Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
551st Meeting

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Friday, April 11, 2008

Work Order No.: NRC-2115 Pages 1-122

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

+ + + + +

551TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARD

(ACRS)

+ + + + +

FRIDAY

APRIL 11, 2008

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11545 Rockville Pike, at 8:30 a.m., Dr. William J. Shack, Chairman, presiding.

COMMITTEE MEMBERS:

WILLIAM J. SHACK, Chairman

MARIO V. BONACA, Vice-Chair

SAID I. ABDEL-KHALIK, Member-at-Large

GEORGE E. APOSTOLAKIS, Member

J. SAM ARMIJO, Member

SANJOY BANERJEE, Member

DENNIS C. BLEY, Member

MICHAEL CORRADINI, Member

OTTO L. MAYNARD, Member

DANA A. POWERS, Member

JOHN D. SIEBER, Member

JOHN W. STETKAR, Member

I-N-D-E-X

BY EPRI:

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

8:30 a.m.

CHAIRMAN SHACK: The meeting will now come to order. This is the second day of the 551st meeting of the Advisory Committee on Reactor Safeguards. During today's meeting, the Committee will consider the following: Digital I&C Interim Staff Guidance and Related Matters; Future ACRS Activities and Report of the Planning and Procedures Subcommittee; Reconciliation of ACRS Comments and Recommendations; and Preparation of ACRS Reports.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Tanny Santos is the designated federal official for the initial portion of the meeting. We have received no written comments or requests of time to make oral statements from members of the public regarding today's session. A transcript of a portion of the meeting is being kept, and it is requested that the speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume so they can be readily heard.

Just passing out a daily announcement that most of you have probably already heard that Bill

Borchard is succeeding Luis Reyes as the EDO, so a new leadership at the NRC.

Our first item this morning will be the interim staff guidance and George will be leading us through that. So, George, turn it over to you.

DR. APOSTOLAKIS: The subject is digital instrumentation and control. We had a subcommittee meeting on March 20th where the staff presented their work and we had detailed discussions.

There are three segments that remain subject of today's meeting. There is interim staff guidance on cyber security, on the licensing process, and new reactor digital I&C PRAs. Naturally, most of the discussion was on the last one, the PRA one, but we also had some comments on the cyber security. The one on the licensing process is more or less straight forward. We just tell the industry what they should be submitting and when. So, for a change, the subcommittee didn't have much to say about that.

We received a memo from the staff after the subcommittee, I don't know if everybody has that, where they list a number of the comments we made and how they plan to handle them. But they also promised to do that today, so you don't necessarily have to look at that memo. But if you want it, we will not

give it to you.

(Laughter.)

DR. APOSTOLAKIS: As I said, the one that was discussed the most was the PRA one and that shouldn't be a surprise to the Committee. By the way, the members present were Jack, John, and Dennis, and we had our consultant there, Myron Hecht, from Los Angeles.

The staff is expecting a letter on the three ISGs. Although today, we'll also have a presentation on the operating experience review and categorization of systems. The industry will also make some comments, but I don't think we should write a letter on these items.

So, without further ado, Mr. Grobe.

MR. GROBE: Thank you very much, George.

My name is Jack Grobe. I'm Associate Director for Engineering and Safety Systems in the Office of Nuclear Reactor Regulation. I first want to compliment the ACRS on the diversity and defense and depth in their digital video display units. It's pretty impressive.

(Laughter.)

MR. GROBE: We'll see if we have a common cause failure during this meeting. I want to

introduce Stu Bailey. You met Belkys Sosa previously. Belkys was an acting person in providing some leadership for the digital activities. We determined that we needed more stability in that area, so we created a new deputy director position in the division of engineering in NRR and Stu Bailey was selected to fill that.

Stu's primary responsibility is to provide leadership for the digital activities and the steering committee interface. So he's here today to answer any questions that you have and I'm going to give a little presentation. So all the tough directions go directly to Stu.

Next slide, please.

I just wanted to summarize a brief background since we haven't been here for a while. The steering committee was formed after a November 2006 commission meeting. At that time, it wasn't clear that we were on a success path for integrating all of the activities of the agency. So the steering committee was formed with five senior executives, one from each of NRR, NRO, research, NCER, and NMSS.

The goal of the steering committee is to provide strategic direction to the activities, the agency, and the digital I&C area to ensure that the

offices are properly integrating to solve the problems and to ensure that we're having effective communication and interaction with our external stakeholders on the issues.

There are seven task working groups that support the activities of the steering committee. Six are led by managers in the various offices. One is led by a senior staff member. Overall, there's more than 50 staff involved in the task working groups. The industry has created a shadow organization to our organization and they've established interfaces and lead individuals so that that facilitates effective communication.

Within the seven TWGs we have defined with the industry 25 specific problems. Not all problems are created equally. Some of them are very complex and detailed. Some of them are simpler.

We're developing interim guidance to resolve each of those problems. To date there's been four interim staff guidance documents issued and those resolve 10 of the 25 problems. You saw three of those last time we met in October. That was the interim staff guide on diversity and defense of depth and the two interim staff guides on highly integrated control rooms, one dealing with communications and the other

dealing with human factors.

The fourth interim staff guide that was issued has not yet been reviewed by the ACRS full committee and that's the one on cyber security. We'll be talking about that today. In addition, there's two interim staff guidance that are in draft, and you'll see those also today, and those resolve an additional five problems. So 15 of 25 problems are either resolved or well on the way to being resolved.

Next slide.

Since last October, which is the last time we met, we've had 18 public meetings of the task working groups, three public steering committee meetings, and we have established the seventh TWG on fuel cycle issue. Fuel cycle was not making sufficient progress to clarify the specific issues that they needed to resolve, so there's now a separate task working group. They've got their problems defined in collaboration with the industry and they're moving forward.

The two draft interim staff guides, as George mentioned that we'll be discussing today, are probabilistic risk assessment. That's primarily focused on new reactors, because new reactors are required to have PRAs in their requirements for the

Part 52 for the combined operating license. The guidance is equally applicable to operating reactors, but the focus of interim staff guide is for new reactors to support the COL process as well as the licensing process.

Mario Gareri is the lead of TWG 1 on cyber and he'll be discussing cyber security. Glenn Kelly was one of the principle authors of the probabilistic risk assessment guidance and he'll be presenting that material. Paul Loeser will be discussing licensing process, and then Mike Waterman will be talking about operating experience and classification of digital systems.

As George mentioned, we'd appreciate a letter. We appreciated the last letter we got after the October meeting. There were two actions in that letter that are not yet resolved.

One is the issue on developing some guidance for how to evaluate operator reactions that are less than 30 minutes. There's been extensive work on that. It's ongoing. It's not yet brought to closure.

And the other one is the spurious actuations question. The digital diversity in defense and depth task working group has that one for action

and they're working on it.

So we look forward to a letter on this issue. I'm not sure if there'll be time, but during the PRA discussion it would be helpful if we got into a little bit of a discussion on whether or not the state of PRA would support relaxation of some of the diversity requirements. It's not on the agenda specifically, but we'd be interested in your insights on that as well.

Next slide.

We've revised our project plan last month to bring more clarity to the long term actions. There's 17 long term actions which will bring the interim guidance to final guidance, and that final guidance will either take the form of a revision of an industry guide, for example, an IEEE standard or something of that nature, an issuance of a NUREG, revision of a regulatory guides, revision of the standard review plan. There's a variety of formal infrastructure documents that will be revised to deal with these issues. Those are all now captured in the project plan.

We've also received four industry reports. There's a variety of industry white papers that they're preparing. Four have been received and are

under review or the review has been completed. As George mentioned, we met with the subcommittee and we've met several times with the subcommittee, and we just met with the Commission I guess it was Monday, things go quickly, and got support from the Commission.

The only action item they were focusing on for the staff was the need for staff training for our operations activities for the new reactors, developing our simulator training facilities. In Chattanooga we have four simulators with analog control rooms and the Commission wanted more detail on our preparation to train our operations staff on the digital control rooms. So we'll be looking at developing some plans for what could be quite large expenditures to update the technical training facility with digital control rooms.

Next slide.

We have a number of remaining interim staff guides. Licensing process you're going to hear about today as licensing process information for operating reactors. The Part 52 process is different than the Part 50 process.

Part 52 includes design acceptance criteria and inspection tests and analysis -- analysis

and acceptance criteria, ITEC. That process is different. It will require some difference guidance, so we'll likely be developing a companion document for new reactors in the licensing process area. And once we finish the new requirements on security, as well as the regulatory guidance for cyber security, we'll be updating the licensing process in both areas to incorporate necessary expectations in the cyber area.

I already talked about manual operator reactions. Fuel cycle facilities is just now getting underway, so that'll be issued later this year. And then I already mentioned the cyber.

As we're using these interim staff guides, we have a number of activities that are underway that are using the interim staff guides. We have a topical report on priority modules that's being reviewed. We have the Oconee full retrofit application that's being reviewed, and we're applying all these interim staff guides for the first time in those areas, as well as some topical reports for new reactors.

As we get feedback on the usefulness and clarity of the guidance, if necessary we'll revise those. If necessary, from industry feedback, we'll revise the guidance. But the real focus, the goal line is to get these into the formal infrastructure.

If they're minor issues, we'll probably not revise the interim guidance. We'll just incorporate those minor issues into the final guidance.

Next slide.

As I mentioned, the goal, nirvana here, is to -- my screen is burping here and you're are not, so thank God for diversity. The goal is to retire the interim staff guide. We're meeting and we have been meeting regularly with the subcommittee and I think this is our third meeting with the full committee. These meeting are not required, but there are required meetings in the standard agency processes for updating standard review plans, reg guides, things of that nature, so we will be coming back to you again in each of these area.

I think that completes my remarks. We'd be glad to answer any questions that you might have. Actually, Stu will answer the questions.

DR. POWERS: I really appreciated this overview you've provided. It's obvious that you've got a very disciplined program moving forward to resolve the 25 issues you've identified on a relatively short term basis.

My question for you is, who's your counterpart within research that's thinking about the

20 year time frame?

MR. GROBE: Interesting question. The steering committee member in research Jennifer Uhle. She's director of division of engineering and research. Rick Croteau, her deputy, is very actively involved. Right now the Office of Research is looking at the long term, and it's not 20 year, it's long term meaning five to ten year time frame, research plan.

That research plan has been in existence for a number of years. We've been working on it. It's time to revisit it because we have much more clarity on our needs. So there's an integrated effort to --

DR. POWERS: That's what motivates the question is it seems like you had a very clear plan for this 2009, 2010 type time frame.

MR. GROBE: Right.

DR. POWERS: And you have seen that there's some challenges you face in the differences between reactors and fuel facilities here that maybe was not appreciated as much --

MR. GROBE: Right.

DR. POWERS: -- in past as it is now. And so I'm wondering if there is any -- no. Who's paying attention to saying, well, this is all going to change

faster than you guys can get out reg guides. And so what does that -- which would be my aiming point at 20 years.

MR. GROBE: Two points, Dana. It's a very interesting issue. If the industry were applying 2000 technology to the new reactors and operating reactors, our job would be a whole lot easier. What's happening is every time something changes, there's some advancement, there's a desire to put that in with no operating experience, little understanding of the sophistication of that new change, I don't think our guidance can keep up with that.

DR. POWERS: It cannot.

MR. GROBE: I used a tricky phrase in the Commission meeting that complexity is an anathema to predictability. If the desire is to have a predictable licensing process, there has to be some stability in how we move forward, and this is, you know, the digital arena is one that has no stability. So that's a very difficult issue.

There is clear direction in the research arena. There's a very detailed, written, long term research plan and research has just initiated in an effort to go back and look at that and make sure it's the right plan. So that's an integrated effort

between research and NRR, NRO, NMSS. I believe NCER has a piece in that also.

The steering committee will be getting updates on that. I think maybe in the six month time frame it might be a good idea for us to have that on the agenda for the subcommittee to look at that the long term plans are. The stickiest wicket is risk analysis.

DR. POWERS: Well, that's one of the brick walls of the future to be able to do that kind of thing.

MR. GROBE: Pardon me?

DR. POWERS: I mean that's clearly one of the real challenges that exists out there.

MR. GROBE: Well, I think enough said.

DR. POWERS: Absolutely.

MS. UHLE: Can I add something? This is Jennifer Uhle from research, and I think as Jack has said that with regard to the rate of change of the technology is hard to keep up from the standpoint of the regulatory process here at the NRC. However, there are other industries that are I would say more able to keep up with the change and, in fact, are motivating that change, and so part of our program in research is to go out and tap that technology

experience that other industries have.

And so we had a program at Pacific Northwest Laboratory to go and identify the right contacts and we are now pursuing aggressively to establish those, and I can point to high speed rail, to FAA, to various --

DR. POWERS: I don't think you want to pointing to FAA right now.

(Laughter.)

DR. POWERS: It may not be a good choice today.

MS. UHLE: Well, we can learn what not to do. And as well as naval reactors and other organizations that, perhaps, have kept up on a more dynamic basis. So, we again, as Jack said, we can come and discuss the research program and what our efforts are later on as we complete the recent update that we're undergoing right now.

DR. APOSTOLAKIS: It would be nice to meet with you before you complete anything. I think with a subcommittee it's a good idea.

DR. POWERS: It's research. They never complete anything.

(Laughter.)

MS. UHLE: The word complete, obviously,

the research plan is a dynamic document. By complete we mean to have vetted it fully within the staff to get the staff views so that what we present to you is just not one person's opinion, but it is a consensus view of the staff. I think that's more an efficient process.

DR. APOSTOLAKIS: I view this type of -- I think it's very similar to what we did with regulatory guide 1.174 where we had very frequent meetings with staff. Nobody knew really where we were going, and, you know, we tried ideas, we talked about them without any expectation that the staff would get something finished. So I think this is part of the problem. This would be a good policy here as well because some ideas and so, oh, come here and -- not to the full committee, I mean the subcommittee.

MS. UHLE: Yes.

DR. APOSTOLAKIS: Talk about it and see what other people are thinking.

DR. POWERS: It seems to me you may be speaking to the research program. I don't think that this program that Jack's outlined for us is where you want to take that kind of approach.

MS. UHLE: Yes.

MR. GROBE: Let me just be clear. There

are specific formal places where we have to come to the ACRS and we will definitely do that. But we get substantial benefit from the insights that you provide, and we've been meeting regularly with the subcommittee and it's our intention to continue that.

DR. APOSTOLAKIS: This ISG, in fact, you didn't have to bring it before us, right?

MR. GROBE: That's right.

DR. APOSTOLAKIS: The ISG, we don't formally review. They brought it because they wanted to.

MR. GROBE: Right.

DR. POWERS: They have certain masochistic --

(Laughter.)

DR. POWERS: The quality of our work benefits the insights provided by this August body.

MR. GROBE: Any other questions?

DR. POWERS: No.

MR. GROBE: Thank you very much.

DR. APOSTOLAKIS: So have you gentlemen prepared also to tell the committee where the points of discuss were at the subcommittee and what you plan to do, or should I make sure that this happens?

MR. BAILEY: The main points of discussion

were related to the task --

DR. APOSTOLAKIS: During your presentation are you going to refer to those?

MR. BAILEY: For the one that I recall the points of discussion, and that was on task working group number three, related to PRAs, yes, we will be discussing that.

DR. APOSTOLAKIS: Well, for the benefit of the full committee, the fundamental point of view I think of the subcommittee, which was not necessarily shared by the staff, although they may be thinking about it, was that at this point we don't have a good understanding of the failure modes of systems that have digital instrumental control imbedded in them, and once you accept that, then a lot of other conclusions come. Can you really assign probabilities, can you do this, can you do that? And we urge the staff to think about it, to focus on identifying potential failure modes, and that was one of the main comments.

And, of course, it's much more relevant to the ISG on the risk part, but, also, on the others, except for the second one which is really administrative. And for cyber security it was the identification of the threats, that there is an

implicit assumption, at least in the NEI document, that the threat is coming from the outside. I don't know if you agree with that.

MR. GARERI: Yes, I'll address that.

DR. APOSTOLAKIS: Okay, great. But that's the thing that was a view that we really don't understand the failure modes yet. So you draw your own conclusions. If you don't understand the failure modes, what is it tat you cannot do. John, you want to say something?

MR. GROBE: No. Thank you.

DR. APOSTOLAKIS: Okay. So I think that was an important theme throughout the subcommittee meetings.

MR. GARERI: Good morning. My name is Mario Gareri with NRO division of engineering. I'm the lead for the cyber security task working group. And, actually, before I get into it, let me address that first.

As far as the scope of this TWG, it was very limited. So what was just referred to is going to be addressed with the new guidance that's being developed by ANSIR and research as far as threat assessments and any kinds of risks dealing with cyber. So you will be getting briefed on that later on, but

it's not part of this task working group, but it being looked at.

DR. APOSTOLAKIS: There are always two issues. One is the scope of the project on which a speaker is making a presentation and the other is what I would call the technical part in which the subcommittee has interest. So it's true that some of the things we said are beyond the scope of individual efforts here, but it's very important I think and that's why we have the subcommittee meetings to express our views regarding the actual technical work of at some point has to have these elements in it.

MR. GARERI: Like I said, let me assure you that it's being addressed in the new guidance that's being developed.

DR. STETKAR: In relation to that, I was kind of reading ahead in your slides, and the only point I wanted to make regarding specifically the cyber security, and it did come up in the subcommittee meeting, was that when I was reading through the guidance I wanted to be sure that there was a sensitivity when you're evaluating the critical assets, that you're also sensitive to things that we think about a lot in the PRA community in terms of support systems so that not only when you're

developing your threat assessment and evaluating your assets, expand that boundary around to include things like ventilation supplies, power supplies, and so forth, that may affect several assets even though they're physically separated in different rooms because a lot of the cyber security and threat assessment process that I saw in the document was focused more on protecting the physical assets by physical barriers and multiple locations and so forth, that that process should be sensitive to these comments.

DR. APOSTOLAKIS: We will have the records of this committee in the sense of we would make all sorts of comments before you even start --

DR. STETKAR: That's my name.

DR. APOSTOLAKIS: Usually we let the guy present one slide.

(Laughter.)

DR. APOSTOLAKIS: So any other comments before he starts? Go ahead.

MR. GARERI: Okay. Next slide.

I'm going to be talking about basically some background. I'm going to talk about the ISG itself and then the path forward.

From the first slide here, let me just

give you a little idea. The TWG only had one problem statement to address and the problem statement itself, like I said it was within scope, deals with two guidance documents regarding cyber security. One of them was the Reg. 1.152 Rev 2 as you can see there. And the other one is an industry guidance that was developed, NEI 04-04 Rev 1.

The reg guide was issued revised in order to capture the cyber security in the design and safety systems in January of 2006 and the NEI 04-04 document was found acceptable by the NRC in December of 2005. So both documents basically came out around the same time frame. The issue here is that one document is specifically, which is the reg guide to address safety systems, and the NEI document was more of a programmatic approach to cyber security.

So if we go to the next slide.

The first bullet is basically about what the task of the task working group was, and, again, it was limited to basically there were concerns from the industry that the two guidance documents were in conflict and what the staff did and the task working group did, we did a gap analysis to actually determine if there were any gaps or any kind of conflicts in the two documents. And in doing that, basically the end

result was that there were actually no conflicts. There were some overlaps and some differences in the two documents, but that's expected because the two documents serve two different purposes.

So, again, the second bullet there says that no inconsistencies were actually found as the industry had concerns and the two documents are actually complimentary to one another.

Next slide.

At that point the task working group could have actually closed out the item because we were finished with the problem statement. There were no conflicts and there were no issues. But the industry committed to revise NEI 04-04 to include and incorporate the criteria regarding safety systems, which was captured in the reg guide.

So at that point the staff agreed that to provide additional clarification to the staff and the industry that that would not be a bad idea to continue with the effort even though, again, it went beyond what we set out to do. So after revising the 04-04 document, what we found is that, because the two documents were so different in structure and the material they were covering, it was kind of difficult to actually do a review using the NEI 04-04 document

when you're doing licensing.

So what we did is we developed a cross correlation table to basically capture the elements and the criteria in the Reg Guide 1.152 into a table that would actually show where that same information can be captured inside 04-04.

DR. STETKAR: Mario, for the benefit of the rest of the committee here who were not at the subcommittee meeting, you mentioned differences in scope between NEI 04-04 and the reg guide. Could you just briefly elaborate on a few examples of those differences?

MR. GARERI: Sure. Well, the differences are the reg guide itself deals more the development life cycle and incorporating cyber security throughout that life cycle when you're developing a system. And, basically, it deals specifically with safety systems. Where the NEI 04-04 looks at the actual setup of cyber security throughout the plant, whether it's firewalls or defensive measures. And, again, the information of 04-04 is security related and, you know, I can't go into the details of that.

But that's the main difference is that one approaches cyber security from a programmatic approach, which is the 04-04. The Reg Guide 1.152

does it from a design perspective and deals specifically with safety systems.

Bill may want to add something.

MR. KEMPER: Yes. This is Bill Kemper.

Just to illustrate maybe if I can. For example, NEI 04-04 would have a requirement that says, a licensee shall within their design an engineering process, a means for securing cyber security is invoked in digital systems. Now, Reg Guide 1.152 goes beyond that and it says, the licensee shall ensure that there are no time bombs, back doors, malicious code, that sort of thing. So you see, it's a lower level of detail.

So in reading 04-04, it's hard to draw from that the this specificity that's needed in a license application for NRR to be able to approve that.

MR. GARERI: I would say, to add to that, basically it looks into the box. The reg guide looks really what's inside the box, where 04-04 looks outside of it.

DR. APOSTOLAKIS: 04-04 deals with broader issues than just safety systems?

MR. GARERI: Yes, it does.

And the revised 04-04 Rev 2 has

incorporated safety system based on the interaction we've had with industry. And that was issued December 31st of last year, and as of this morning I don't believe the industry has any issues with the ISG.

DR. SIEBER: Isn't that just the reverse of the way it should be, though? Shouldn't the industry guides be very specific as opposed to that and the reg guide and the reg guide be more general?

MR. GARERI: In some cases the 04-04 document is very specific, and that's why it's, again, security related information as appendices, which actually gives you the details of what to do to put defensive measures in. But in some other cases, like I said, I had a different goal in mind so it does not address safety system in the design aspects of it. That's the difference in the two documents, but it does have detail.

DR. SIEBER: Yes, I always picture the regulation and the underlying regulatory guidance --

MR. GARERI: Yes.

DR. SIEBER: -- relatively broad in nature in an industry-specific document that the staff accepts would be one way to comply with the overall guidance based on rule --

MR. GARERI: The one thing we didn't --

one thing to keep in mind is when 04-04 came out, there's still no regulations on cyber, so that was really an industry -- and submission of to get something there. And that's on the way. Right, that's going to be my last slide.

Next slide.

The ISG itself basically provides additional clarification to cyber security. Again, it does cover the background of cyber security in general, but it specifically talks to how to use the 04-04 draft 2 revision 2 document when, you know, put in a license middle or dealing with cyber security in a safety system. Again, the ISG includes that table which makes it easier for reviewers and industry to understand exactly how to use the 04-04 document when dealing with safety systems.

And, again, either the reg guide can be used or the NEI document now in conjunction with the table if someone decides to actually use that to address cyber security in safety systems.

Next slide.

This is the last slide and what's happening now is the ISG itself has been rolled over, is being rolled over to the draft guide 5022, which is being developed to address cyber security. This draft

guide is basically going to become a reg guide which will support the rule.

DR. APOSTOLAKIS: Why is it Part 73? Is that for security stuff?

MR. GARERI: Yes. This deals with physical security. As you can see in the sub-bullets there, the long term actions of the actual regulations coming out on cyber security, the regulatory guide to support the rule, and the updating or revision of the standard review plan, chapter 13, will all happen outside of really the TWG effort, even though we're still engaged with ANSIR and research.

DR. APOSTOLAKIS: Can you explain the first sub-bullet, issuance of new rule 54 proposal 55? What does that mean?

MR. GARERI: Right. That's what I was going to get to.

So what happens is that the regulations that are coming out, the proposed rule was under 73.55(m) for cyber security. In taking another look at it, ANSIR has determined with research that it would be best to put it into 73.54 so that it can actually address more than just power reactors.

So, officially, it's the proposed rule of 73.55(m), but it will come out as 73.54. It just

hasn't been made public yet. That's why I have it in brackets.

DR. APOSTOLAKIS: As has been said already, this interim guidance has been issued, December 31st, '07, so any comments that we may want to put in our letter will be addressed really to this effort of developing the regulatory documents in the future?

MR. GARERI: Exactly.

DR. APOSTOLAKIS: And the staff, of course, can take those under advisement or not. But we are not really commenting on the guidance itself because that's final, it's out.

Any questions? All right. Shall we move on?

MR. GARERI: Thank you.

DR. APOSTOLAKIS: I have a question. I'm sorry.

MR. GARERI: I almost made it.

DR. APOSTOLAKIS: There was a semi-question I think on an issue that was raised during the subcommittee and I'm not sure whether the concern is real or not. Concern, it's not a concern. What is a definition of cyber security? Are you defining it some place?

MR. GARERI: I'll have Dave maybe add to this if I'm incorrect in saying it, but I believe the new regulatory guide that's going to be coming out, we're making a point to actually describe it or define it in there, because, again, there is some confusion whether or not it's an outside attack or internal.

DR. APOSTOLAKIS: Can you tell us today or is it --

MR. GARERI: I look at it that cyber security attack would be basically something that would be coming from the outside. But at the same time, if you have a trojan or something, a back door put into the software itself, that would also impact the -- it would give you a vulnerability to a cyber attack. Do you see what I'm saying?

So either way, if the bug or the design itself is faulty, then you're vulnerable to an attack from the outside. I'm not sure if maybe Dave wants to add to that.

DR. RAHN: This is David Rahn. I'm assisting in shepherding the development of the regulatory guide, and the cyber security program has a two-phased approach. There's an overall protection of a facility, and that protection is for potential outside attempts to attack the facility and insiders.

And there is a design basis threat rule which defines what are those potential threats. That's in 73.1. That document defines the overall focus of a cyber security program that a facility needs to have.

Within the facility, there's a bunch of digital assets. Many of them are performing safety related, some are performing emergency preparedness functions, and some are security functions. And there are also systems that protect those systems. Many of those have digital components in them and those components have to be designed, when they put into the system, they can either have their own hardening against any potential threats which could take them down. That means that from the initial development of that digital system there would be --

DR. APOSTOLAKIS: Let me interrupt. You are getting down into detail now. This is how to achieve something.

DR. RAHN: Yes.

DR. APOSTOLAKIS: Is there a high level definition of what cyber security is?

DR. RAHN: Within the regulatory guide the focus is taken that cyber security is a portion of a security function for the whole facility. The object is security for the facility and it's how it affects

the digital assets within that facility.

DR. APOSTOLAKIS: Period?

DR. RAHN: Period.

DR. APOSTOLAKIS: So it doesn't matter whether it's on the outside or inside?

MR. GARERI: Exactly. It doesn't --

DR. APOSTOLAKIS: -- broad definition?

DR. RAHN: Yes, very broad definition.

MS. BANERJEE: George, can I add something, please? This is Maitri Banerjee. The Part 73 rule is supposed to come to us in May, the first week of May time frame.

DR. APOSTOLAKIS: Coming to us means to the full committee?

MS. BANERJEE: Actually, we are going to get a copy of that.

DR. APOSTOLAKIS: The documents are coming?

MS. BANERJEE: The documents are coming and security subcommittee is going to take a look at it and Mario is going to make a decision how much of it we are going to review in May.

VICE-CHAIR BONACA: Supposed to look at the components of the security and then make a determination whether or not the committee should

review them.

DR. MAYNARD: I have got question along that line. Is there a clear definition or division between what's being done for cyber security and the overall security, and not so much that it be separate, but that it actually fit in and not have overlap between the rest of the security requirements for a plant?

MR. GARERI: You're talking about as far as the physical security?

DR. MAYNARD: Right, because like one of John's first comments, he's talking about the support equipment and that's important, but I'm not sure you have to define that in cyber security if that's defined as the rest of your security plan requirements and stuff. I'm wondering, is there overlap, is there work being done to make sure that we don't have incompatible stuff here?

MR. GARERI: I'm not longer with NCER and I haven't been engaged up to the last point. Okay, Bill. He's raising his hand.

MR. KEMPER: Yes, Bill Kemper again. I just attended a meeting with David, as a matter of fact yesterday, to discuss draft language on 73.54. You know, the ink's still wet on this thing so we're

still working on it. But, yes, specifically, 73.54 is titled protection of digital computer and communication systems and networks, so it's intended to provide the specificity, if you will, so that you can differentiate this particular security attribute from the overall physical security plan. All be it, it's part and parcel of the site's physical security plan. I hope that answers your question.

MR. SHUKLA: Dr. Apostolakis?

DR. APOSTOLAKIS: Yes, sir.

MR. SHUKLA: All these ISGs are subject to further revisions and enhancement based upon their use until they are rolled over to a permanent regulatory document. So --

DR. APOSTOLAKIS: Yes, but I mean --

(Simultaneous speakers.)

DR. APOSTOLAKIS: Okay. Any other questions?

MR. GARERI: Thank you.

MR. LOESER: I'm Paul Loeser. I'm one of the digital I&C reviewers.

If you'll go to the next slide, please.

Basically, chapter 7 provides guidance to the staff on how to do a digital review. Things like BTP-14 19. However, digital systems are somewhat

unique within our review process in that we not only look at testing for the final design, but we also need a determination of a high quality design process. This is because digital systems are complex enough that we can never test them enough to say that they are perfect. So we look at this design process and this process takes too long. We can't do an actual independent review, the equivalent of an independent V&V ourselves because this takes too long, and, frankly, we don't have the people.

DR. POWERS: When you say it takes too long and it takes too many people?

MR. LOESER: Typically, the rule of thumb is that it takes as long to do a thorough review of the process as is spent originally in the design.

DR. POWERS: Right.

MR. LOESER: And if they have five or ten people working for two or three years, we don't have five or ten people who can spend two or three years doing this, so we have to look at some lesser degree. What can we do to achieve reasonable assurance that this is really a pretty good system, was done in a pretty good way, and there is a reasonable assurance that it will operate the way it's supposed to and perform the functions it's supposed to.

DR. POWERS: And what I think I'm struggling for is what's a reasonable amount of time to spend on this?

MR. LOESER: Well, we have been spending typically on a overall topical report on a new type of system that we've never seen before --

DR. POWERS: Right.

MR. LOESER: -- tends to be in the neighbor of one to two man years of effort if a licensee is using an approved platform in exactly the same manner it may take half of that, or if they have modified things, it would be more.

One of our final products is a list of documentation that shows what type of thing we would need depending on the complexity of design. I'll be getting to that in my last slide.

DR. POWERS: Okay. So I know what's too much, I know what you're doing now. What's desirable?

MR. LOESER: Well, we thing, obviously, less is desirable. But the question -- that's not really the question we were asked to address here. We are addressing that. As a matter of fact, last night we had a brainstorming session on how could we modify our current process to somehow to do this faster, easier, cheaper in NASA terms.

DR. POWERS: You left out better.

(Laughter.)

MR. LOESER: We want equally good. It wouldn't have to necessarily be better. We think we have a good determination now. We want to make sure that whatever we do we come up with something that's equally good.

DR. POWERS: Or better.

MR. LOESER: That is, it's still -- or better would be nice, but still provides us with a high degree of confidence or reasonable assurance, whatever you wish to say, that this system will function to perform whatever safety functions are specified.

DR. POWERS: I actually have a reason for wanting to do this. So a brand new, unfamiliar system topical report gets submitted, and if you could do that with one man year, then that would take this off the high priority activity list or not?

MR. LOESER: I'm not quite sure what you're --

DR. POWERS: Well, currently, you spend you say on the order of two man years when you get a brand new system in. If you cut that in half, would that make everybody happy and they say, okay, let's --

MR. LOESER: I think it would make them happier.

DR. POWERS: Happier.

(Laughter.)

DR. POWERS: I mean at what point do you no longer have an action plan and things like that going on and you say, well, if you can make it better, that's great, but, otherwise, I'm not going to emphasize it?

MR. LOESER: I would sort of hope that no matter how good our process is we would never be closed to the idea that we could improve it --

DR. POWERS: I'm not asking you that. I'm asking you, when do you quit making it a big priority and coming meeting regularly with George's subcommittee and things like that?

MR. BAILEY: I think we're making progress on that as we speak. We're reviewing --

DR. POWERS: I know you are. I'm asking you when you quit making progress.

MR. LOESER: I don't think I can answer that question on any process when do you decide that it's good enough. I can't tell you that. And I also can't predict at what point management starts telling me it's taking too long or industry starts complaining

that it costs too much. I don't know that because I can't see into their minds.

DR. POWERS: I'm really asking your mind. I'm not asking for other people's. I'm not going to hold you to this. I'm not going to put a gun to your head.

MR. LOESER: I keep telling people I'm inherently lazy. I'd like to make it as easy as possible, but still be able to convince myself that I'm signing my name to a good product. If I could do it in 20 minutes, I would, but I can't. I don't know how.

MR. BAILEY: I don't know that it's much of an answer, but it's our own observations and industry's observations of how the reviews are going. When we see that they are going smoothly all around, then I think we can say this needs less focus. That doesn't mean we won't still be looking for improvements.

But right now we've seen that it is not always smooth. All of the documents that we would be looking for are not always available right up front. We're really trying to fine tune this so that it also fits in with the licensee's life cycle of developing and implementing one of these digital modifications.

DR. SIEBER: I think this is a function of what you want as a result. For example, if you don't spend a lot of time and the system fails, you know, a multitude of ways, you know you haven't done a good job. And right now, since we only have one project in the industry that's full scale with protection and control and all that in there just on it's very beginnings, I think you have to look elsewhere to see where others would have failed, for example, in Europe, to determine what it is you have to do to make sure that you don't repeat those kinds of failures.

MR. LOESER: That is, in fact, happening. Research has a project, you'll be hearing about it later, to look at other industries, not just the European reactors, but also --

DR. SIEBER: Rails, planes.

MR. LOESER: Yes, everything that uses high reliability software, MIL-SPEC.

DR. APOSTOLAKIS: This probably is not a good idea, but anyway.

DR. CORRADINI: I, just for clarification, Jack, you said there is one case in industry where they're doing it for, and I thought you said control and protection?

DR. SIEBER: The Oconee project is pretty

big.

DR. CORRADINI: But that's including reactor protection laws.

MR. LOESER: And the SF.

DR. SIEBER: The other 30 or so projects, in my opinion, have been relatively small.

MR. LOESER: That is correct. This is the biggest one we've had.

DR. APOSTOLAKIS: Just to move it along. We had the presentation here sometime, I don't know, last year where another team within the Agency had a similar problem, namely, during construction of a facility, reactor, they just cannot inspect everything. It takes too much work, too much effort, okay?

MR. LOESER: Yes.

DR. APOSTOLAKIS: So they developed a methodology, it's really a sampling methodology, but a sample is not random. They use some method to risk inform the process, and so on. I'm wondering whether you should look at that and see whether you can get any help from it.

MR. LOESER: Well, we actually something like that. What we do is we do a reasonably thorough investigation on the process they use, and then we

sample the design outputs in our threat audit to see that the process worked correctly and that the --

DR. APOSTOLAKIS: All I'm saying is that you may find the method there of approach that they use helpful. That's all. I'm not saying you are not doing anything.

MR. HILAND: This is Pat Hiland. I'm the director of engineering in the Office of NRR, and let me just try to add some clarification. You're correct. The current application that we have in from Duke on the Oconee project is significantly larger than any that we've seen before.

We've gone back and looked at the way we've done business before and it's not reasonable to expect us to review the Oconee application to that level. And what we've mapped out is that we're trying to define what is a licensing review, what would be an onsite review of the factory or the onsite test information, and then, finally, what would be an inspection activity. Inspection activity will likely be by the regional inspectors after the amendment is approved.

We have an example in the steam generator replacements. You know those amendment requests to

replace steam generators, I've never done one, but I believe they're approved far in advance of the actual work on site, and those who have been at a site when a generator replacement is ongoing, that's a lot of work and we have a defined inspection program that's about 850 hours. So it's a sample inspection. You can't be there all the time to do that. That's what we're doing in the Oconee place.

We have given an initial estimate of how much effort and how long that effort's going to take. We're talking with the licensee, and they gave us what their desires were, and we're different. We're off by about four or five months today, so we have to go back to see if we can improve that schedule by adding more resources if that's the correct approach, or the licensee moving up some of their activities as the factory accepts its tests.

You know, currently, they're scheduled to get the results in January of '09. Will that support our review to meet their schedule? Maybe, maybe not. Don't know. So I'm trying to answer the question in broad terms.

DR. APOSTOLAKIS: The question, I'm not doubting that you have a plan and inspection and so on. I'm not saying that. All I'm saying is there's

another group within the Agency that has a similar problem. They appear to have developed a methodology for selecting the sample in a reasonable way, and all I'm saying is look at it. If you find something that is helpful to you, use it. I never doubted that you can had an approach already.

I don't remember who was doing that, but we wrote a letter. So through the letter we can --

MR. HILAND: I'll work with Girija and find out. We'll get that.

DR. APOSTOLAKIS: Yes, so it would be very easy.

MR. LOESER: So much for the easy presentation.

(Laughter.)

DR. APOSTOLAKIS: We are behind schedule.

MR. LOESER: Anyway, what we basically do is we look at what the licensee or the vendor plans to do and how this will be done. This is by reviewing the plans and procedures. Was it actually done? And this is at the vendor audit. And then what were the results? And this is looking at the design outputs and the final test procedure.

This is considerable amount of documentation and the industry decided that this

amount of documentation not be presented to the staff and put on the docket; in particular, they were worried that once it's on the docket, any changes they make to their configuration management plan would need to be reviewed. We've reassured them that this is not the case. It would be done on 50.59. They would only be re-reviewed if the change was significant enough to change the determination that we had made that it was adequate.

TWG 6 actually had four problem statements, four issues. One is the level of detail necessary in the review of the licensing actions. Two is the applicability of this guidance for operating reactors. Three was the clear licensing protocols for the review. And four was clear guidance on cyber security issues for I&C. The fourth one we really didn't look at. This is left for the cyber group.

In order to do this we needed to deliver a specific clarification on what documents needed to be delivered to the staff, at what phase in the review process it was needed, which of these documents needed to be on the docket and which would be sent off the docket, and which documents don't need to be docketed or sent to the staff at all but only available onsite during the site visit.

We considered the inputs and we basically provided such a list. We're still working on refining this list. This list right now encompasses the most complex possible amendment, so licensees or the staff would delete from the list rather than trying to add things to id.

This does not modify or supercede existing regulations, with one exception. That is the site activities of maintenance operation and training would be left to the region to review. We don't consider that a licensing issue, so that would be --

DR. APOSTOLAKIS: Can an ISG change the regulation?

MR. LOESER: No.

DR. APOSTOLAKIS: No. It's just guidance?

MR. LOESER: Yes.

DR. APOSTOLAKIS: You cannot introduce new requirements, can you?

DR. SIEBER: You can.

MR. LOESER: You're right. It changes the guidance. It changes no regulation.

DR. APOSTOLAKIS: You cannot impose requirements through an ISG?

MR. LOESER: That's correct.

DR. APOSTOLAKIS: It's a softer version of

a regulatory guide. Is that true?

MR. LOESER: Well, we're hoping to turn it into a regulatory guide eventually.

DR. BLEY: Less of a review process than a regulatory guide, is that right, the review and approval process?

DR. APOSTOLAKIS: Exactly.

MR. BAILEY: Well, and you can make a less significant change during. You cannot deviate --

DR. BLEY: More flexible.

MR. LOESER: I mean we're doing things like considering revising the standard review plan to account for some of these. We're writing a new inspection procedure for the regions to use when they're looking at the portion that is now being assigned. Things of that nature. But none of this goes to changing regulation or legal requirements at all. All those are still in place.

DR. APOSTOLAKIS: Very good.

MR. LOESER: So we have provided the ISG, which besides the explanation, also has a table 1 that shows all the documents that need to be reviewed and shows at what time during the review process or the design process they need to be reviewed. We also have a second set of tables that show for reviews of lesser

complexity. That is, if they're using a platform that has already been reviewed, we only then would have to look at plant specific documentation. Or if the platform has been modified at little but not totally, we'd only need to look at the changes and only to the degree necessary to realize that this doesn't change our original concept.

And we're still working on refining these tables unless we have continuous dialogue with the various licensees and the licensee members of the working groups.

DR. APOSTOLAKIS: So this is going to be issued when?

MR. LOESER: Sometime this year. We're getting fairly close. We're hoping to have it in a couple of months. But depending on how much we refine this, I can't guarantee right now.

DR. APOSTOLAKIS: Any questions, comments?

DR. SIEBER: I guess I would reiterate the fact that the Oconee modification is fortuitous because it's big enough to help develop the licensee's and the industry's approach and the staff's approach to this and I would advise or recommend that you take advantage of this opportunity to think about the review you're doing in terms of regulations that you

need to do future review.

MR. LOESER: Yes. We are certainly doing this. We are using Oconee as a potential test case. If we have any new insight, we will try it out there. We're in the process of doing this and, at the moment, we're in the early stages of the review. I believe we have just sent out the acceptance letter for the review. So we don't have enough experience yet to be able to report results from the Oconee review.

DR. SIEBER: Yes. You're probably going to be writing regulations before you're done with that review. On the other hand, as things evolve during the review process to the extent that you can work them into the guidance documents, I think that would be helpful.

MR. BAILEY: That is our plan. Our plan is to refine the staff guidance based on what we find in Oconee.

DR. SIEBER: Okay. Thank you.

DR. APOSTOLAKIS: Okay. Let's move on. Hope this time we go quickly.

CHAIRMAN SHACK: The noncontroversial one.

DR. APOSTOLAKIS: Any questions before we start this time?

(Laughter.)

DR. APOSTOLAKIS: Mr. Kelly is the presenter.

MR. KELLY: Yes.

DR. APOSTOLAKIS: Very good.

MR. KELLY: Good morning. I'm Glenn Kelly. I'm with NRO. I'm a senior reliability and risk analyst.

I'm going to talk to you today about the review of digital I&C systems and the guidance that we're providing to the NRC analysts on how for new reactors we should review the digital I&C system PRAs.

Next slide, please.

The problem statement that we had was that existing guidance doesn't provide sufficient clarity to be used current, and I want to emphasize the word current, methods to properly evaluate digital I&C systems. So we're asked to provide guidance to make it easier for the staff reviewers and part for industry to see what they should be doing for new reactors. We've been asked to consider common-cause failure modeling uncertainty analysis of digital I&C systems.

In looking at this I just wanted to remind the committee that 10 CFR 50.42 requires that new

reactor designs submitted under Part 52 must have PRAs. The PRAs would be design and plant specific and they would include models of digital I&C systems. They only need to show, though, that under Part 52 basically that they meet the safety goals. There's no requirement for much more than that.

Our short term action, then, was to develop this interim guidance. We've done that. And just to bring the committee aware of some of the issues that we were dealing with, the risks assessments, we have a lack of consensus on them, how to model digital I&C systems, and we have issues associated with the robustness of the data for digital I&C systems. And as you've heard before, digital I&C systems are constantly being improved, and, in turn, that makes it hard to get data that says we've had so many years of experience with this particular software, whatever, and it shows X, you know. What happens is that the software changes so fast that, before you know it, you're onto a whole new version, and, therefore, you can't say, well, okay, I've got ten years' experience with this at 20 plants and this what I've learned from them. So we're working with that.

In particular, what we were looking at

here was for new reactors for determining the very basic guidance about our analysts would do these reviews. The guidance that's in the ISG is not about how you make risk-informed decisions involving digital I&C systems. That's going to be addressed in later ISGs, but we're not dealing with that here.

Next slide, please.

The content of the ISG, basically, we've outlined various attributes and risk insights that we're hoping we'll be able to derive out of the information that gets provided by the utility. The risk insights that we feel will be most robust and useful will be those that are at a fairly high level. And one of the reasons for that is that we have very little detail information at this point on digital I&C systems.

As a matter of fact, much of information that would be needed to do a very detailed PRA review might not be available until the PRA that is going to be performed one year prior to fuel up. So at that point they'll actually already have this COL and we'd be potentially then reviewing something at that point to give us information as to whether or not they've met the DAC associated with the digital I&C system.

We've provided guidance to the PRA

reviewers for situations where we're going to have a more limited review, for situations where we're going to have a more detailed review. And, again, part of that has to do with as we go through the various stages of it, a design certification, or a COL application, or even potentially down the road that one year prior to fuel load.

We have very, very different levels of information about what's in a digital I&C system. We've provided an appendix to the ISG that has captured a number of the insights that have come out of the ABWR PRA review and the AP-1000 PRA review. And this is just to give the reviewers some information on the type of things that they might be seeing or could expect to be able to develop or have the applicant develop out of their risk assessment.

Next slide, please.

The subcommittee was kind enough to provide us with a lot of interesting comments during the meeting that we had on the 20th.

DR. APOSTOLAKIS: Did you say kind?

(Laughter.)

MR. KELLY: It was a very interesting time.

DR. APOSTOLAKIS: That's an

understatement.

MR. KELLY: What we've done in taking these comments, and, again, these are some of the key comments that we got from the subcommittee, originally, we had on performing an uncertainty analysis, we discussed specific guidance on types of sensitivity studies that we might expect a licensee to submit to us. It was felt that we were too specific about this. That a licensee might come to believe that this was all they needed to do was to do these particular ones, or that what, in essence, we were doing is creating an NRC approved methodology for this is how you perform uncertainty analysis.

So what we did is we kind of backed it up and made it a higher level guidance saying we would like you to perform sensitivity studies. We think it's important and what we're going to do is we're going to list some of the areas that in the guide today are the most contentious or the most worrisome for us, or that we feel have the greatest uncertainty. and with the expectation that some of these will end up being exercise when they perform their sensitivity studies.

It was also pointed out to us that some of the guidance, as I mentioned earlier, we broke our

guidance into less detailed/more detailed guidance for the review. The subcommittee felt that some of the guidance in the more detailed review really belonged up in the less detailed review, and, in particular, the subcommittee showed strong interest in having more information on performing how the failure modes and effects analysis was performed, and, in particular, the process because on a less detailed review, you would not have enough time to actually go into how they performed the FMEA, but you can look at the process that they used for developing that FMEA. And then if you need to, you can go into the details at some later time. So we've modified that.

We also simplified the guidance on common-cause failure analysis, in part because, as George pointed out, if you don't really know how to model common-cause failure analysis, it's tough to tell them to do it right. So what we did is we basically said, we'd like you to address common-cause failure analysis and tell us basically what are you assumptions, what's the basis for why you did that, and we can look at that see how well it captures the expectations today of how one might express common-cause failure.

Now, one of the things I think is very clear here is the average PRA reviewer is not going to

have lot of knowledge about digital I&C systems, certainly in coming to the working on this TWG. I gained a lot of knowledge about digital I&C systems, and given how we've streamlined our review process, it would be very difficult for every reviewer to come in and get up to the same level of knowledge at least that I've gotten to.

So our expectation is that the PRA reviewers will be very heavily coordinating their review with the digital I&C reviewer because that's where the real expertise and insights into the system itself belie in the review process.

Next slide, please.

So our path forward right now is I'm in the process of revising the ISG to take into account the subcommittee's comments and some other comments that we've gotten, and we're hoping in the next month or so to get the ISG out in final form.

And that finishes my presentation.

DR. APOSTOLAKIS: Good job. I would like to make a few comments on this.

First of all, I think this is a good example of a very useful and productive interactions between the subcommittee and the staff. It was not really contentious. I mean these are hard issues. We

expressed some views, the staff expressed views. I'm not sure. I don't think we really disagreed on anything and I'm very pleased that the staff, as Glenn said, is rewriting the ISG to reflect some of the conclusions, so to speak, of our interaction.

This is a very hard problem. Just to elaborate a little bit. There were I believe 14 steps for the standard review in there to be supplemented by 10 steps, and these include both failure mode evaluation, or the identification of failure modes and probabilities. And this issue of sensitivity studies on the probabilities was something that was discussed a lot.

As Glenn said, first of all, we don't want to give the impression to anybody that these probabilities are somehow meaningful and we want to do sensitivity studies to see what happens because my personal view is they're not meaningful. And I went back to AP-1000 and looked at the data they have there and all you can find is the common-cause failures of a number of digital systems. The rate is $1.2\ 10^{-6}$, but you find no evidence supporting arguments why that is so.

And so if you take that number, then you say, I'll multiply by ten and see what happens, so

100, and, of course, the issue of sensitivity studies itself is not well defined. I mean where do you stop? Do you multiply by 1,000? Do you go all the way until you have a probability of failure rate of 3.

(Laughter.)

DR. CORRADINI: That would be unique.

DR. APOSTOLAKIS: And we sort of objected to that. The staff did not object to our objection. And it all comes down, as I said earlier, to the issue of the question: do we really understand how these things can fail?

I don't think that the state of the art right now is such to say, yes, we have a fairly good understanding. We don't. So the focus really should be on that, and not only on this particular ISG, but also in future activities of the staff, we have to make sure we have a better understanding, we improve our understanding of failure modes. So this was the main subject of discussion and it was very good interaction, very good interaction.

DR. STETKAR: I wanted to ask a question. This is kind of in preparation for the upcoming subcommittee meeting.

There's a lot of discussion of PRA of digital I&C systems, and in kind of a simple sense one

can separate that into the models and the quantification of those models for the hardware, the microprocessors and so forth, and the associated software recognizing that the line between those two may not be as clear as I've defined. But for the purpose of this discussion let me do that.

In your opinion, where are the larger challenges these days, or the largest challenges in the risk assessment of the digital I&C? You mentioned that there isn't very much experience; there isn't very much guidance for this fuzzy thing we call digital I&C. Are you more concerned in the software area or are you more concerned in the modeling of the hardware itself?

MR. KELLY: I believe that today the majority of the concern is in the software. The software has some very, very unique challenges. The type of challenges that you run into is that you timing issues about when something fails. You can create loops. You can have dependencies on things that have happened before or things that may happen in the future.

None of those things that I just mentioned are well handled by our traditional event tree, fault trees that most PRA analysts at nuclear power plants

routinely work with. I spent the last two days going through looking at a draft report on dynamic methods and my own personal opinion about that is that it's not clear to me that the dynamic methods offer a solution to doing a good job in a model. There are just a number of issues associated with dynamic modeling.

So I just think in general at this point it's going to be very difficult to model the effect that a digital I&C system might have. And one of the major things that's associated with it, I mean the reality is that if the systems have -- if the hardware has a reasonable reliability and the if the software has a reasonable reliability, if we're just talking about single failures of components and things like that, that's really not going to be an issue. The way they've designed the systems, it's not going to cause you to go to core damage. It's not going to cause a lot of big problems.

The problem is really going to come with the common-cause failure and how far does the common-cause failure propagate. What's the probability that the frequency with which you actually get these common-cause failures, there are issues with how you even handle something like that because the common-

cause failure itself potentially resides in the software for all time. It's there or it isn't there. And so treating that is a random variable as some issues associated with that.

But even if you can get around that, then generally what you're talking about is you have some causative event, some event that's going to run you through a different loop of your software that you had before, give you different inputs that you had before that's all of a sudden is going to give you this common-cause failure.

Now, assuming that the common-cause failure exists in the software, is the initiating event that could maybe, and this is where my knowledge gets a little fuzzy, is this something that can simultaneously lock up the computer screens and affect the ESF? Exactly how far can this thing go? What kind of failures can I really end up getting? I don't think we really understand those very clearly. So we have a few uncertainties. Let's put it that way.

DR. STETKAR: Thanks. We're running short on time.

MR. KELLY: I'm sorry.

DR. STETKAR: No. Thanks for your insights because part of what we're looking at in the

subcommittee and broader in the committee are the applicability of PRA methods to handle digital I&C problems and I wanted to be sure that when we're looking at that very, very broad problem that we're focusing our attention in the areas where we think we have the greater lack of understanding and lack of knowledge, in other words, that, if indeed, the software is the larger concern and the area where our current experience and methods may be lacking, that we should focus more in that area rather than how one models a chip, or a solder connection on a print circuit board, or wires between CPUs, or things like that.

MR. KELLY: I think it's very important that we very carefully define what it is that we need to understand, determine, and then work towards that goal.

DR. STETKAR: Thanks.

DR. APOSTOLAKIS: I think next week on the 17th there is a subcommittee meeting on one effort to say something about the risk. So a lot of these issues will come up again.

Any other comments, questions? Thank you, Glenn.

The next one is operating experience.

MR. WATERMAN: I'm Mike Waterman. I'm with the Office of Research in the division of engineering, and I'm here today to talk about our review of operational experience and classification of systems. And all of this arose out of a presentation we did I think last year, or something like that, where we were talking about developing diversity strategies that a licensee could use to facilitate more rapid approval of submitted systems, and strategies that could reasonably address most of the common-cause failures that occur.

I believe it was Dr. Apostolakis pointed out that if we're going to develop diversity strategies, we probably ought to know what kind of failures the strategies are to address, and so, therefore, we ought to go out and take a look at what kind of failures have occurred not only in the nuclear industry, but in other industries. We had actually already started a project to do that and the ACRS' recommendation just reinforced that goal.

Additionally, it was recommended that we not only consider what kind of failures had occurred when we're developing diversity strategies, but what kind of systems are these diversity strategies going to fit into. A particular strategy might be great for

a reactor protection system, but it may not be so good for engineered safety features actuation system. So, therefore, we should go out and do an inventory of what kind of systems were out there, what kind of digital systems were going to be implemented, what kind of systems were already in existence, and consider those when we were developing the diversity strategies so we had strategies that would cover a gamut of things.

Next slide, please.

And so that's essentially what we've been doing. And the idea is as we come up with the diversity strategies, which have been developed in draft form by the Oak Ridge National Laboratory under the research, that we can start using that failure criteria to assess how good those strategies are.

Next slide, please.

Some of the things we've discovered in looking around the world are that our concerns with the possibility of software common-cause failure are valid. We've seen lots of failures. We've seen things such as the Aryan problem with the French Aryan thing. Switching system 7 failure telecommunications. There was a software error apparently in the northeast grid blackout that occurred a few years ago.

Ad infinitum.

What we have found, most of the failure data that we've looked at is the failure to report a very high level system reset, software failed. Those kind of failure reports. You know, software, something happened to the system and the plane started losing altitude and we shut off the automatic pilot and turned it back on; everything worked fine. That's typically the level of detail we've been getting.

Now, that's not a very good level of detail for actually developing a diversity strategy where you're considered, you know, should be use timing.

DR. SIEBER: Just shut it off.

MR. WATERMAN: That's scarce detail and causes of failures is making the collection of the data fairly interesting. One of the recommendations that we got out of our last subcommittee meeting is that instead of just looking at safety related systems, we ought to really be looking at systems that, if you will, are at a software integrity level 3 level instead of just at the integrity level 4.

Now, integrity level 4 and 3, when we were writing IEEE 1012 -- well, I was on the working group for IEEE 1012. When we were writing that standard, we

introduced the idea of software integrity level so we could, if you will, parse out how much level of detail you put into a particular verification and validation project.

And integrity level 4 were systems where if the systems failed lots of people died, businesses went out of business, financial institutions lost lots of money, those kind of really serious events, and integrity level 3 systems were maybe only one person dies or there's serious injuries, and business loses money, but they don't go out of business, and things like that, and Dr. Stetkar pointed out that feedwater systems, for example, at a nuclear power plant, are not safety systems. We don't regulate those.

But when they fail, the company loses a lot of money, and, consequently, when they put in a digital feedwater system, they want it to be very high quality. That's an availability issue, not really safety issue because the design basis of the plant can handle that, but it's an availability. If the plant shuts down, the licensee loses lots of money, and so they put a lot of effort into that, so we should be taking a look at those systems, too, because they have good quality. So when they fail, we ought to be considering that failure data.

As far as the root cause analysis, you get into this obsolescence thing. People are putting in digital systems because analog systems are becoming obsolete. Boy, you talk about obsolescence occurring fast. You look at digital systems and see how fast they become obsolescent.

And so for root cause analysis, it's really nice to have somebody around who's familiar with a system to such a point that when a system fails they've got years of experience. They can say, yes, that component fails all the time; that's what causes it. When you've got these new digital systems coming in, where's the base of expertise? It's certainly not year and year of expertise on a 286 because nobody uses an Intel 286 any more.

And so the new systems coming in for doing root cause analysis is a whole new field. As a matter of fact, IEEE had considered doing a standard on root cause analysis through the nuclear power engineering committee just to define here's how you do root cause analysis. And they're not doing that now because it's a very complicated problem.

Next slide.

DR. BLEY: Mike?

MR. WATERMAN: Yes.

DR. BLEY: In going through this data, especially the common-cause failure stuff, have you been able to generalize some categories, functional categories of causes for the common-cause failures that probably would apply across all these different specific systems?

MR. WATERMAN: Well, you could do the high level categorization, three classes of failure, right? You have your failures in design and specification where the main expertise, possibly, wasn't incorporated into coming up with the right specs and the right requirements. And then you've got the translation failures where, no matter how good the spec is, no matter how good the design is, when it comes to implementing it, somebody screwed up, you know, typing a Zero instead of an O, and a variable name for example, or something like that, or not doing verification validation not finding the errors that were incorporated by the coder or something like that.

And then you have that last class, the operation error. You've got a system that's fault free, if you will, but nothing is fool proof because fools are so ingenious, and a CPU card is slid in on hot mode and none of the memory locations have been initialized to plant conditions for example, like the

kind that's a system failure that we saw just recently here.

So those three classes of failures there, you could subdivide it down into failures in deriving a design out of specification, failures in life cycle process if you will where verification validation could have been better, and things like that. But we haven't got enough data right now that we could actually pin it down and say, ah, timing is a big issue, for example, in software or order of execution is a big issue. We're still working on that.

That kind of data would be terrific to have because that's what you need to actually develop a diversity strategy.

DR. BLEY: I think until you can get that kind of functional level ordering, it's --

MR. WATERMAN: But that doesn't mean we can't come up with diversity strategies right now, and we have come up with three different diversity strategies mostly focused around design, a design that incorporates completely different technologies, analog and digital for example. That kind of diversity.

Or I think the second strategy is a design that incorporates digital technology for example, but the technology itself is radically different within

the technology, for example microprocessor versus a field programmable gate array, something like that. And then you've the third strategy where you're using microprocessors for example, but you're using different manufacturers of microprocessors, for example Intel versus AMD, for example risk reduced instruction set computer versus a complex instruction set computer.

DR. SIEBER: That brings up a problem that I think you're going to face in the future. If you look at a power plant that was built to last 40 years, maybe 60 years, these digital systems are not going to have that kind of life time, and the initial failures are going to be this processor failed, that module failed, and you're going to go out to buy it and you aren't going to be able to buy it, and so there's going to be a substitution; and it's going to be done in a hurry and the compatibility and your ability to go through and do flow testing for open loops and all that kind of stuff is the plant's availability is going to pressure you to do that pretty fast, and I think you're going to be in this business a lot more than you think you are because things are going to change that fast.

MR. WATERMAN: And licensees have

attempted to address that by, for example, purchasing enough microprocessors, Intel 286s for example, to last 20 years. The problem with that is that a few years down the road when they go to the website to find out what new problems have come up, they find out Intel no longer supports that processor and they're not longer updating the information. And so you've got all the spare parts, but you really don't know what the performance is years down the road.

And the other thing is is I've seen the case where a designer has said we're going to use the 286 chip, even though faster chips are available, because we know the 286, we've been using it for years, and, therefore, we're going to do it with the 286. And then they implement the 286 and the configuration has never been implemented in before, for example master slave microprocessors.

DR. SIEBER: And the development by the manufacturers has stopped so you're dead in the water with that.

DR. APOSTOLAKIS: Coming back to the issue of categorizations, let's listen, please. Our consultant brought to my attention that there has been some literature where they try to create classes of failures of the processor, for example early response,

late response, no response. I think that kind of categorization would go along with what Dennis said. I guess you agree?

MR. WATERMAN: Absolutely.

DR. APOSTOLAKIS: Okay.

DR. STETKAR: The only thing I'd warn about that, and I think it's a good idea because it's good to have classes to throw things into, just don't make them too rigid initially. I remember in the early days of risk assessment when we started looking at events, the idea was to have a classification scheme first and then force fit everything into the boxes you had defined, and sometimes that doesn't work so well.

DR. APOSTOLAKIS: No, no. But in terms of giving some broad view to the --

DR. STETKAR: Right, right.

DR. APOSTOLAKIS: -- looking for, I think that would be a useful thing.

DR. STETKAR: I guess what I'm saying is don't codify the classification scheme and force all of the experience to fit the --

DR. APOSTOLAKIS: Right. Okay, Mike. What else do you have to say?

MR. WATERMAN: Next slide, please. Isn't

it interesting that it's my fault we're behind schedule.

(Laughter.)

MR. WATERMAN: We're also doing the classification where the path forward is, obviously, we're going to continue together with failure information. The type of failure is really important because you tend to think of failure, oh, just quit operating. You know, it doesn't work as well any more. Sometimes failures have the downstream effect and the failure may be the system continues to operate but it's just a little misleading.

You know, if you think about Three Mile Island was not a failure of a PORV or a feedwater system, it was the operator's interpretation of what to do after it failed, right? The operator was misled, so that's a class of failures right there in the digital system, and it's just like, is the failure subtle enough that the operator is misled and how they are to respond.

As you can see off of our path forward, we're working on the draft strategies now. It's not ready for prime time. I may be working with the contractor a little bit to refine those strategies.

We'll continue to develop our inventory of

new and existing digital systems so we can fit those strategies in and see how well they work, and that's it.

DR. APOSTOLAKIS: Thank you.

MR. BAILEY: That's it. Anything else for the staff?

MR. HILAND: Before we leave the NRC's presentation, could I make one additional comment?

DR. APOSTOLAKIS: Sure.

MR. HILAND: Regarding the dialogue we had on the current licensing review for the Duke submittal, and I'm just going to parrot what I said to the Commission on Monday regarding that submittal is the licensee has chosen not to follow IEEE 1012 and that's an IEEE standard we've endorsed by our regulatory guides. It deals with V&V and so that's a challenge that the staff will have.

In addition, there are several other regulatory guides that endorse IEEE standards involving software QA documentation, and our initial look in our acceptance review, they've taken a lot of exceptions. And so when we were talking about the length of time and the amount of effort, as you know, a licensee doesn't have to follow a regulatory guide. That's only one acceptable method and so we're going

to focus on those activities very early in our review to make sure if there's a red flag that has to up, it'll go up early.

But that's just a head up.

DR. STETKAR: Just I'm curious. Is that because of the particular platform that they're using and where it's coming from, or is it the decision of the licensee? Only because the licensee's personal, only because of the experience from that particular platform in applications in Europe for example.

MR. KEMPER: It seems to be rooted in that. It's basic. It's a particular vendor that we're dealing with which is a European-based vendor.

DR. STETKAR: But I was just curious because there is a lot of experience in Europe --

MR. KEMPER: Right.

DR. STETKAR: -- with that platform.

DR. APOSTOLAKIS: Now, when a licensee uses an item list, you must have reviewed that standard, right?

MR. KEMPER: Yes, typically we endorse those.

DR. APOSTOLAKIS: Because -- that the Agency has not reviewed?

MR. KEMPER: They can, they can. They

certainly can, they can submit that. We would evaluate that. We would evaluate the merits of the plant form itself based on that standard.

For example, we got an application from Wolf Creek that used an aviation standard, DO218 I think it is, to qualify their FEGA application. Well, of course, we don't endorse that. So the first question we asked was how does that comply or comport to Reg Guide 1. -- excuse me, IEEE 74.32 because that's the primary document that we would use to approve a computer-based system. And they did that. And since then we understand what they did and we've moved down the process and things are going along quite well with that application quite frankly.

DR. APOSTOLAKIS: Are you happy with the IEEE standards?

MR. KEMPER: Well, I am.

DR. STETKAR: It's a matter of time and effort.

DR. APOSTOLAKIS: It seems to me that somebody decided that you should never be allowed to use one standard. They always refer you to another one, and the other one refers you to another one, and then you complete the cycle and come back to the original standard.

DR. SIEBER: Endless loop.

DR. APOSTOLAKIS: Endless loop.

MR. KEMPER: This is true.

DR. APOSTOLAKIS: Speaking of failure modes.

(Laughter.)

DR. APOSTOLAKIS: So if you guys are happy, we're happy.

MR. KEMPER: Good to hear, thank you.

DR. APOSTOLAKIS: Okay. So the next is, what, industry comments. Please, go ahead.

MR. CLEFTON: Good morning. I'm Gordon Clefton. I'm with NEI. The subcommittee asked us to bring a presentation of our evaluation research on operating experience that the industry's been doing.

Just as a lead-in to that, I'd like to point out that I'm the lead of the shadow organization that Jack referred to earlier that I got seven TWG industry people that support the NRC. We've got probably 150 to 175 people ranging from operators to senior vice presidents assisting us to make sure that we speak as one voice and have a feeling together of how we can make the industry successful in the implementation of application of digital I&C.

We really looked at the fact that that's

the future of the nuclear industry. We need it for obsolescence, we need it for futures available, and we're doing everything we can to assist in the approval of the packages that we submit.

Need to go on to a couple of slides here today.

Just quick moments to talk about our objectives and, as you can see here, our shadow organization matches what the NRC is doing. We're looking for safety focus applications. We're looking for stable, predictable, timely licensing process and guidance. That's significant right now in the fact that the regulatory risk associated with submitting applications is threatening the submittal of applications.

We've talked about the Duke Oconee package. The industry is watching that one very closely.

We have a need for continuing level of coordination, cooperation between the NRC and the industry, and we're looking for consistency in the processes. We've got a management structure that's in place that identifies the issues. We're moving them to resolution in a disciplined manner. It's been identified earlier. With this we think we can get

realistic guidance.

DR. APOSTOLAKIS: You spoke of the regulatory activities. Surely you're not implying that there are delays that are not justified on the part of the staff? I mean the industry has complained in the past that the staff is not moving quickly enough, and so on. It seems to me that the staff is dealing with very, very hard problems here, so you probably acknowledge that.

MR. CLEFTON: Absolutely.

DR. APOSTOLAKIS: And are you doing anything, in fact, to help this effort? In other words, they have a project or projects on how to risk inform the process. Do you have similar projects and do they deal with defense in depth and diversity issues? Do you have your parallel projects so eventually we will have some intellectual meeting of minds? Or are you just sitting back and waiting to see what the staff will do?

MR. CLEFTON: No. We're absolutely involved in producing projects, looking at applications. Remember, we have digital in the plant. The digital that's coming to the NRC for approval now are those that would not screen out with 5059 process saying that the plant was adequate to make decisions

of implementation.

We've had digital feedwater systems for many years that have been working successfully in the power plant. We've got secondary aspects and such that are out there that are practical in use already.

VICE-CHAIR BONACA: You know, one thing that seems to be important from the presentation is the proper classification characterization of failures so that you build. I mean you're the only one who can build a database.

MR. CLEFTON: That's true.

VICE-CHAIR BONACA: Because you have the experience and it seems to be a critical element to me if we cannot understand the other modes and the effects, there is going to be very little progress. And, again, I mean you can support that?

MR. CLEFTON: Yes. That's our presentation today. We've brought the experts of Ray and Bruce from the industry to speak to it. We'll get to that with analysis in a moment.

VICE-CHAIR BONACA: But it's almost like, how do you implement within an organization procedures for sure that when issues arise they are properly characterized, evaluated so there isn't just a blip there that says something malfunctioned and that's it.

DR. APOSTOLAKIS: Yes.

MR. CLEFTON: That's correct.

MR. TOROK: There's another part to your question though. I think in regard to the industry activities supporting a number of these ISGs. We provided a number of white papers on specific issues. We're continuing to work on more. The one we're talking about today happens to involve operating experience, but there are others in the areas of defense in depth and diversity, in human factors, cyber security, and risks, that's right, in the PRA area. There have been white papers submitted and more in progress.

DR. APOSTOLAKIS: Are we getting those Girija, the committee?

MR. SHUKLA: Yes.

DR. APOSTOLAKIS: Is the committee getting those white papers?

DR. SIEBER: No.

DR. APOSTOLAKIS: Okay.

MR. TOROK: Have you seen, for example, when a common-cause failure applicability?

DR. APOSTOLAKIS: I think I saw it, yes. I see so many documents.

MR. TOROK: So you're seeing some of

these.

DR. APOSTOLAKIS: That's good. But as long as when you speak make it clear that we all have a common problem and we're trying to understand it.

MR. TOROK: Yes, absolutely.

DR. APOSTOLAKIS: Rather than say the regulatory instability and all that stuff.

MR. TOROK: That's a good point.

MR. CLEFTON: We're sharing the concerns that the NRC has and resource capability of handling --

DR. APOSTOLAKIS: Good.

MR. CLEFTON: -- so that they're aware and we are that we can't expect a detailed design review expect regulatory assurance and that's a very difficult decision for a reviewer to make is how much is enough is management pressure for schedule and such, so we're working with the industry to try and help the NRC to put our packages in order that they can be reviewed the best that's possible and that comes from good guidance. It's for the submitter and for the reviewer. But the rules are the same as what the NRC has.

We can go on to the next slide and talk in conclusions.

What we've got is the project plan, which Duke Oconee is RPS, ESPS, the system that's in there right now and the pilot project. We expect this to validate the ISGs that are written and available to us. This is of highest importance to us. We're working on this. It's very significant in the industry applications.

Duke's is pressed by time, as we talked earlier, that they're looking at a 2009 installation into unit 1, then unit 3, then unit 2. So they've got several years of application. As you all know, we've worked outages very carefully for months and months in advance. These have to be approved so we've got a thumbs up, go ahead with it far enough in advance to implement.

That's why the package went in on the 31st of January this year. We're working with the NRC to try and refine differences in schedule where we can progress on both sides effectively. The emphasis, again, is on good strong guidance, stable, predictable, and timely that's realistic, that we can use.

What I'd like to do today is introduce Ray Torok and Bruce Geddes. Bruce is from --

DR. APOSTOLAKIS: Before you do that, I'm

sure you addressed this to some people. You are heading a group, the shadow group?

MR. CLEFTON: Yes, sir. I have seven TWGs that match the NRC's TWGs.

DR. APOSTOLAKIS: And you are representing the industry, not NEI?

MR. CLEFTON: That's correct.

DR. APOSTOLAKIS: You are industry?

MR. CLEFTON: We are industry. Industry are us.

DR. APOSTOLAKIS: Okay. You are working with EPRI and NEI and so on?

MR. CLEFTON: INPO.

DR. APOSTOLAKIS: Yes, and INPO. But your group consists primarily of industry group?

MR. CLEFTON: It's industry and vendors and operators and managers.

DR. APOSTOLAKIS: Okay.

MR. CLEFTON: It's a combined interest.

DR. APOSTOLAKIS: Thank you.

DR. BLEY: I think you folks told us at the subcommittee that your groups have been working very closely --

MR. CLEFTON: Absolutely.

DR. BLEY: -- so that you've actually had

input into these ISGs on the way?

MR. CLEFTON: And that's an ongoing situation. We've got meetings working probably three to five times a month with the different TWGs so that can interface on the assistance of the industry that we've got out there and make sure that the new plant vendors are aware of what we're creating, and, of course, the existing --

DR. BLEY: And you will be commenting formally on the ISGs as well, is that right? Is that something on the schedule today?

MR. CLEFTON: That's not on the schedule.

DR. BLEY: Okay.

DR. APOSTOLAKIS: Who's funding this activity?

MR. CLEFTON: Each of the industry participants are funding it separately. There's no separate cash involved on it. The EPRI has their own financial for some of their topical reports that come out, but the gathering is --

DR. APOSTOLAKIS: Who decides that, in a particular issue you need somebody to spend some time investigating and doing some what we call research, then it's members of this group that are doing this or you are going and say, hey, you have a record of this;

why don't you look at this problem?

MR. CLEFTON: We have the advantage of several of the members of the group are in management positions that they can bring it from their own organizations with no extra costs, so we don't have a budget and a funded aspect associated with it.

DR. APOSTOLAKIS: Okay.

MR. CLEFTON: The spokesmen that typically come to our meetings or participate by teleconference, links in, or webcasts are tip of the iceberg, if you will, of resources that are available in the industry, so we haven't had to fund separate resource as such. We've had volunteers step forward with each of the topics.

DR. APOSTOLAKIS: Now, does EPRI have parallel efforts? I mean do you have a research project some place that is trying to develop something like the staff has research projects in several places?

MR. TOROK: We certainly have a research area in instrumentation and control. Right now several of the activities have been tailored to support the NEI effort specifically.

DR. APOSTOLAKIS: Right, but they are activities where you go to an organization and you

say, here is a problem; we'd like you to tell us what to do about it in two years or a year, or whatever, a typical research project in other words.

MR. TOROK: Well, yes, we have an internal advisory structure that consists of representatives from the various utility members of EPRI, and they have to approve what we're working on.

DR. APOSTOLAKIS: But this is the mechanics of it. Do you actually have such projects?

MR. TOROK: Yes, and the one we're going to talk about is one of those projects. Right?

MR. CLEFTON: This one has come with a collection of available digital related events. It's of significance because we had to go through and evaluate whether they were truly digital events.

DR. APOSTOLAKIS: Good.

MR. CLEFTON: And raise from EPRI versus from Southern Engineering Services and who's supporting NEI and EPRI on this issue, so it's a representation of coming straight from the industry, the people that are out there. This represents, what do we have, a three-hour presentation that's now down to a few a minutes, or 30 minutes.

DR. APOSTOLAKIS: So this --

MR. TOROK: We want to apologize for

putting you farther behind schedule.

(Laughter.)

DR. APOSTOLAKIS: So this is an activity that parallels what Mr. Waterman presented on behalf of the staff?

MR. CLEFTON: It's actually in cooperation.

DR. APOSTOLAKIS: It's brother?

MR. TOROK: Yes. I would call them complimentary, but it's certainly on the same subject.

DR. APOSTOLAKIS: Now why do you always have 10, 20 minutes? I mean would you mind if in one of the subcommittee meetings you actually come and spend and hour or two?

MR. TOROK: We would be happy --

DR. APOSTOLAKIS: I mean you fly from California anyway.

MR. TOROK: We would be happy to come and spend four hours with your subcommittee.

DR. APOSTOLAKIS: Okay. Let's make sure that next we actually review what the industry is doing in more detail. We're not going to write a letter on it, but it's very informative because it would be useful I think for us, especially for a project like this to know the details, not just we are

trying to do the best job in the world. We all try. Some of us succeed.

MR. TOROK: We would certainly appreciate that opportunity. And, in fact, not just for the operating experience, but for the other areas, the human factors, defense in depth, diversity, and so on.

DR. APOSTOLAKIS: I really would like that. I really would like that to spend serious time because usually we reserve 15, 20 minutes at the end and here is the industry to tell us, you know, they are doing something. We should get into it.

CHAIRMAN SHACK: That's it. We'd better move on.

DR. APOSTOLAKIS: Mr. Riley wants to say something.

MR. RILEY: I have something real quick.

DR. APOSTOLAKIS: Yes.

MR. RILEY: This is Jim Riley, director engineering NEI. I just wanted to say we'd be happy to provide or spend some more time with you folks talking about the various things we have ongoing with digital I&C.

One thing that I would like to just add a minute more on because I think it's pretty important. Gordon talked about it. NRC did, too. That we are

using a pilot plant concept on this, that's Oconee. We have a separate task force set up within the NEI to assist Oconee in their review of the NRC RAIs and as the process goes through. The whole purpose of that task force is to assist in any issues that come up, generic issues not plant specific, during the staff's review of the license amendment request. And, also, to identify any new issues that maybe we hadn't recognized when we were doing the ISGs.

The whole point in this is to try out the ISGs and see how they actually work in application and, hopefully, smooth them out so it's a much better product when we're done. And we're just getting started on that, but I think that's very important. And I know we're working, the staff's well aware of this, I think we're all working together on it and I think it should help the final product quite a bit.

DR. APOSTOLAKIS: At some point it would be useful I think for us, for the subcommittee at least, to be briefed on this effort, if you don't mind?

MR. RILEY: Happy to do that, too.

DR. APOSTOLAKIS: Because the actual lessons learned from a practical application is really where the action is or should. Thank you very much.

MR. RILEY: Thank you.

MR. TOROK: Okay. Well, first of all, we'd like to thank you for the opportunity to come back and talk to you about this EPRI project that's ongoing in support of the NEI working group.

I'm Ray Torok. I'm the EPRI project manager on this. Bruce Geddes is our principal investigator supporting the project. That's why we're both here. Bruce will answer the tough questions.

We, also, we presented some of the same information to the ACR subcommittee on March 20th and they were also very kind to us with suggestions about things where we could do a better job or add clarification.

So we've tried to react to some of that, so we do have some new material here. That's sort of a warning. I just didn't want you to stop paying attention, think you were going to see the same thing again.

We're going to briefly describe what we did on the project, what we think the operating experience is trying to tell us, and how we arrived at those conclusions. And, of course, we'll give something on the conclusions and recommendations coming out of it.

Now, this project started for us as a result of an ACRS recommendation to the staff to investigate operating experience and come back and use the lessons learned from it to refine the guidance, the regulatory guidance on defense in depth and diversity. And while we were not the staff, of course, we recognized that that was a good idea and we had the right mechanisms in place to pursue this ourselves, so we started doing it.

The basic idea here was that we would look into various published reports with NRC and INPO. From NRC that means things like licensee event reports, Part 21 notifications, event notifications, and I may be forgetting some of them. From INPO, of course, there are operating experience reports.

Now all of we looked at 322 reports over a period of about 20 years in both 1E and non-1E systems. Now, you notice there it says digital events in quotes.

DR. ARMIJO: Yes. How do you define that?

MR. TOROK: We want to clarify that a little bit because that caused some confusion the last time. Basically, a digital event for the purposes of this is anything that was reported that involved or affected an digital system. Doesn't necessarily have

to be a failure, might be a plant trip, might be discovering some flaw in a digital system, anything that was reported was fair game. Okay.

DR. ARMIJO: Just on that point. Last year there was a failure in a digital feedwater control system at Perry.

MR. TOROK: Yes.

DR. ARMIJO: Which if you keep peeling that onion you get down to maybe a transformer failed or parts of it.

MR. TOROK: Yes.

DR. ARMIJO: Is that in your analysis?

MR. TOROK: Yes. If it was reported -- in that case, yes, that one is. But we also at some point differentiated between events that were really digital system failures or software failures and ones that were caused by other things, and Bruce is going to explain that in a few minutes.

But that's an excellent point because there are a number of definitions you'll find us using that are important to understand here. And that's one of them, what's the difference between what we call a software event and a non-software event.

For this purpose, a software event is where, basically, a design flaw in the software was

involved, that sort of thing. Another way to think of it would be a problem that would affect a digital system and happened because this was a digital system, as opposed to one that would have happened the say way for an analog system like a power supply failure or an incorrect set point that would affect analog or digital the same way. So we tried to break it down that way, and, again, Bruce will show you that.

There are a couple of other things I wanted to mention though. We used some other words. Defect is one of them. What's a defect?

A defect is just a flaw somewhere in the system. For software that typically would mean what would be called a software fault or a bug.

MR. GEDDES: But it would also include procedural issues or human error.

MR. TOROK: So it's fairly broad term the way we're using it here.

The word failure, something actually misbehaved one way or another. Now, it's important to note for software, a software failure, that needs a defect plus a trigger, and I think that was mentioned earlier. A trigger is a set of conditions that causes the software to do the wrong thing. Now, typically, in a software-based system, the kind of thing that

does this is an unanticipated condition, something that wasn't anticipated in the design. So that's what a failure is.

Now, we also talked about common defects. A common defect is one that occurs in multiple redundancies and can affect a redundant system. And we also talked about a common-cause failure. Now, here you need common defects plus concurrent triggers if you're talking about a software failure that can become a common-cause failure. And what you find is that not every common defect can lead to a common-cause failure, and Bruce will explain some of that later. But I wanted to make sure we were all more or less clear on those terms.

Now, at the back of the presentation there's a list of key terms. It goes into more detail. I don't think we need to go through the rest of it now, but it's there for your reference.

Another thing that I wanted to point out here was that we're only looking typically at problem reports here, so we're not talking about positive experience. We tend to focus on what went wrong and there are a number of good reasons to do that. There's a lot more to learn there typically. But we're ignoring a lot of successful operating

experience.

Core protection calculators have been operating for a long time with not very many problems. There are many instances of digital feedwater control systems that have done a wonderful job of doing away with the analog system problems. I know of somewhere during the first startup transient with the new digital feedwater system, it was credited with paying for itself in the first startup just by being able to handle transients that they couldn't handle before, that would have let the plant trip. So there's a lot of those kinds of experiences out of there that we're not talking about.

Now, in one case, one of these digital platforms that people have been talking about here, they have a lot of experience, not in the nuclear industry, but in others, in petrochem. They have over 6,000 units in service for I don't know how many years. They're saying their total service time is in excess of 450 million hours and they've never seen a failure on demand.

Now the problem there is if you're trying to generate statistics for PRA, you don't have a lot to work with. So that's one of the things that makes it so difficult. Now, in this case, one of the first

things that comes in your head is how many demands did they have and how many failures if I'm worrying about statistics? It's hard to get that data especially for systems like these where they're designed to be extremely robust.

They don't fail often, and that's one of the problems with generating a statistical argument, which drives us to consider things in regard to design features that are typically built into these systems which make them robust because they're not robust by accident. They're designed to be that way. So I just wanted to mention that.

Now, for our purposes, since we're primarily trying to support the defense in depth and diversity issue, our focus is on actual common-cause failures that can disable systems or potential common-cause failures that can disable systems. Things at lower levels aren't so important for the purposes of this discussion, although we did look at them. So that's an important point.

We also wanted to capture insights in regard to potential corrective measures that make sense, depending on what we're seeing. One of them is a diversity strategy like Mike talked about. What kinds of diversity would have been helpful here? Or

another way of looking at it is, what kinds of diversity prove to be helpful in these events? And we've seen some of that because it turns out that there's a lot of internal diversity built into the plant systems as it is and it turns out that's a good thing, which should be a surprise. They were designed by smart people.

So in regard to insights, there's diversity. What kind of diversity would have been helpful? And, also, what kinds of design in defensive measures are proven to be helpful here? So we're trying to look at those things to capture insights.

I should also mention that while the focus here has been on the D3, the defense in depth and diversity issue, and common-cause failures, a lot of the insights that we get from these events, especially the non-safety ones, have a lot of value in terms of lessons learned that we can factor back into the utilities and the processes to improve the way they handle these systems.

So we have another project ongoing at EPRI where we're working on that. We're taking selected cases from the same set of information and building it into our training program on digital upgrades. So that's ongoing, too. I just wanted to point that out.

I wanted to very briefly go through what we're seeing here. In looking at these events, we were trying to look at software errors in the broader context of all the causes of potential and actual common-cause failures that have been reported. Now, when we did that, we discovered that software is a relatively minor contributor. Although there have been a number of actual common-cause failures and potential common-cause failures, 49 of our 322 events involved actual or potential common-cause failures. Of those 49, eight involved software. So software has not proven to be a big -- in practice over the last 20 years that software is not proving a major contributor.

The more prevalent causes of the problems have been things like incorrect set points, incorrect system parameters, process issues, really, which, of course, would be equally problematic for analog systems. If the set points are wrong in multiple redundancies of an analog system, you had problems same as if it's in a digital system.

Also, for the non-safety systems, the dominant cause was really hardware issues, and there are a number of important differences between safety and non-safety and Bruce will get into that later.

So while the numbers of events and the numbers of common-cause failures and potential common-cause failures are not large statistically speaking, the operating experience shows no indication that the introduction of software in these systems has been particularly problematic in terms of -- compared to other factors that can degrade reliability and safety.

On the contrary, the operating systems suggest -- it certainly doesn't prove, but it suggests that whatever is being done now in terms of design practices and designed in features in these digital systems, whatever is being done now to ensure that they're very robust in regard to failures and common-cause failures seems to be doing pretty well because, as I said, software has not been a major contributor.

DR. ABDEL-KHALIK: Doesn't that depend on the level of complexity of the software though?

MR. TOROK: That's an excellent point. And, yes, absolutely, and we'll show you a little more on that. That's an excellent point.

Now, with that, I'd like to turn it over to Bruce who's going to show you how we looked at the data and drew conclusions from it.

MR. GEDDES: Thanks Ray.

We actually read, evaluated,

characterized, and built a database for almost 322 reports. You can see down the left hand side of this figure, we used this pyramid construct to separate 1E from non-1E, and we've got another slide that points out the fundamental differences between the two types of systems out there.

On the 1E side we found 49 reports. Breaking that down further, 27 of them reported a common defect. They did not all result, of course, in a common-cause failure. Twenty-two single defects were report, and out of those 27 common defect reports, these are software or non-software defects that are common and multiple redundancies, four of them are related to software.

The other 23 were life cycle management, parameter issues, set point issues, operator error, or procedures, other kinds of defects that can result in a failure at the system level, and what this means is a loss of safety function. We saw zero, actual common-cause failures on demand.

We did see six reports that could have led to a possible system level failure. We are calling those potential CCFs. One of them is software related. The other five are non-software related, in other words, about the same ratio of software to

non-software events.

Of the remaining common defects, we saw ten single failures, in other words triggered into one channel even though the defect was common on multiple channels. We saw six spurious actuations, four subsystem level meaning a trip function or some other function of the system, could have led to a potential CCF, one subsystem level actual CCF.

Next slide.

On the non-1E side, we see bigger numbers, okay, and we have some fundamental differences between like a 1E and non-1E systems that tend, we believe are causing these numbers to be higher. Going, again, down the left hand side of this figure, 273 non-1E events, 77 of which contained a common defect.

Sir?

DR. STETKAR: Probably the largest difference is the fact that there is many, many, many more non-1E applications --

MR. GEDDES: Yes.

DR. STETKAR: -- than digital I&C, so it's not necessarily correct to imply that the failure rate is higher in non-1E because it's fundamentally designed differently. There's just more of them out there, so you're going to see more events. So the

implication is that they may not be as different as you might think.

MR. GEDDES: Well, we do have some backup slides on failure modes and there's been a lot of discussion. We can give you a glimpse. Time permitted, we can show you some failure modes of the non-1E systems and it's important. Those failure modes we don't believe are necessarily translatable directly to the 1E systems.

DR. STETKAR: I just wanted to make sure.

MR. GEDDES: That's a very good point, but we need to make both points together because there are differences.

DR. BLEY: Two things on that. One, have you ever tried to normalize them for the number of systems out there? And, two, are you preparing a report on this information that we might be able to get a look at when it's done?

MR. GEDDES: Absolutely, yes. We have a white paper that's coming out in May and a final EPRI technical report that's later this year.

MR. TOROK: But the answer to the first question was no, we haven't tried to normalize. And to do that is a much more difficult problem. You have to go back and capture the information on all the

other systems and all the --

MR. GEDDES: Absolutely.

MR. TOROK: -- moving toward.

DR. BLEY: That was the hard part in doing mechanical systems for ten years.

MR. TOROK: And we started talking about whether that kind of effort is feasible, but we're not doing anything there right now.

DR. STETKAR: I was going to wait until the end, but you gave me a lead in and we may never get to the end anyway.

You mentioned you have all of the classification and evaluation you had done is based on 332 event reports, let me call it that. You've obviously done some screening of the experience to identify these 322 events. Have you made efforts to go back to the plants and ferret out more details in terms of what actually went on? In the staff's presentation they mentioned some frustration. We used to see throughout the PRA business of finding an event report, the pump failed and the corrective action was replace pump; or software failed and we reset the processor. Did you make to actually go back to those 322 events and flush out more information? That's the first question.

MR. GEDDES: Only in a couple of cases and I can elaborate on that.

DR. STETKAR: Why only in a couple of case?

MR. GEDDES: Well, we found in the reports about half of the 322 reports were licensee event reports, the other half are INPO operating experience reports. And what we've seen over the 20 years is the quality of the reporting has improved and we do see there's three specific things that we can read directly, black and white, in the reports: the cause of the event, the failure mode of the event, and the immediate corrective actions and the corrective actions to prevent recurrence.

Those three pieces of information are in these reports and readily available, and we felt like that was enough for us to do this research. Now, we will go back and do some more detailed review and bring out more information in the final EPRI type of a report on selected events.

DR. STETKAR: My point is that in the risk assessment experience in areas, in some of these very, very difficult areas, talking about common-cause failures now of hardware pieces of equipment, diesel generators, pumps, valves, those types of things, fire

events, human error events, in many, many cases simplistic categorization of both the failure mode, if I'll call it that, and the cause based on very, very high level summaries often does not give you the type of information that you really need to understand what happened.

Now, I'll grant you that the resources, if we're talking about 100,000 events, the resources required to go back and delve into more details would be daunting. But we're talking about 322 events here and a lot of them, because of the history of digital control systems, probably have occurred in the last 10 to 15 years. That's where implant documentation tracking systems may be much better than what is reported in an INPO report or an LER.

The reason I bring this up is that our experience from PRA is sharing the information between both the industry and the regulator at the level of a detailed narrative of what actually happened oftentimes leads to better understanding of the problems, the scope, definitions of failures, and things like that rather than tabulations of numbers of events categorized into different boxes with summary tables of numbers.

MR. TOROK: Well, there's two questions

going on here. Let me first say that a lot of the information came from INPO databases, and, of course, we, EPRI, can't release INPO information on our own to NRC or anybody else. However, we have been talking to INPO about this, what can we give to NRC and so on, and it looks like it will be feasible to just strip selected information out of the reports and then provide a lot more of the details to NRC and everybody else. So we're trying to do that and we will to the extent that we can.

Now, the other question had to do with distribution of what was seen, and that's a hard question. Bruce has to answer.

MR. GEDDES: If I may, I've picked up a lot of discussion points listening to you all today about failure modes. What are the failure modes? How does software fail? And looking at the 20 non-1E software events, and I apologize for having to look sideways, but maybe I could stand up.

CHAIRMAN SHACK: No, no. You have to stay down. You can't stand up and move around.

MR. GEDDES: This is a simple Pareto chart of 20 software events on non-1E systems and these might be the 20 that we go after instead of 322.

The first bin is eight. Eight of those

events were application logic errors. In other words, in any digital you've got an operating system with fundamental core functions like accessing memory and operating certain transfer functions. At the upper end of the architecture is the application logic, the function blocks that make the system do something useful. These are errors in that logic at the application level.

The next bin is buffer overflow. Those could be and probably are operating system issues. They could be an application call that does something inappropriate. The designers of the application didn't quite understand the -- didn't maybe not completely how the operating system works, but these are buffer overflows.

The next category is inadequate indications or alarms. Somebody mentioned operators trying to understand and diagnose an event. In this case there's three of those.

Inadequate human machine interface operating system issues. In some architectures you've got a control layer, in other words, processors that interface directly with the plant, and then a layer above is a human machine interface system with a client serve arrangement, that could go dark and the

control systems keep functioning. A typical feedwater control or electrohydraulic system control might have that architecture, especially with a larger DCS type systems. So that's a case where the HMI failed, but the plant kept operating.

The next bin is faulty deadband function. That's a operating system issue where there's a function block to insert a deadband into a processor control and that function block had an error in it, that the code inside the function block itself was incorrect.

The next one is a faulty communication function, another operating system core function issue. The next to the last one is --

MR. TOROK: Incorrect exit call in firmware.

MR. GEDDES: Incorrect exit call in firmware, that's another operating system issue. An incorrect signal range, that's an application issue.

So you can see a few operating system issues and a few application issues. We think these are interesting. We think these begin to answer the question: how does software fail and how do those failure modes propagate. I would argue I think that application logic errors tend to be isolated within

particular systems, and operating system issues can propagate across the architecture.

Let's go back to where we were on the --

DR. APOSTOLAKIS: We have six minutes.

DR. ARMIJO: This is the interesting part, George.

DR. BLEY: You'll leave us those extra slides?

MR. TOROK: Yes, yes, we will.

MR. GEDDES: We can be here all day. I can go to the airport, find out if the FAA will let me go home or not. I don't know. It's Delta, but they've given us a heads up.

Vulnerability of CCF, we do want to get this point across. Looking at 1E systems, independence and sharing of resources, those are the fundamental differences. The triggers of the events where there's a common defect quite often rely on that these kinds of fundamental design attributes between 1E and non-1E.

In a non-1E system there's quite often a master slave architecture with some kind of a shared resource. It could be a back plane, a network segment, a power, somebody mentioned a feedwater event, the power supply issue, that was the shared

resource.

In some case even those shared resources are redundant, but they might have diode connections, and if those aren't configured properly or tested or maintained properly, or they just fail, that can lead to an event. And that's not necessarily a fault of the digital system, but it does get involved in the event and you don't see those fundamental design attributes.

Independence is maintained in 1E systems by regulation and that's a very, very important point. To try to transfer those non-1E failure modes into 1E systems, you have to transcend. You have to take into account these fundamental design attributes and understand the triggers that lead to events. That's a very key takeaway here.

DR. STETKAR: However, I know in at least one of the new reactor designs that we'll be looking at for licensing in the United States you will see safety-related 1E systems with that type of diode backup sharing of things, so that for that particular type of design this experience might be relevant. That's the only point of not necessarily --

MR. GEDDES: I understand. It's not --

DR. STETKAR: -- separating between 1E and

non-1E.

DR. APOSTOLAKIS: How do you define functional complexity?

MR. GEDDES: This is application level complexity.

DR. APOSTOLAKIS: Is it a quantitative metric?

MR. GEDDES: No, qualitative.

MR. TOROK: What it refers to really is that in the 1E side, the system is typically just looking at some input-censored data --

MR. GEDDES: Bistable functions versus closed loop events control algorithms for feedwater --

MR. TOROK: It's just a trip. It's on and off and that's all it is. Whereas, on the other side, you've got feedback control, closed feedback and so on.

MR. GEDDES: I think it's important for the community to understand that 1E systems aren't always quiescent, dormant, waiting for an event. They're constantly scanning process values, comparing them to a set point and writing in a zero or a 1 on a millisecond level, constantly. They do the same thing over and over whether there's a demand or not. When there is a demand, it writes a 1 instead of a zero to

the reactor trip breakers. That's a very important point.

DR. SIEBER: Let me ask this question. If you show us this chart ten years from now, what will change? For example, in ten years will there be shared resources for 1E systems?

MR. GEDDES: No.

DR. SIEBER: Will you have functional complexity, maybe become high for 1E systems? How is this going to change and what's going to prevent it from changing?

MR. GEDDES: I think the 1E column is a function of regulation, and the non-1E column is a function of plant reliability and availability, and we're learning. You notice formal software quality assurance methods varies under -- but it's improving.

There's nothing like a reactor trip to be a learning opportunity for an I&C engineer. And that's what's happening in the non-1E column. We are improving dramatically on the non-1E side and in ten years I expect event free operation.

DR. SIEBER: Well, a lot of the trips of the plants are pretty events, you know. It's too hot, you trip it. Flux is too high, you trip it, and so forth. As opposed to control systems particularly --

CHAIRMAN SHACK: Jack, we had better let them finish.

DR. SIEBER: -- integrated control systems where it's altogether different.

MR. TOROK: We would be happy to come back later.

DR. APOSTOLAKIS: Yes, I think you would do that. Tell us --

MR. TOROK: There's a point down -- we need the red box here.

MR. GEDDES: I think we've covered that.

MR. TOROK: The 1E systems are much better protected for a bunch of reasons.

DR. APOSTOLAKIS: Good.

MR. TOROK: Now we're there, right. Same thing we said before, software has not been particularly problematic compared to the other contributors to common-cause failure which suggests that the designers and users of these types of equipment have learned how to do pretty well. The 1E and non-1E is still apples and kumquats. It's tough to compare and we tried to explain why, although there are a lot of good lessons learned from both.

Recommendation wise, we agree with Mike. Let's keep looking at things, at information from

whatever sources we have, and let's start thinking about factoring this back into the D3 guidance as suggested earlier.

Now, I was just going to point to this. We've got some other things we saw which were kind of interesting, like there are many cases where, in doing corrective actions for a non-software-related issue, a hardware failure perhaps, added features were put in in software to protect against that from happening again, which is really nice. They're using software for what it's good at. So that was encouraging.

We also saw events that confirmed the effectiveness of certain kinds of diversity, in this case signal diversity and functional diversity. For example, reactor protection systems have lots of different signals. They can all start trips. That's a good thing. We don't want to do away with that.

On the other hand, we saw no events where using platform diversity and redundant trains of a system seemed to be the right thing to fix the problem. Because the problems weren't coming from the platforms, they were coming the application code, set points and requirements, and things like that, not from the base platforms.

I mentioned the last one already. So

we're done.

DR. ARMIJO: This is not my area, so it may be a dumb question. These operating system errors, what do you do to fix them or how do you test these systems in advance to be sure these errors are not there?

MR. TOROK: That's a good question. That's where I mentioned so-called defensive measures here. There's a difference between a good operating system or a good platform and a bad one. Now, 15 years ago, I'd say we didn't know that much about how to figure out which were the good ones and which were the bad ones. We know a lot more about it now.

And I'll give you a couple of easy examples.

MR. GEDDES: Based on non-safety system experience.

DR. ARMIJO: Right.

MR. TOROK: Yes. For example, everyone's heard of the Y2K problem. Well, that happens when operating systems try to track dates and they tangled up over that. So if you're evaluating a system before you put it into a critical application, safety or non-safety, one of the things you want to do is look inside the box and make sure it's not using dates, or

if it is, it's doing it very carefully.

MR. GEDDES: Or turn that feature off.

MR. TOROK: Yes. Now, another example might be in a well-designed system for critical applications. What the operating system does, it's functions don't change at all during a plant transient. It just does the same thing over and over again. It reads data; it ships data someplace else. It can't tell that a transient's going on.

The reason that's important is because you can have all the bugs you want in that operating system and a plant transient can't trigger them. So it eliminates the operating system as a contributor to common-cause failure. So you're looking for those kinds of design features when you evaluate these systems before you before you put them.

And there are many other things. We call them defensive measures. And from our standpoint that's one of my soap boxes I guess. I'd say these systems are reliable, well, in part because they have good development processes behind them, but maybe more importantly because they have good designs with lots of the right kinds of designed-in defensive measures. And so we're working more on methods to credit that.

DR. APOSTOLAKIS: I think future meetings

have to be structured better so we have more time to go into the interesting stuff. But let's start with the subcommittee meetings where you will have a stronger presence.

I'd like to thank you, gentlemen, and also the staff for very informative presentations today, and back to you, Mr. Chairman, on time.

(Laughter.)

MR. BAILEY: Let's take a ten minute break and then we'll try to catch up on some of that time that we've lost.

(Whereupon, the foregoing matter went off the record at 11:07 a.m.)