DOE, and DOD. I mean, there's a lot of documents out there. It's just a matter of put an NRC stamp on it. It's actually one of the things my friend next to me is going to be working on.

MEMBER BROWN: So it will be a NUREG, not an appendix.

MR. MORRIS: Correct. Originally, it -

MEMBER BROWN: All the details you took out will become a NUREG. I'm trying to summarize what I've -

MR. STURZEBECHER: Right. And examples of how you would do it, direct features.

MEMBER BLEY: Now, there is a comment up here that mirrors what Deborah said earlier about physical and logical boundaries not having one-to-one correspondence. When you speak of logical boundaries, are you speaking of the functional things that I see in the NUREG, or what do you mean by logical boundaries?

MS. HERMANN: Well, in -- at an abstract level software is logical, it's not physical.

MEMBER BLEY: That's true.

MS. HERMANN: And so your -- depending on how you -

MEMBER BLEY: So this is just dealing with software.

MS. HERMANN: Software and the implementation of security controls that are embedded in software.

MEMBER BLEY: I mean, did they want you to make them the same?

MS. HERMANN: No. We're just clarifying that.

MR. STURZEBECHER: Right. They didn't want the vital area tied to a before -- or a three tied to physically because it's going to change. It's site-specific, and it goes with the performance-based, and that's the key to understanding what they're going to propose.

MR. HECHT: Do you consider software to be stuff in P-Logs, Flash memory?

MS. HERMANN: It's what resides -- it's sort. The EPROM -

MEMBER BLEY: Anything with the program.

MS. HERMANN: Yes. The boundary between hardware and software is getting grayer and grayer. Software is stored on a physical media, but software itself is logical.

MEMBER BLEY: Okay.

MEMBER BROWN: Software is stored on a physical media?

MS. HERMANN: Yes.

MEMBER BROWN: Yes, I got that part. But software itself is logical.

MS. HERMANN: Not physical.

MEMBER BROWN: Software is stored on physical media, but software itself is logical, not physical.

MS. HERMANN: In French, the word for software is logic.

MEMBER BROWN: I don't deal with the French.

(Laughter.)

(Off the record comments.)

MR. HECHT: I just want to also point out that -

CHAIR APOSTOLAKIS: Myron. Go ahead.

MR. HECHT: In Part D, or the final statement about the backfit, there appeared to me in my simple reading of it that there was something of a contradiction like the very final page where you're making the backfit statement. It says in the beginning of Section D, it says, "The NRC does not intend to approve any imposition or backfit in connection with issuance." And then in the final statement, "The NRC has determined that in accordance with 10 CFR 50-109(a)(3), a substantial increase in the overall protection of the public health and safety or the common defense and security will be derived from the backfit. And the direct and indirect costs of implementation are justified."

MS. HERMANN: That's a Scott question.

MR. HECHT: It looks like there's some boilerplate, but you -

MR. MORRIS: Well, it reads like boilerplate, and certainly you'll find similar language in other regulatory guides. But the regulatory analysis that was conducted as part of the rule itself, 10 CFR 73.54 and the bigger rule, all the power reactors security regulations that it's part of, that's where you'll find the regulatory analysis, and it's pretty detailed. It's a lot of financial number crunching in the analysis. We can certainly make that available to you, but it's -

MR. HECHT: No. It's just a question of there appear to be a contradiction where the first paragraph says the NRC does not intend to impose, and the final paragraph says it's really worth doing a backfit.

MR. MORRIS: Sounds like a good question for a lawyer.

MR. HECHT: Yes. This is what we call in law school the -

(Laughter.)

CHAIR APOSTOLAKIS: Okay. Any other comments or questions from the members?

MEMBER MAYNARD: I did have a comment on this. I've been reviewing some other reg guides, especially in the security area. And, first of all, I believe that cyber security is important. I think we need to have programs in place and some things. I'm getting concerned in the cumulative effect of a number of things that we're doing as to what point do we start impacting other aspects of plant operations that could cause even more of a problem. We could end up with security IT watchers and the operating staff if we get carried away on some of this stuff. And no matter how far you go on this, with enough time and effort, people can always find a way to defeat it. We're dealing with that all the time in all areas. No matter what somebody comes up with, somebody can come up with a way. So I think at some point we've got to determine what's reasonable, and make sure that it doesn't start impacting other things that are equally, or even more important maybe to plant safety.

And I get into it not all together just does it have a direct operational -- but any time you're taking funds, money doesn't grow on trees, so you're taking it away from something else. You may get some increase, but typically it's not as much as whatever the new cost is. Whenever you're taking resources away, it takes it from some place. Management attention, I don't care how good of an operation you may have, if you stop focusing on that and start focusing on something else, that starts degrading. So I think it has to be looked at in an integrated approach as to what level is reasonable considering the overall operation of a power plant to insure that we don't start degrading overall safety just to try to improve something in one area. That's the comment I have.

CHAIR APOSTOLAKIS: Okay. Now, since there is a letter to be written next week, would it be appropriate to go around the table and see what input you gentlemen want to give me?

MR. MORRIS: If I may, Dr. Apostolakis, could I just offer a few sort of closing thoughts?

CHAIR APOSTOLAKIS: Absolutely. Yes.

MR. MORRIS: Okay. Great. Thank you.

First of all, I personally -- I appreciate the opportunity, and I'm glad that we had the opportunity to share this with you all. As you know, we have not typically shared the regulatory guides that we have built and are building in the security arena with the ACRS, so this is a somewhat unique opportunity. And it's actually outstanding to get some fresh perspective on what we've done, because the Staff has had their head down on this for a long time, so this is very good. And I do appreciate it.

I do want to just sort of -- a couple of things were mentioned during the course of the discussion I didn't really hear closure on, and I kind of wanted to make sure that I address very briefly. One is this concept of external versus internal. The internal attack to the extent it's manifested or presented, is extremely problematic, not only in cyber security, but physical security.

And we've done an awful lot in security world, in the personnel security world, and insider mitigation programs to make sure that the people who have access to these systems and these networks are appropriately screened, checks done, behavioral observation, a whole range of things, programmatic and design to deal with the insider problem. But you're never going to completely eradicate it, at least the potential of it. But I didn't want to just sort of walk away with it without coming to some kind of -- coming back and saying look, this is something we're very concerned about, not just in cyber, but across the board.

With respect to -- there was some talk about -- we didn't talk about it directly. There was some tangential comments about Chapter 7 reviews, and Chapter 13 reviews, referring to Standard Review Plan. Chapter 7 is more your system-level reviews. You're down at the system level. If you're familiar with the Duke Energy's application at Oconee to put in a new RPS SFAS system, that's what I would call more of a Chapter 7, down in the weeds system-level kind of review. That's really not what this Reg Guide was designed for. This Reg Guide was designed for the higher level programmatic Chapter 13 site cyber security program, as opposed to system-level licensing kind of concerns. So just a little bit of a different perspective. And this is actually an area that we guard against quite closely with just finding roles and responsibilities between the Staff and New Reactor Office, and Office of NRR doing the system-level stuff, and NSIR taking a giant step back and looking at the programmatic reviews. But there is overlap, and it is a challenge for the Staff.

The other point -- there were a couple of excellent points made about we shouldn't put a lot of energy into stuff that's happening out at level one, two, and three. And I fundamentally agree with that, the focus is the stuff that can directly affect safety. And so, again, the whole point of this is really a defense-in-depth graded approach, where if there's something that can happen that can effect or cause radiological sabotage, meaning a release of fission products to the environment, those are the things we need to focus our energy on, not only for physical security, but also cyber security. And that's not lost on us. And to the extent the words can be improved to make that point more clear, I think that's an excellent point.

And the idea of the use of examples, I

think has a lot of merit. I don't disagree with it. I think it has been somewhat of a challenge, frankly, interacting with industry on that point, because I think it was Jim from NEI mentioned that there tends to be -- the industry tends to take it as de facto regulation, even though it's just guidance, and one way to do business. So we were trying to be sensitive to that, but I do hear the Committee, and I think it's a valid point, and one that we should seriously consider going forward. So I'll leave it at that, but I do appreciate the opportunity, and look forward to doing this again next week with the Full Committee. Although, I have to say, I won't be here. I'll be in Vienna, so you guys have a good time.

(Off the record comments.)

CHAIR APOSTOLAKIS: We have a comment.

MR. QUINN: My name is Ted Quinn, and I'm representing Diablo Canyon today. And I'm an instructor for the NRC digital classes we've had in the past few years. My comments are there's three levels of documents in cyber security that has been covered today. There's public domain, there's official use only, and there's safeguards. And I think the Staff has done a very good job. I support what Jim Riley said, in trying to have the policy issues and the high level in a public domain, or as close to public domain as you can. And then examples will be at lower level. What you saw today was NRC regulations, what we have out in industry, and the vendor and utility community is those same documents, called the same, and they will be corresponding and complementing what the NRC requirements are at the different levels. For example, some of the examples of implementing really don't belong in a public use document. They will go at a lower level, just so when you get briefed next time on the lower level document.

I suggest just a couple of recommendations. First, the challenge will be in implementation for this, for two reasons. One is, at the plants, or at the vendors when you're looking at the systems, we would -- it would be great if in the inspection processes there's some level of correlation with acceptance criteria that's applied pretty much across the board. It would be really beneficial if there's not one plant that's asked to do things that are not consistent with others. And the other is, the Staff has done a very good job in being a filter to other agencies that are making requests in the same area. And it's really encouraged that as you get challenges from other agencies, that you continue to be that filter that you've done. It's so important, that it comes from one -- it's so important, so thank you.

CHAIR APOSTOLAKIS: Great. So we want to do that, go around the table?

MEMBER SIEBER: Sure.

CHAIR APOSTOLAKIS: Jack, you're anxious to tell me something.

MEMBER SIEBER: Okay. I guess, first of all, there was discussion about the fact that the rules and the Reg Guide, and all speak in generalities. I think I understand why you're doing that, so that's okay with me. On the other hand, the details of how this is going to be done is going to be in plant documents, which are going to be restricted safeguards information. And I think that's where the keys to whether the plant will work or not work will be found.

On the other hand, because we speak in generalities, it's not clear to me what criteria licensees need to meet to be able to have a satisfactory security plan, what's good for one may not be good for another, just because of the passage of time between them. I don't know that we would do anything to the rule, the Reg Guide, or the documents that we've been shown so far to change that, but that's something that has to be kept in mind.

Another thing that strikes me a little bit, had some experience in I&C, and operating plants and so forth, is I hope the implication is not put out here that the physical security organization in the power plant should be the ones to run the cyber security program. To me, cyber security is an I&C function, which is part of the maintenance department. Operators in the control room do not change software. They don't have the tools or the equipment to do that. And the I&C Department is the ones who physically do it, but a lot of that software comes from vendors. And so your cyber security process and controls have to reach into the vendors office, so that you have a secure path all the way to your machine.

And another thing that I learned through the years is if you have a modem somewhere on your computer, you might as well just forget about security. And vendors say I would like to be able to input this directly into your machine from some off-site place. I wouldn't do that. I wouldn't allow technicians to be able to change software from their homes. They'll tell you I'm available 24 hours a day, I'm so smart, I can fix anything on your machine. All I need is a dial-up port. Don't do that. And I don't know whether you want to put it in regulations, but if I were back in the licensee business, I would never do it again.

(Laughter.)

MEMBER SIEBER: So when we write these overarching rules, if we keep in mind the physical security stretches into vendors shops, that it really belongs to the people who work with the computers, and not the guys that carry the firearms, that would be comforting to me.

CHAIR APOSTOLAKIS: Okay. Thank you. Sergio.

MR. GUARRO: Yes. Well, let's see. I've been struggling a little bit with this problem of how you go from a level of abstraction, just general, and have to cover the programmatic aspects, and, at the same time, deal with the fact that, in fact, you cannot be too specific, you don't want to reveal information, and the issue of where do you put the boundary so that you have a document that not only gives general guidelines, but gives criteria that are practical enough so you can get a sense for how much you need to do to satisfy the regulation. I mean, if I were a licensee, maybe I'm biased in this, but looking at this document, on one hand I say well, okay, it's good because it leaves me -- it's not too prescriptive. But the flip side is that I wouldn't know at what level I will have to stop in order to satisfy the rule. So it seems to me that the path of having some kind of a model that you use to provide example, and it's a sanitized model, so it's not anything that reveals information that can be exploited by anybody, but serves the purpose of providing an example, the type of graded approach that you have to have, and address the different layers of your circles there, conceptually understand the circles, but what physical hardware and logical software corresponds to what circle is not clear to me based on what I read here. So that would be my suggestion.

CHAIR APOSTOLAKIS: By the way, you don't have to sit there now. All these comments are addressed to me, not to you. If you want to sit down, that's fine. If you want to stay there, that's fine, too. Dennis.

MEMBER BLEY: Yes. A couple of things

Jack said I'd like to echo. The configuration control with the software, whether it comes from at the vendor's site, anybody who can touch it all the way. I know there are words in here dealing with that, but that seems to me probably one of the hardest things to keep control of in a place that's really important. And I suspect it won't be in the Reg Guide, because it's already there a little bit, but in the implementing guidance that's going to come. I think that's really important.

One thing that was talked about earlier today, John brought it up, and Deborah talked about it, too, and that's that the guidance on vulnerability assessment ought to include something akin to Haz Op, and how can -- what things can make these systems not fail to do what they're intended to, but do something they're not intended to do and get us into trouble. I don't think it's there, but it would be really useful.

Overall, the level of the guidance, the more I got used to it, the more comfortable I am with it. A few examples to make it clear what these things are about would be helpful, not to tell people how to do it, but just clarify. That would be useful.

CHAIR APOSTOLAKIS: Okay. John?

MEMBER BLEY: Sorry.

MEMBER STETKAR: No, that's okay. Don't be sorry. I don't have anything to add to that.

CHAIR APOSTOLAKIS: Okay. Mario?

MEMBER BONACA: I think there have to be some examples in the guidance that will make it more of a guidance, rather than an expansion of the rule. So I think I'm voicing some perspective of the others. That's it.

CHAIR APOSTOLAKIS: Otto?

MEMBER MAYNARD: I got more comfortable with the level, especially I think if there is to be more details, you're probably starting to look at the safeguards aspect of it, if you really want to make it meaningful, and it's probably not appropriate for this document, that level of detail. Example is fine. I think you have to be careful that you don't imply that the example is the criteria.

CHAIR APOSTOLAKIS: Be careful how you write it. Charlie?

MEMBER BROWN: I want to -- Jack very succinctly stated some of the issues that of great concern relative to how you communicate. Anything you have in there that's got a modem in it, or anybody's access from any other points, that you're just asking for trouble. But in that light, examples can be not just necessarily what you do, but things that you say don't do. And that may be prescriptive, but that may be a way -- that may be some types of -- even though you might generalize it, you can prepare examples that illustrate the problems with that type of easy access into stuff by having modems in various of these computer systems, or whatever they are, whether they're the control room stuff, not necessarily the RPS. They probably won't have that, maybe.

The other issue that bothers me in this whole thing is the software control, how you -- I haven't seen it in the I&C world in any of the definitions, and I may just not have looked at the right stuff yet, but that -- as I've learned over the hard way, there were two things. Number one, making sure people aren't putting new parts in that have different software in it, and that any transmission or any installation of new, whether it's done by inputting data, be it a laptop or be some other device into the memory, or whether it's replacing a chip, if that's the way they want to do it, it has to be very carefully controlled. And I say that from personal experience.

My first project, I found guys were sending proms to the shipyard, just every time I turned around I was watching -- I'd see little notes going around that another prom was being -- because we found a software error. Finally asked the guys, I said well how do you know what version you've got? Oh, it's on the drawings. I asked them to show me. Two weeks later they couldn't show me. We stopped everything, established a methodology for doing this. It's very important, particularly when they're in the test program, and they start finding glitches. They're installing it, and they find that they've got to make some changes. You can really get out of control when you're in that installation and testing mode. That's point one.

The second point is the hardware that you use to do these either communicate with the systems. You've got to maintain hardware control, hardware that you put an application on, and then communicate with the system, so you can't get this laptop with this stuff in it. Now you're buying the latest one three years later. It's got supposedly the upgraded the version of the software, the general operating system. You go plug your application in, you try to

-- it just blanks everything up. That's happened. I've seen it happen, not programmed, learned that the hard way after I retired. They've been fixing it for the last five years, and it's taken a lot of effort to do that. So it's not just software, it's hardware tools that connect it that have to be maintained in their configuration. It's very critical. Otherwise, things can get messed up very easily. So that's it for me.

CHAIR APOSTOLAKIS: Myron?

MR. HECHT: I think I've already used up my allocation, but if I were to say a few things, more definitions of terms, particularly terms that we all think we know. Vulnerability, as opposed to threat, as opposed to cyber risk. And the other thing is I think it's very important that we have some idea of the scope of in general the threats, and I understand at very specific levels it gets into safeguard information, and I wouldn't want to do that. But on the other hand, to know that we're talking about more than some Russian somewhere sending a virus to my computer to make it send emails, act as a robot, I think it's important to know.

And one thing that I was thinking about, as everybody said, give me examples. I think what we're all trying to ask for is, what are the acceptance criteria, I mean, when it says there's a method to do this, and it lists something, what -- how can we determine whether that method is acceptable? That's a challenge to you guys. I don't think I have an answer, but I think that's basically what we're looking for.

CHAIR APOSTOLAKIS: Thank you. Okay.

MEMBER BLEY: Mr. Chairman?

CHAIR APOSTOLAKIS: What?

MEMBER BLEY: In preparing our presentation for next week, is there something you'd like to see us specifically add, or remove from this presentation?

CHAIR APOSTOLAKIS: Well, you have seven slides, and how much time do you have, an hour and a half?

MEMBER BLEY: I believe.

CHAIR APOSTOLAKIS: At least.

MEMBER BLEY: I believe it's an hour and a half.

CHAIR APOSTOLAKIS: An hour and a half.

MEMBER BROWN: It took two and a half.

CHAIR APOSTOLAKIS: I would like to see -

MEMBER SIEBER: Eighteen slides.

CHAIR APOSTOLAKIS: I'm sorry?

MEMBER SIEBER: Eighteen slides in an hour and a half.

CHAIR APOSTOLAKIS: Yes, cut them down a little bit. A lot of the history and the stuff that you have there is not necessary.

MEMBER BLEY: Okay.

CHAIR APOSTOLAKIS: The number of comments from the stakeholders, no. But the contents of the comments is important. Do you think -- well, it's only next week, but do you think you can have a couple of slides addressing the questions that were raised?

MR. MORRIS: Sure. We'll do that.

CHAIR APOSTOLAKIS: Okay. That'll be good. I will mention them in my introduction, too, but I think this is what the Subcommittee said, and this is what we think. Yes. Cut down the number of slides, because it's -- for some other members, all this will be new, so they may ask questions. That's it, as far as I'm concerned.

Do you want know my view, too? Well, I really think they ought to put some examples, and I agree with Otto that the language has to be appropriate. That's fine. I'll go along with that. And those will address, even though we don't we call them that, that they will at least give some idea to the licensees as to what is acceptable. It would define in some way, outline, not define what is acceptable. So other than that, I think everything you gentlemen said makes sense to me, so it will find its way to the letter. And that's it. Thank you very much. Appreciate it.

Now, the schedule calls for another presentation on diversity strategies. I suggest we take a break until 4:30, and then we spend maybe an hour plus with that.

(Off the record comments.)

(Whereupon, the proceedings went off the record at 4:13:55 p.m., and went back on the record at 4:37:15 p.m.)

CHAIR APOSTOLAKIS: The next subject is a review of Draft NUREG CR on diversity strategies of nuclear power plant instrumentation and control systems. Mr. Michael Waterman, an old familiar face will be making the presentation.

MR. WATERMAN: Hello, Dr. Apostolakis.

CHAIR APOSTOLAKIS: Assisted by Mr. Wood

of a distinguished National Laboratory. It's late in the day, Mike.

MR. WATERMAN: I'll bet you're glad to see me.

CHAIR APOSTOLAKIS: Take that into account.

(Laughter.)

CHAIR APOSTOLAKIS: So you also have the floor tomorrow morning.

MR. WATERMAN: Yes, I do.

CHAIR APOSTOLAKIS: So in about an hour, pick the right place in your presentation where it would make sense to recess for tonight.

MR. WATERMAN: Okay.

CHAIR APOSTOLAKIS: Okay.

MR. WATERMAN: Very well. My name is Mike Waterman. I am in the Office of Nuclear Regulatory Research, in the Division of Engineering in the Digital Instrumentation and Control Branch. I'm a Senior Engineer there. With me today is Dr. Richard Wood from the Oakridge National Laboratory. Dr. Wood is the Project Manager and the Principal Investigator for this project. We contracted with Oakridge National Laboratory a few years ago.

Dr. Wood is also, I would say, 99 percent of the author of the draft NUREG. I think it's an excellent document. He put a lot of time into that document, and he's here with me today to help answer some tough questions.

Also in the audience are my Branch Chief, Russ Sydnor, and my Deputy Division Director, Stu Richards. Dan Santos is here. He's our Senior Technical Advisor on digital instrumentation and control. Of course, Steven Arndt's here, too, so I feel pretty comfortable with -

CHAIR APOSTOLAKIS: Of course, Steve Arndt is.

(Laughter.)

MR. WATERMAN: Before I start, I'd like to say some words about the draft NUREG. That NUREG/CR was delivered to us in December time frame of last year. We sent it off to NRR and NRO, our customer, if you will, and asked for their comments. We received those comments around the end of January, and we haven't had enough time to actually incorporate all of these really insightful, excellent comments into the version that you have. So what you're looking at, I can assure you, will probably change, and so just keep that in mind as we move through here.

We'll incorporate those comments. We're making that document also available to the public, because I'm really looking forward to hearing from industry and the public. I expect to get some really excellent comments out of them, too, to improve this report, and make it something that we can really use to help move forward through this area of diversity in digital instrumentation and control.

CHAIR APOSTOLAKIS: So this is focused only on diversity.

MR. WATERMAN: This is focused only on diversity, and I'll get into -- yes. Thank you for that point.

MEMBER STETKAR: Mike, just a simple request, because we have like an hour and there's a ton of information here. And the Committee is going to bog down in the beginning when you start talking about all the experience. If you could, if the questions start going on a little, I'm really interested in getting to the back-end of this, where you do the numerical assessment process, because that's sort of where the whole thing is going. So just, if you can control the time and the presentation to shut down people so we have enough time to get to the back end, I'd really appreciate that.

CHAIR APOSTOLAKIS: Tomorrow morning.

MEMBER STETKAR: Tomorrow?

MR. WATERMAN: I've got all day tomorrow.

MEMBER STETKAR: Oh.

MR. WATERMAN: I've got all night tonight, all day tomorrow.

CHAIR APOSTOLAKIS: We will be fresh.

MEMBER STETKAR: Never mind.

CHAIR APOSTOLAKIS: For the numerical stuff.

MEMBER BROWN: It's my understanding this is diversity strategies? That's the way the title of one of the other documents -

MR. WATERMAN: That's right. This research did not go out with the intent of determining if diversity is needed, whether or not diversity is needed. That research has already been done, and I'll get into that in a minute.

What this research did was we wanted to go out and find out - you're ruining my presentation, Mr. Brown.

(Laughter.)

MR. WATERMAN: To go out and find out well, what's the world doing about diversity, how are they implementing it? And I'll get into that in just a second.

CHAIR APOSTOLAKIS: And how much is enough. Right?

MR. WATERMAN: That's right. Darn it, as the industry would say. So I'll frame where the research is starting from, I'll talk a little bit about operating experience considerations. I think I've only got two slides on operating experience, so I'm not going to get into depth on that. Talk about the assumptions we used when we went into the research, about how we could use the data, a little bit about the sources of data that we looked at, and then get into the data evaluation method that we proposed out of this; a fairly simplistic method, but it seems to be working. And then I'll summarize the results of the evaluation, talk a little bit about constraints on using the evaluation method, and talk then about where we're going from here, and summarize the presentation.

Now, let's talk about regulatory focus on diversity. First, 10 CFR 50 Appendix A, GDC 22 has words to the effect of "use diversity to the extent practical." Right? As a matter of fact, quote, "functional diversity or diversity in component design and principles to be used to the extent practical."

Now, a Staff Requirements Memorandum to SECY 93-087 also comes out and talks about diversity, and it says, "verify adequate diversity has been provided." And then we did some research back in the late `80s, early `90s through Lawrence Livermore National Lab, and they produced a report, NUREG/CR 6303 on evaluating diversity in nuclear power plant safety systems. And that provides guidance for identifying the need for diversity. There's methodology in there, you can do blocks, to identify the need for diversity.

The issue is, is that the regulatory guidance and requirements do not define what constitutes adequate diversity. They just say go apply diversity, but there's no guidance in there that says okay, how much diversity is enough in a safety system design? And because nobody's really defined how much is enough, we've got an amazing amount of licensing uncertainty out in the industry, because we have all these different interpretations of what we mean by adequate. So the licensees are sort of pulling their hair out. They submit a design, it might get rejected because there's not enough in there. So the Agency and the industry really need to start coming together here, and coming up with a common ground to work in with regard to how much diversity is enough.

We identified that issue further. We formed a Task Working Group, Task Working Group 2, which was focused on diversity in defense-in-depth, and question number one in there was, "How much diversity is enough? After you identify a need for diversity, how much is enough?"

What the research does not address is whether or not diversity is needed. We've already done all of that. So we've got a research effort going, we had one going that is addressing that question of how much diversity is enough.

CHAIR APOSTOLAKIS: Wouldn't that be a policy issue, though? That's not a technical issue.

MR. WATERMAN: How much diversity is enough?

CHAIR APOSTOLAKIS: Yes.

MR. WATERMAN: Well, actually, it is a technical issue.

CHAIR APOSTOLAKIS: Well, the technical part would be to develop a metric that tells me how much diversity I have. But how much is enough comes from upstairs.

MR. WATERMAN: Well, how much diversity is enough should be enough to address the common cause failures that you either postulate, or you've identified. For example, if I decide well, I'm going to use a different micro processor, or different software - well, is that enough? I don't know.

CHAIR APOSTOLAKIS: So you're talking about decisions at a much lower level.

MR. WATERMAN: At a much lower level, at a level where the regulator and the industry can come to a resolution -

CHAIR APOSTOLAKIS: I understand. That's fine.

MR. WATERMAN: Okay? So let's define defense-in-depth and diversity here. Now, defense-in-depth is a principle of using different functional barriers to compensate for failures of other barriers. Right? For example, here we've got this -- and this is conceptual before the industry gets upset about reactor trip systems and engineering safety features backing up each other. We have here a hazardous condition that is addressed by the control systems; whereas, maybe there's a hazardous condition that can't be addressed by a control system, so you have a reactor trip system to trip the reactor, so you've got two different functional barriers there.

Now, contrast that with diversity, which is a principle of using different means within a functional barrier to compensate for failures within that barrier. And here we've got diverse reactor trip system here, and a diverse engineered safety feature system down here; such that, this is an example here of diversity, where your diverse reactor trip system blocks this particular hazardous condition from defeating the reactor trip system. Whereas, here you've got something that defense-in-depth would handle. The reactor trip system couldn't handle it, so maybe you have another -- so that gives you a context of what defense-in-depth is, what diversity. I've heard a lot of people use them interchangeably. They shouldn't be.

So what are common cause failures? Well, if you look at IEEE 100, the authoritarian dictionary of standards and terms, they have a couple of definitions for common cause failure. The definition number two here is out of IEEE Standard 603, and IEEE Standard 379, which is single failure standard that we use in the nuclear power industry. And that's multiple failures attributed to a common cause, sort of short, and sweet. I probably had something to do with writing that.

If you look at IEC's definition -

CHAIR APOSTOLAKIS: Actually, this Agency sponsored a major project on CCF a number of years back with EPRI and so on. And, actually, they were very careful to say that it's failure of redundant components due to an unspecified cause. For example, although, of course, if you take it literally, an earthquake is a common cause failure, it doesn't belong to the class of failure causes we call common cause failure, because it is a specified cause, and it's analyzed in a PRA explicitly. It's those other things that are not analyzed explicitly. I mean, if you go back to the NUREG, I don't remember what the number was, but they said these are a class of common cause failures.

MR. WATERMAN: Yes. IEEE Standard 379 excludes a certain class of common cause failures from single failure consideration. But if you look at the wording in there, I've yet to find a common cause failure that can't be excluded by 379.

CHAIR APOSTOLAKIS: We did have a definition in NRC's -

MR. WATERMAN: Yes. But earthquakes and all those external things are excluded from consideration in single failure -

CHAIR APOSTOLAKIS: Because they are done separately.

MR. WATERMAN: 62340 defines it a little bit more, I think a little bit more clearly, as a systematic incorporation of latent faults into multiple systems followed by a triggering of those common faults. And Dr. Thuy Nguyen, that's right along his line there.

CHAIR APOSTOLAKIS: You know, every time we look at those kinds of documents, I find them either to be - let me put it this way - not very carefully done. Is it because we're spoiled here, where we review, and review, and review? I mean, these IEC - geez, IEEE Standards and software. I mean, it's a vicious circle.

MR. WATERMAN: Well, these are -

CHAIR APOSTOLAKIS: Go here, go here, go here, and you end up at the beginning again.

MR. WATERMAN: These are consensus standards written by a committee. And you know what they say, a camel is a horse built by a committee, so yes.

MEMBER BROWN: Well, that's what I would have said on the stuff I used to look at, or have to get involved with, is you're trying to satisfy so many different people coming in that the compromises drove it to the lowest common unpalatable denominator.

CHAIR APOSTOLAKIS: They have Markov models and all that stuff, and I say, my God, why did they decide to do this? Did anybody ask what the Markov model does, Steve, or you?

MR. ARNDT: Well, actually, Richard and I, and a couple of other people in this room sit on the IEC Standards -

CHAIR APOSTOLAKIS: Oh, so the new documents will be much better.

MR. ARNDT: I wouldn't count on it.

MR. WOOD: I participate in IEEE and IEC, and I'm sometimes amazed by what gets stripped out of those documents just to achieve the consensus. But in the IEC world, they do have the option of informative annexes so that a particular country that feels strongly about specific guidance can include that, and then endorse it in their own endorsement of the overall standard.

CHAIR APOSTOLAKIS: But nobody seemed to

disagree with my assessment.

MR. WATERMAN: As a matter of fact, I've been on IEEE Working Groups for the past 15 years, and what we found, usually, is you get the most work done when only two or three people show up.

CHAIR APOSTOLAKIS: Okay. Good.

MR. WATERMAN: So guidance for addressing CCF, NUREG 6303, just to set the stage for what it does and doesn't do, it describes a method for analyzing computer-based nuclear reactor protection systems that discovers and identifies design vulnerabilities to CCFs. And in that NUREG, it identified 25 diversity attribute criteria that compromise six different diversity attribute categories, so we've got a little taxonomy here. A category is made up of -- or an attribute is made of a -- 6303 also ranked the criteria in decreasing order of relative effectiveness within an attribute. If you look at it, they say this is more effective than this, and that's more effective than that.

It did not rank the attribute effectiveness relative to other attributes. It just listed them alphabetically, and addressed each attribute. And that NUREG was published in October of 1994. And for those of you who want to get a copy of it, it's publicly available under that ADAMS access number.

So, the diversity attributes and criteria in NUREG 6303 are oriented toward computer-bases safety systems. They sort of technology-dependent. And in order to address other types of safety systems, such as analog-based systems, and FBGA-based systems, the equipment attribute right here was divided into two new attributes, an equipment manufacturer attribute, and a logic processing equipment attribute. They're a little bit different.

The logic processing equipment attribute criteria were renamed to make the criteria less technology-dependent, so if somebody wants to use analog to back up digital, it can be applied a little bit easier that way.

The software diversity attribute down here was renamed the logic attribute. That's terrible aspect ratio, isn't it? And this change was made to account for logical representation, such as -- you could say that an analog system doesn't have a software equivalent, but it really does. When you design an analog system, you get out your detailed schematic and you say I'm going to have signal processor come down, and I'm going to feed that signal through a comparator, and it's going to go into a by-stable, and it's going to trip. So it's all laid out, it's not really software like C, but it's a type of logical representation. And so we changed it from software languages over to logical representation there. And it has its own algorithms. Right? I mean, you've got an algorithm, convert the data, check the data against a set point, and initiate a trip. So doing that allowed us to have a little bit more technology-independent criteria.

CHAIR APOSTOLAKIS: Okay. So what -- I'm trying to understand these circles.

MEMBER BLEY: So the only criteria that really changed are the ones that are now under logic processor equipment.

MR. WATERMAN: Logic processor equipment, that's right. Well, all the others are pretty general, anyway. Right?

MEMBER BLEY: Yes.

MR. WATERMAN: Yes.

CHAIR APOSTOLAKIS: So the word criteria or attribute should have been also in the circle -

MR. WATERMAN: If you look over here, here's the criteria.

CHAIR APOSTOLAKIS: I understand. But

the attributes are -

MR. WATERMAN: And the attributes are like signal equipment.

CHAIR APOSTOLAKIS: Also on the right.

MR. WATERMAN: And also on the right. Yes.

CHAIR APOSTOLAKIS: Okay.

MR. WATERMAN: That's right.

CHAIR APOSTOLAKIS: So if we look at this now, there is an attribute that you call human, or life cycle.

MR. WATERMAN: Yes. It was called human in NUREG 6303, but it really applied to the human activities that go into developing a product.

CHAIR APOSTOLAKIS: And then if I look inside in the orange sectors, it says, "Design organization". So now, I can develop criteria that will address this attribute by doing something regarding the design organization. That's the intent of this.

MR. WATERMAN: Well, one diversity approach is to use different design organizations. Right? Another one would be different management teams within the same company, things like that.

CHAIR APOSTOLAKIS: Okay. I understand.

MEMBER BLEY: And the new one, your standard beyond design are life cycles.

MR. WATERMAN: Well, now the life cycle still exists. We really didn't change the names of the criteria. It's still orange. Orange is orange.

MR. WOOD: It was mostly a semantics change, because the tendency to interpret human, the human attribute as something related perhaps to the operator in the plant, versus the humans that are involved in the life cycle phases.

MEMBER BLEY: Okay.

MR. WATERMAN: Yes.

MEMBER BLEY: Thanks, Richard.

MR. WATERMAN: So design diversity, what we did was -- what Richard did was, he described each of these attributes according to process, product, performance, and purpose. And so, I can briefly go through that. Design diversity purpose is related to technology choice and use, analog versus digital, micro processor versus field programmable gate array, Intel versus AMD. Those three categories, for example. And just going down through that, I can talk to those, if you wish, or you can read them. I was going to read them to you, but I thought everybody could probably read them.

Design is really the driver for all the diversity strategies that we'll talk about later. Design defines what technology is actually being employed as a diverse technology to the system you're trying to defend against common cause failures.

MR. WOOD: If I could interject, to help set -- Mike is presenting these in a systematic fashion. The way that we structured the understanding of the diversities and their effectiveness, is to identify things in terms of purpose, and process, and product, and performance. The purpose deals with like the functional requirements, or things like that. The process is the life cycle process that's engaged to create the product, which is the platform and the application itself. And then performance includes not only the performance of the system itself, but the influences, external influences that affect it. And the reason we kind of grouped those things is, purpose and process deal with sources of common cause failure vulnerability, and product deals with the location, or the impact of those vulnerabilities. And performance deals with the triggers that lead to the common cause failure. So those are ways of kind of parsing the information and determining whether the diversity attributes have an effect on the sources, or where the vulnerabilities occur, or how the vulnerabilities are triggered into failures.

MR. HECHT: I'm trying to understand, particularly with respect to process. Are you saying that you could achieve diversity by having two organizations use different life cycles to achieve the same -- to write software to the same specification?

MR. WATERMAN: That was the crux of the issue, Myron. That was exactly it, was that some people might argue that all I need is a different design organization, and I've got enough diversity. Well, other people might disagree with that. And the purpose of this research was to identify, are there combinations of those diversity attributes relative to experience, and judgment, and things like that, that are optimum combinations that will give you adequate diversity? So your question was right on the spot of yes, you could have different design organizations, but it's probably not enough. And we'll get into that.

Equipment manufacturer diversity is related to source of the hardware components or the aggregated systems. The process impact is attributed to the perspective effective from use of different resources, for example, components, manufacturing lines, the humans who are doing the actual construction of the device.

On the sources of systematic fault, the product impact is attributed to differences that may arise from the use of the different equipment, and the performance impact is via the different responses to external influences that you would get by having different manufacturers produce, for example, fundamentally different devices. You're going to have some kind of differences in response to external influences; and, therefore, while one might be susceptible to a common cause failure, you would think that something manufactured by a different manufacturer, and a fundamentally different device, it may not be susceptible to the same common cause failure triggering event.

Logic processing, that's related to differences between the types of logic processing equipment employed. Now, you remember over in design, we had different technologies. Now we're talking about different logic processing equipment employed. And the process impact is attributed to the perspective effect of the architectural differences for logic processing, on the source of the systematic faults, for example, errors that may arise. The product impact is attributed to susceptibility differences from the use of different processing elements or components. And the performance impact is via different responses to external influences.

The functional diversity, the process is attributed to differences in objectives, functional relationships. This is where you're talking about different functions, such as trip the reactor on high temperature, trip the reactor on departure of nuclear boiling, trip the reactor on high flux. They're all different trips, but they're all designed to protect the reactor using different instrumentation. And so, you'd lay out some functional diversity in there, so that if one particular function failed to trip the reactor, there would be a backup function in place to carry over.

The human life cycle diversity was related to the human influence, if you will, on the resources, the resource allocations, and the cultural effects. If you've got a team that they work a certain way, and they put things together a certain way, and by that process they could introduce common cause failures, if you have a completely different team, hopefully, they wouldn't do the same thing, so that type of thing there. Independent verification and validation is an example of addressing human diversity by having completely independent verifiers and validators look at something, process, product, and performances there.

Logic diversity. Remember, this was the old software diversity. It was related to different means, if you will, of instanciating the logic. You've determined the functions you want to do. Now you want to instanciate those functions into the systems that it operates in a certain way. And we can go through that, also take a look at that. I'm trying to rush along here.

The signal diversity is related to providing diverse indications, capturing different functional relationships. For example, you could use pressure transducers to give you a couple of different kinds of measurements. Right? You can use it to give you pressure, you use them to give flow, you use them to give level, so pressure transducers could be used in a lot of different ways, even the same pressure transducer.

MR. HECHT: Mike, just looking at logic

diversity, signal diversity, and functional diversity, they seem to overlap.

MR. WATERMAN: They certainly do. There's interrelationships among several of the attributes.

MR. HECHT: Okay. And that doesn't matter, or -

MR. WOOD: That's part of what makes it -- has made it complicated to use the guidance in NUREG 6303, is that you can do things in functional diversity, or you can accomplish a similar effect through design diversity, or through signal diversity, or in combination of different ones of those. And there was no systematic means of assessing that you've got adequate coverage of the perceived vulnerabilities.

MR. HECHT: Yes, because if I were to do a linear multiple regression just using those as separate variables, I think I would call those co-variates.

MR. WATERMAN: Well, if you take a look at function, function you may say I want to trip on high temperature. Okay? Now, you may decide that you want to use diverse temperature transducers to do two different high temperature trips. Right? So one is not dependent on the other. And in the logic, you may decide well, I'm going to use this type of algorithm for the high temperature trip in one system, and I'm going to use a little bit different algorithm using the same sensor and the same function to calculate a high temperature trip using this other one. So they're not -- it's not like if I pick one, I'm stuck with the others type thing. You can use a certain combination.

MR. WOOD: And if I may, let's take the issue of signal and functional and the relationship between the two. If the functional diversity is that you've got -- you're taking advantage of the different relationships between events and measurements to establish backup trips, then there's a significant tie. But if the functional diversity that you implement is instead of looking at measurements from the plant and determining do I need to trip; instead, like one of the railway example, I'm looking at the performance of the safety system and assessing whether or not it's actually performing safe functions, or potentially unsafe functions, so I'm not looking at measurements from the plant any more. And I've achieved a very radical functional diversity, and decoupled it from signal diversity in the traditional sense. There is a lot of subtleties involved in these things.

MR. WATERMAN: Use of operating experience. Knowledge of operating experience is necessary for the developer and the NRC reviewer to determine the set of failures that should be addressed. For example, if a licensee came in and said I've got a diverse system that addresses all the common cause failures, it would be handy for the Staff to know well, did you really address the full set of common cause failures? And by the same token, it would be handy for the licensee to also know did they actually address the full set of common cause failures. And one source of information is operating experience. It's not the only source, obviously, because there are some drawbacks to relying strictly on operating experience, and those drawbacks were identified in commercial grade item dedication. Right?

Failures of micro processors aren't always reported. It's a lot cheaper for a company to simply replace the defective micro processor than it is to do root cause analysis, write up the report, send it back to the vendor for a part that only costs $100, it's just not worth the time.

MEMBER BROWN: Do they really replace the parts, or the card on which that part resides? I haven't seen anybody that takes a 142 pin ball pin micro processor and try to unsolder it when it's been -- you'll destroy the entire -

MR. WOOD: They'll replace the cards.

MEMBER BROWN: Okay. Thank you. I just wanted to make sure I've categorized that -

MR. WOOD: But if you're looking at -

MEMBER BROWN: And there's a lot of other parts than just the micro processor on that card.

MR. WOOD: Yes. In the airline industry, they have line replaceable units that they pull in, plug in.

MEMBER BROWN: Okay.

MR. WATERMAN: You would hope that they would do root cause analysis on it.

MEMBER BROWN: I'm just trying to make sure I connected the individual from the what would really get replaced.

MR. WATERMAN: I was giving an example of why operating experience doesn't cover the whole gamut, because sometimes it's just cheaper to replace the part.

MEMBER BROWN: Well, it might not have

been the micro processor.

MR. WATERMAN: Might not have been.

MEMBER BROWN: Might have been the ADD converter, might have been the DIO, might have been any one of those things that failed.

MEMBER SIEBER: Connector.

MEMBER BROWN: Exactly. Could be a connector.

MR. WATERMAN: Talk to my car mechanic. And

MR. WOOD: And I'll make an observation on this point, that it's important that the knowledge you gain from the operating experience, what you've seen is addressed, but that doesn't mean that there aren't other things that you haven't seen. So you can't choose your diversity strategy strictly on the basis of what you've seen. You have to have given thought to what are the potential vulnerabilities. And I can point to instances in other industries where there may not have been any operating experience that showed a particular part was vulnerable, had high failure rate, or even a low failure rate; yet, they had diverse instances of that part because it was something that was complex, and they could not anticipate all of the potential failure modes and causes. So complexity is a big driver for looking for diversity.

MR. WATERMAN: The limitations of operating experience are hey, if it's a new technology, how much operating experience do you have? Right? If you've got new versions of currently used components - I mean, when we went from 486 to Pentium I, was it? To a Pentium chip, I mean, when you do that, how much experience do you have with regard to that new chip?

MEMBER STETKAR: How about a Z80?

MR. WATERMAN: Or a Z80, yes. Boy, that - you are almost as old as me.

MEMBER STETKAR: Probably older than you are.

MEMBER SIEBER: Yes, I was an old man when Z80s were new.

(Laughter.)

MEMBER BROWN: Relatively speaking.

MR. WATERMAN: And then the other operating experience limitation that I've run across are applications using existing components, new configurations. I remember an application that the developer decided they were going to use a 286 micro processor chip, because they'd been using that chip on Department of Defense Mission Critical Systems, and it always worked for them. They understood the chip. They put it into a new application in the nuclear power industry, and in that application it used master/slave processors that they never used in Mission Critical Systems in the military, and there was an error on the 286 chip with baton passing the priority baton. And they started getting these random trips on their channels, and it took about 10 months to work around that. That was just a 286, everybody understood, and yet it was used in a new type of configuration, if you will, and suddenly these failures started coming up.

CHAIR APOSTOLAKIS: It seems to me another major -- oh, you're continuing the limitations of operating experience? Another limitation, which we see all over the place, is that a lot of these events that threaten you are rare. They are very low probability events, so they may not appear in the operating experience, because we don't have a very long record.

MR. WATERMAN: Yes.

MR. WOOD: You have -- specifically, in the nuclear application, you have rare events in the plant coupled with a rare event, which would be the common cause failure, which means you're talking about an extremely rare combination. If you look at say experience with aircraft, where we're talking about control systems, the demand space that's presented to it is much greater, so you can have a great deal more confidence in your experience base, but there are still rare events, conditions the plane would face, which you may not have any experience on that coupled with a failure. So it's difficult to draw understanding from the experience base, but what you can draw from the experience base is if you see something, you had better make sure you've taken care of it. Whether you take care of it through diversity, or you take care of it through design measures, that's a different issue, but it can inform your decision.

CHAIR APOSTOLAKIS: So I would adopt this to the limitations.

MR. WATERMAN: The industry has been involved in looking at operating experience, and done some pretty extensive work, produced pretty long reports. I haven't had a chance to read the whole report yet. But what I did get out of the report was this is a plot of comparison of 1E system common defects identified as a percent of total 1E defects identified. And I took the total count, and I divided each one of these categories of failures by a total count to come up with percents over here on this axis here, and these are the various categories that were identified. And then for each of these categories, I just did a quick assessment of what is inadequate hardware design? What would that be representative of? And I sort of color-coded it according to our little diversity attribute wheel over here.

And as I went through each one of these, color-coding it, and some have two colors and stuff, and I'm not really sure that all of the -- I've identified all of the various attributes that were affected in these failures. But what I did find was that I seemed to have a whole rainbow of different types of failures here that pretty much correspond to all of the categories here, which tells me that from a conservative standpoint, if we're going to be looking at potential common cause failures, which is what we ought to be addressing, that we probably ought to consider all of the attributes right here as things that might be necessary in a diversity strategy to address potential common cause failures. Now, there haven't been a lot of common cause failures in the nuclear industry.

CHAIR APOSTOLAKIS: All these were single failures, or common cause failures?

MR. WATERMAN: No, not common cause.

CHAIR APOSTOLAKIS: Common defects.

MR. WATERMAN: These were common defects that were found, some of which were potential common cause failure mechanisms.

CHAIR APOSTOLAKIS: Okay.

MR. WATERMAN: Potential, I'm saying potential.

CHAIR APOSTOLAKIS: Yes. Now, if you look at the -

MEMBER BROWN: Is that the EPRI document you're talking about, you pulled this stuff out of?

MR. WATERMAN: Yes. Something like that. I was supposed to mention -

CHAIR APOSTOLAKIS: What do you mean, something like that?

MR. WATERMAN: I'm not supposed to. You could say anything you want about -

MEMBER BROWN: I could say it? Okay. I just said it.

MR. WATERMAN: Yes, it is.

CHAIR APOSTOLAKIS: It's a phantom

report? What? I think I have it.

MEMBER BROWN: It was supposed to be -- they were supposed to talk about it at this meeting, but there were some reasons -- the Staff hadn't finished the review, and so they asked it to be deferred to another one.

CHAIR APOSTOLAKIS: But we all know it exists.

MR. WATERMAN: They put a lot of work into that report.

CHAIR APOSTOLAKIS: Okay. Now, let's go to what you have there as operator error. So you have two colors, and what you're saying, the yellow corresponds to function.

MR. WATERMAN: It could be function on operator error, it could be human life cycle.

CHAIR APOSTOLAKIS: Can you explain a little bit what that means, I mean, operator error refers to function.

MR. WATERMAN: Yes, I can.

CHAIR APOSTOLAKIS: Okay.

MR. WATERMAN: If the operator misinterprets a function, or if the function is incorrectly specified that would lead an operator to have some kind of an erroneous response to a condition. It might be the operator took every action correctly, but the function itself just was incorrect.

CHAIR APOSTOLAKIS: So I'm trying to -

MR. WATERMAN: Now, mind you, this is like a five-minute assessment.

CHAIR APOSTOLAKIS: Where is the -- so the software performs the wrong function?

MR. WATERMAN: Perhaps the function itself was -

CHAIR APOSTOLAKIS: Can someone explain it, from the non-existing report?

(Laughter.)

CHAIR APOSTOLAKIS: Okay. You don't exist. Come up.

MR. GEDDES: My name is Bruce Geddes. I'm the Principal Investigator for the report in question. I'm here representing EPRI today.

CHAIR APOSTOLAKIS: Okay.

MR. GEDDES: Could you restate the question, please?

CHAIR APOSTOLAKIS: Well, if you look at this fourth from the right column, it says, "Operator Error." That's Operator Error.

MR. GEDDES: Right.

CHAIR APOSTOLAKIS: And then Michael is saying there is a yellow connection to function, and there is - what color is the other one?

MR. WATERMAN: Perhaps it was the function that misled you.

CHAIR APOSTOLAKIS: And then the other one goes to life cycle. I'm trying to understand what all that means. What kind of an operator error is related to function, and where is the software in there? The software is doing the wrong function because somebody made a mistake?

MR. GEDDES: No, we didn't see anything like that. These were cases where an operator either didn't follow procedure correctly, or the procedure itself was inadequate, and there was an operator error that led to the event.

CHAIR APOSTOLAKIS: Okay.

MR. GEDDES: Okay?

CHAIR APOSTOLAKIS: And where is the digital I&C in there?

MR. GEDDES: He was interacting with a digital system. That's all that means. In other words, it was an event report that involved a digital system, but the cause of the event was an operator error, not a software problem. In some cases, we did see where, for example, an equipment state was not understood by the operator because the indications and alarms were ineffective or could have been more effective, but the primary cause, the root cause of the event itself was reported by the licensee either in an LAR, or an INPO OE report as an operator error. And in most cases, it's pretty black and white. The reports are very self-evident, so you can read the report. If you understand how confirms operate and conduct of operations, and how plants are put together, it's pretty straightforward.

CHAIR APOSTOLAKIS: But why then would this qualify as a common defect?

MEMBER BROWN: It wasn't.

MR. GEDDES: No, these are all common defects.

CHAIR APOSTOLAKIS: They are?

MEMBER BROWN: There was only one.

CHAIR APOSTOLAKIS: But it's not even a defect, it's the operator that -- I don't understand.

MR. GEDDES: Okay. Well, first -- this is the first time we've seen this, so we need to have a little context. Mike, I need to know, if you can help me, are these just the common defect events, or all 49 1E events?

MR. WATERMAN: These were the one events out of your first plot in the figure.

MR. GEDDES: Okay. That was all 49 events. Half of them involved a common defect, so this includes single failures, and failures due to common defects.

MR. WATERMAN: I think there's only 27 events represented here.

MR. GEDDES: Okay. Then it's just -

(Off the record comments.)

CHAIR APOSTOLAKIS: We have some help.

MR. TOROK: This is Ray Torok from EPRI. And I'm taking here, in all fairness to Mike, we really should find the time to sit down with Mike and Bruce in the same room and talk about what these individual events are, because we're going to stay confused about it until then. Mike took a shot at it here, but it needs some kind of discussion with our guys, as well, I think.

MR. WOOD: Well, if I could suggest, I don't think Mike is saying that the defect is the result of some defect or flaw in the function. I think what he's saying is that functional diversity could be a means of responding to that defect.

CHAIR APOSTOLAKIS: That's where I get

lost. The digital system is correct, and the operator made a mistake. The full system responded correctly. It's just that it was the wrong instruction. So why is it even here? On the other hand, talking about the hypothetical report that does not exist, so I appreciate -- we will not take your comments into advisement, because you don't exist.

(Laughter.)

MR. GEDDES: Well, we might as well sit down.

CHAIR APOSTOLAKIS: Thank you very much.

MR. GEDDES: Okay.

CHAIR APOSTOLAKIS: Anyway, this is something that I -

MR. WATERMAN: The reason I looked at this, is I just asked myself a question, do we have attributes here that aren't addressed by experience? Do we have attributes over here that we've never seen any failures in a particular attribute? So I went through here and did a rough, quick guess about well, what could have been the causes, colored it up so I could compare colors. I'm kind of a visual-type person like that, and I find that yes, I could probably find some color somewhere in here for every one of these attributes. Okay? That's all I was doing, wasn't doing some quantitative analysis. I just needed a visual representation. That's why I do the circles.

CHAIR APOSTOLAKIS: The intent is good, but after you interact with the authors, next time around we'll probably question the actual connections.

MR. WATERMAN: We can re-tinge, but I suspect that every one of those attributes is represented in some kind of a defect that's been found.

CHAIR APOSTOLAKIS: Okay.

MR. WATERMAN: What are the sources of data that we looked at? In aerospace -- Bruce?

MR. GEDDES: I'm sorry.

CHAIR APOSTOLAKIS: Yes.

MR. GEDDES: I have one more comment. Bruce Geddes, again. We're encouraged that you've looked at the report, and -

MR. WATERMAN: Only glanced.

MR. GEDDES: Well, I appreciate that. We spent some of our time looking at diversity attributes, but we didn't go down that path in the published report, but we're gratified and encouraged that you've picked up the report and are using it.

We appreciate that.

MR. WATERMAN: And I really want to get what I can out of that report to improve my -

CHAIR APOSTOLAKIS: Is that an unusual occurrence?

MR. WOOD: It's a notable occurrence.

CHAIR APOSTOLAKIS: It's a notable -- you are really supporting Michael there.

MR. WATERMAN: In the aerospace industry, Oakridge looked at two systems. They looked at space shuttle primary avionics software system, and they looked at the international space stations command and data handling system. In avionics or aviation, we looked at four airplane models. We also looked at the FAA regulations and how they were instanciated in those models. I think that's probably correct, isn't it, Richard? We looked at three air bus versions, the A320, A340, and the A380, and we look at the 777.

CHAIR APOSTOLAKIS: What is FCS?

MR. WATERMAN: It's a Flight Control System.

CHAIR APOSTOLAKIS: Oh.

MR. WATERMAN: Thank you. In the chemical process industry, apparently, as Richard, I'm sure, will back me up on this, most of the chemical companies are very reluctant to divulge their control system approach, their design, and so Oakridge was essentially relegated to looking at the Center for Chemical Process Safety Guidelines, and out of those guidelines identifying how all of that fit into various diversity -- would fit into a diversity strategy.

In the rail transportation industry, we looked at the Federal Railroad Administration Guidelines, and we wanted to see how they were instanciated in these types of systems here. The Austrian Federal Railways, Electra Railway Interlocking Control System, the Paris Rail, and the Los Angeles Metro Green Line Vital V or V-Frame.

In the international nuclear power industry, we went out and we wanted to see what various digital plants were doing for their diversity approaches. And all of these are plants that were essentially doing first of a kind applications. There are other plants out there that are also doing applications, but we wanted to take a look at some prototype applications from around the world to see what the rest of the world was doing, so in Darlington Nuclear Generating Station in Canada, you can read in there, Sizewell in the UK, Chooz B in

France, Kashiwazaki-Kariwa in Japan, Temelin and Dukovany in the Czech Republic, Lungmen in the Republic of China, and Olkiluoto, which is still being built in Finland.

MR. WOOD: The rationale for the selection of these particular plants was to look for experience of evolutionary reactors that designs -- that made all very extensive use of digital systems. There are other plants, other Candos in other Westinghouse plants and so forth that have also digital systems, but these were representative of those. So you won't see a full list of all the plants in the world that could be chosen.

MR. WATERMAN: Now, some of the plants we looked at were digital, but they screened out because they weren't applying any kind of diversity to speak of for their digital systems. And since we're looking at not the need for diversity, but how much diversity is enough, we just screened those out. They have no information that we can use.

CHAIR APOSTOLAKIS: Olkiluoto is being built.

MR. WATERMAN: Olkiluoto, but they're far enough along that they know what their design is, and how they're backing it up.

MR. WOOD: And Lungmen is being completed. Those are two that are not completed yet.

MEMBER STETKAR: Did you screen out plants in -- I was just curious about selections, one notable set that I'm kind of familiar with are Germany and Switzerland, but they've established essentially a diversity strategy, but based more on external influences. Did you screen those out because of their sort of unique approach to the whole world of instrument control and safety -

MR. WATERMAN: Well, if you look at -

MEMBER STETKAR: They do have digital systems, but they've established a very distinct method of diversity for perhaps other reasons. And I was curious whether those other reasons were why you didn't -- or did you just not get any information from them?

MR. WOOD: We had information on some of those other plants. They weren't significantly different from the examples that we had.

MEMBER STETKAR: Okay.

MR. WATERMAN: If you look at -

MEMBER STETKAR: As far as just the software.

MR. WATERMAN: If you look at Beznau in

Switzerland, for example, we took a look at Beznau, and Beznau uses a TXS, but their only diversity is functional. It just screens out. It's like tell us what you're really doing.

International positions on common cause failure, we looked at the Institute for Safety Technology, ISTec in Germany. They provided us their concept of what's adequate. And that's Germany, incidentally. The Center for Software Reliability, they were doing a research project called DISPO, and that's out of the UK. And then Oakridge aggregated the IEC standards to come up with the diversity approach that would be representative of those aggregated IEC standards.

MR. WOOD: I'd like to point out that the DISPO project is a British effort that's been ongoing for 10 years looking at software diversity. And they've spent quite a lot of time, and quite a lot of effort on that, so we were able to leverage the knowledge that they've gained. In other cases, obviously, ISTec has been doing a lot of study and investigation, so we tried to capture what others had learned, as well.

CHAIR APOSTOLAKIS: Now, they gave you access to everything they've done?

MR. WOOD: They gave us access, in the case of DISPO, they gave us access to their reports, all of their reports. And we visited, and had discussions with the principal investigators.

CHAIR APOSTOLAKIS: And they are public reports?

MR. WOOD: Not all of them, no. And we didn't report any information that's not public.

MR. WATERMAN: The Western European Nuclear Regulators' Association put out a common position report, if you will, that involves seven countries signing off on a common position about the things to do to make a system resistant to common cause failure also. That's a pretty good document. And it addressed two different areas, architectural diversity, and technology diversity.

So we have all this data. What are the assumptions that we used in using this data? What's the basis for our diversity positions? First, that the diversity positions and designs by other organizations, industries, and companies are based on operating experience and engineering judgment. In other words, there's smart people in the world in other places. Right? And the designs that they're building are based upon their operating experience, and engineering judgment.

Secondly, that the NUREG CR-6303 attributes and criteria can be combined with that operating experience and engineering judgment to develop some sort of an evaluation process. And that evaluation process can be used, if you will, to evaluate other diversity strategies that weren't included in the evaluation process development. And, finally, that the U.S.'s nuclear power plant operating experience can provide us with valuable insights for developing diversity guidance.

So, if you will, essentially what we did is we took this wheel, if you will, it's been called the Waterman Wheel by some in industry, much to my chagrin. This is our diversity attributes and criteria modified to account for the fact that we're trying to make it technology independent. And we correlated all that information into a spreadsheet format, if you will, here, and put all the diversity attributes and design.

CHAIR APOSTOLAKIS: Are you sure you want to get into this now? Let's do that tomorrow.

MR. WATERMAN: This is a fun show. Let me at least get done with this.

(Laughter.)

MR. WATERMAN: We then used -- this really sums up how we did it. And I think it's an important slide to go through, if you will.

CHAIR APOSTOLAKIS: That's why I want to look at it with a fresh mind. Tomorrow morning.

MR. WATERMAN: But if I do it now, you'll get to see it tomorrow, too. Okay. That's fine.

CHAIR APOSTOLAKIS: For heaven sakes. You are so proud of it, Mike.

MEMBER BROWN: Like the Waterman Wheel.

MR. WATERMAN: There is also a Sanchez Pyramid, but we'll get into that tomorrow, too.

MR. SANTOS: Who is Sanchez?

MR. WATERMAN: Or Santos Pyramid.

(Laughter.)

MR. WATERMAN: So we're going to wrap up for today. Is that what I understand?

CHAIR APOSTOLAKIS: I think this is a good place. Now, if you really feel the urge -

MR. WATERMAN: Yes, it really is.

CHAIR APOSTOLAKIS: -- we can go forward. Okay. Thank you very much.

MEMBER BROWN: Can I ask a question?

CHAIR APOSTOLAKIS: Absolutely.

MEMBER BROWN: As you've gone through all the stuff for common cause failures, you've used that as a -- no pun intended, a generic term. Why wouldn't this -- we keep talking about digital systems, why doesn't this same thought process apply in your all minds?

MR. WATERMAN: It absolutely does.

MEMBER BROWN: Okay. So I wanted that answer, because I want people to understand that these method -- the diversity issue is just not a digital I&C issue. This is a instrumentation issue in any type or form.

MR. WATERMAN: Absolutely.

MEMBER BROWN: Whether analog, combinational logic digital, or software-based digital, any one of the three. The FPGA, as I refer to, is combinational logic.

MR. WATERMAN: If you look at some of our common cause failures, who remembers the continuously energized relay off-gassing issue, which the off-gassing resulted in welding the contacts closed. That was all analog. Right?

MEMBER BROWN: How many relays did that happen to?

CHAIR APOSTOLAKIS: That was in Germany?

MR. WATERMAN: That happened in the U.S.

MEMBER BROWN: No, how many relays -

(Simultaneous speech.)

MEMBER BROWN: Just one off-gas and it welded itself shut?

MR. WATERMAN: No, I think there were several. That became a generic issue. Well, at the same time, when they're continuously energized, does it really matter, if they weld slowly and you never challenge them?

MEMBER BROWN: No, my point using the same plant at the same to cause all the systems to lock up. And most of the CCFs you've been talking about today have been a CCF that causes the digital systems to lock up based on common failure, and, therefore, you lose a lot of stuff, like everything.

MR. WOOD: But let's also remember we're not necessarily talking about simultaneous failure. We're talking about concurrent failure in some time frame between when you've tested or observed it, and when you next test it or observe it. The challenge may happen at any time in that -

CHAIR APOSTOLAKIS: Right.

MR. WOOD: The Rosemont pressure transitions were another example of -

MEMBER BROWN: I'm just referring to

we're operating and we have a failure that takes everything out. In other words, the same common failure fails in every division at the same time. And it doesn't take detective action -

MR. WATERMAN: Or a failure causes the inappropriate action.

MEMBER BROWN: That also could be the case, yes.

MR. WATERMAN: High pressure injection actuation -

MEMBER BROWN: I'm not finished.

CHAIR APOSTOLAKIS: There is an outcry. No, go ahead.

MEMBER BROWN: No, I'll make my other observations tomorrow based on sticking with the little Waterman Wheel.

CHAIR APOSTOLAKIS: When we will be able to follow, actually.

MEMBER BROWN: I'll bet you nobody has done all these things.

CHAIR APOSTOLAKIS: So thank you very much. We'll pick it up at 8:30 tomorrow morning.

(Whereupon, the proceedings went off the record at 5:35 p.m.)