*Official Transcript of Proceedings*

# NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, March 20, 2008

Work Order No.: NRC-2084 Pages 1-322

**NEAL R. GROSS AND CO., INC.**
**Court Reporters and Transcribers**
**1323 Rhode Island Avenue, N.W.**
**Washington, D.C. 20005**

**(202) 234-4433**

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE MEETING

+ + + + +

THURSDAY

MARCH 20, 2008

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, One White Flint North, Commissioners' Conference Room O-1F16/G16, 11545 Rockville Pike, at 8:30 a.m., Dr. George Apostolakis, Chairman, presiding.

SUBCOMMITTEE MEMBERS:

GEORGE APOSTOLAKIS, Chairman

DENNIS BLEY, Member

JOHN D. SIEBER, Member

JOHN W. STETKAR, Member

ACRS STAFF PRESENT:

CHRISTINA ANTONESCU, Project Manager

GIRIJA SHUKLA, Project Manager

MYRON HECHT, Consultant

TABLE OF CONTENTS

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

8:37 a.m.

CHAIRMAN APOSTOLAKIS: The meeting will now come to order. This is a meeting of the Digital Instrumentation and Control Systems Subcommittee of the Advisory Committee on Reactor Safeguards.

I am George Apostolakis, Chairman of the Subcommittee.

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

Girija Shukla of the ACRS staff is a designated federal official for this meeting.

The purpose of this meeting is to discuss three new digital I&C interim staff guidance for cyber security, licensing process and review of new reactor digital reliance CPRAs; and these are only two. As well as the operational experience review and digital categorization update and the progress associated with the research and digital risk assessment methods.

We will hear presentations from the NRC staff, Nuclear Energy Institute on the industry comments on the ISGs, and Electric Power Research Institute on the industry review of operational experience.

The Subcommittee will gather information, analyze relevant issues and facts and formulate proposed positions and actions as appropriate for deliberation by the full Committee. The rules for participation in today's meeting were announced as part of the notice of this meeting previously published in the *Federal Register*. We have received no written comments or requests for time to make oral statements from members of the public regarding today's meeting.

We will have Mr. Don Chase of ScienTech on a bridge phone line listening to the discussions today. To preclude interruption of the meeting, the phone line will be open one way during the presentations and Committee discussions.

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

We will now proceed with the meeting. And

I call upon Mr. Jack Grobe of the NRC to begin.

MR. GROBE: Thank you, George.

I'll certainly speak with sufficient volume. I don't know if will be sufficient clarity. You may help do that.

My name is Jack Grobe. I'm Associate Director of the Office of Nuclear Regulator Regulations for Engineering and Safety Systems.

I guess a year or more ago Louise asked me to chair -- I apologize.

My name is Jack Grobe. I'm Associate Director of NRR for Engineering and Safety Systems.

Louise about a year ago asked me to share to chair the Digital Instrumentation and Control Steering Committee which integrates five offices' activities; NRR, NRO, Research, NSIR and NMSS in the areas of digital instrumentation and control.

The level of activity of the Digital Instrumentation and Control Steering Committee has been extraordinary over the past year. Because of that, we rotated several young ladies, Belkys Sosa and Patti Silva into leadership positions assisting me in managing the activities of the steering committee. We concluded that wasn't sufficient, so we created a new position. It's the Deputy Director position of the Division of Engineering in NRR strictly for digital instrumentation and control. Stew Bailey was selected for that position. And it's not to exceed one year currently. We're hoping at the end of a year that digitalized C&I activities will be down to a dull roar and should be able to be handled by the normal chain of command. So Stew has a 12 month opportunity to excel in the area of digital instrumentation and control. And he's going to give the presentation this morning.

MR. BAILEY: Good morning. I'm Stewart Bailey. As Jack just said, I'm the recently appointed Deputy Division Director for Digital I&C.

Can we go to the next slide, please?

Just to recap, what we're looking here is the structure of the steering committee and the task working groups.

In early 2007 the steering committee was generated along with the first six task working groups. And these groups were set up to address the areas that have been identified as needing prompt attention to address issues related to digital instrumentation and control.

Membership on the task working groups comes out of the NRC line organizations. And we have a lot of support from industry in addressing the technical issues.

Next slide, please. Thank you.

As Jack said, we continue to work at a very rapid pace to prepare for this rush if I&C. I think we fully expect that the new reactors will be using digital I&C extensively. And we have heard that the existing fleet is looking to do retrofits essentially for the sake of obsolescence. As a result of this, technical issues were identified and task working groups were set up to address these technical issues.

And our activities since 2007, we have had 15 public meetings of the task working groups to address the various technical and process issues.

We've also had three public steering committee meetings.

As we will discuss, we generated one new task working group. This is for the fuel cycle facilities. That information was initially in the licensing task working group but it was determined that the licensing issues that they face and their process was sufficiently different that it would be more efficient to have a separate task working group address those issues.

We issued three interim staff guidance. The first one was cyber security, which we will be discussing.

The second one was probabalistic risk assessments -- oh, I'm sorry. That is in concurrence, probabalistic risk assessments.

And also, we are developing interim staff guidance on the licensing process.

Both of those last two will also be discussed later on.

Next slide, please.

We recently revised --

CHAIRMAN APOSTOLAKIS: Excuse me.

MR. BAILEY: Yes?

CHAIRMAN APOSTOLAKIS: When we say "interim," how long is that supposed to be?

MR. BAILEY: We'll get to that in a little while. Interim staff guidance was a vehicle to allow us to quickly get out our positions on the technical issues. We are looking at updates to the Standard Review Plan or NUREGs or other agency documents within the next couple of years. And at that point we will be retiring the interim staff guidance.

MR. GROBE: One of the concerns that I

have, we were trying to slice the baby up to achieve a number of goals. We needed guidance to the industry rapidly.

The normal public processes for dealing with a regulatory guide or a NUREG or a revision to the Standard Review Plan take at least a year. It requires going out for public comment and meeting with the ACRS, with the CRGR. So it takes quite some time.

We created this interim staff guidance position, and this has been used in a number of different offices for different purposes. In some cases, the agency has depended on interim guidance for an extended period of time; maybe as long as a decade.  I didn't see that that was an appropriate thing to do because we did truncate some of the public engagement in developing these guidelines as well as the various committees.

Recognizing that the interim guidance didn't require a formal ACRS review and approval, we set up a series of subcommittee meetings like we're doing today. But we anticipate as rapidly as possible getting this into the normal infrastructure and eliminating the interim staff guidance.

So depending on the nature of the

guidance, that would either be a revision to the Standard Review Plan issuance or update of a regulatory guide, in some cases revisions to industry standards, IEEE standards. There will be a variety of formal documents that would be issued to finally resolve these issues.

It's important to integrate these because some of them effect the same Standard Review Plan.

So the schedule for accomplishing these goes over the next several years. But the goal is to get them into the formal infrastructure as rapidly as possible.

CHAIRMAN APOSTOLAKIS: But what kinds of reviews do the interim guidance documents get? I mean, you mentioned that one of the reasons that the revisions to the SRP and possibly regulatory guidance, one of the reasons is that you have reviews by the ACRS.

MR. GROBE: Yes.

CHAIRMAN APOSTOLAKIS: And used by other, the GR --

MR. GROBE: CRGR.

CHAIRMAN APOSTOLAKIS: CRGR.

MR. GROBE: Yes.

CHAIRMAN APOSTOLAKIS: Industry comments.

Does the industry have a chance to comment on the interim guidance?

MR. GROBE: Absolutely. I don't believe--

CHAIRMAN APOSTOLAKIS: So what makes this shorter?

MR. GROBE: All of the administrative trappings. You know, for example what we're doing now, when we complete a draft of our interim guide, we may be meeting with the industry in a public meeting several days -- we try to give at least 10 days, but some cases several days after we finish the draft we meet with the industry on that draft.

Most of these guides have gone through at least two drafts where we've discussed them publicly with the industry and obtained comments.

Internally these documents are concurred in by all the TWG members which represent multiple offices. As a minimum NRO, Research and NRR concur on the interim staff guidance before they're issued. And they've incorporated or considered all the industry comments before they're issued.

And we get substantial value out of these dialogues with the Digital Instrumentation and Control Subcommittee of the ACRS.

MEMBER BLEY: Is it written comments from industry or just primarily interaction?

MR. GROBE: Both. Both.

CHAIRMAN APOSTOLAKIS: Very good.

MR. BAILEY: Okay. I think that took some of the things that I was just about to talk to.

CHAIRMAN APOSTOLAKIS: So skip them then.

MR. BAILEY: I will skip them then.

But I did want to give some credit here. In addition to our long term actions we are getting extensive support from the industry. And they have provided us with four reports on topical areas in terms of including minimum inventory of human system interfaces, a document related to computerized procedures and implementation guidance for those procedures, guidance on manual operation actors and common cause failure applicability.

So these are to assist in the NRC's decision making in developing the interim staff guidance and ultimately, the final updates to NRC documentation.

MEMBER SIEBER: Are you getting interaction with the actual instrument manufacturers and suppliers?

MR. GROBE: In some cases, more than we'd prefer. But extensive interaction with the vendors, with the new reactor designers, Mitsubishi and others, extensive interaction with the operating reactor folks.

So typically a public steering committee meeting might have 25 or 30 representatives of the various different industries.

The task working group meetings are at more of a tech staff level and there's extensive participation by a number of people.

The interesting challenge is trying to get an industry position. Because each of these different components of the industry have different needs and perspectives, and many of them are in a competitive nature with each other. So the decisions, like most decisions the agency makes, there are people that are pleased with the decision and people that aren't because it goes contrary to the direction they thought they were going which might have given them a competitive advantage over what they perceived their competitors are doing.

So it's been very difficult to get industry positions. We have many industries that we're dealing with here

MEMBER BLEY: When you said you've tried

to have the operating folks in, is it in the licensee engineering staffs or are you actually getting input and participation from operators, maintenance personnel?

MR. GROBE: Let me phone a friend. Give me some input.

Have we had actual operators or has it been mostly the engineering designers?

CHAIRMAN APOSTOLAKIS: You have to go to a microphone.

MR. ARNDT: You can correct me. It's been mostly the engineering staff, the design staff although in some areas some of the operational staff have participated in areas where they consider that to be a particular interest. For example, in the human factors area.

MR. GROBE: We currently have under review two fairly substantial operating reactor license amendments. Oconee has in house, and we're just starting our review of an extensive application to retrofit the reactor protection system and the engineered safety features actuation system with digital.

Wolf Creek also has an application in house to replace the main steam feed isolation system with a digital upgrade.

So those, we're having extensive interaction with those two organizations which includes interaction not only with the engineering organizations but input on the issues that affect the operators.

MEMBER BLEY: I'm just curious. Were the operating kinds of people invited to participate and have just not shown up, for the most part?

MR. GROBE: Oh, absolutely.

Well, we depend on the industry to send whoever they think is appropriate.

MEMBER BLEY: I understand.

MEMBER SIEBER: So these meetings are noticed in the *Federal Register*.

MR. GROBE: Not in the *Federal Register*. They're public noticed and they're on our public website.

MEMBER SIEBER: Oh, all right.

MR. ARNDT: What we've seen is dependent upon the particular technical issue associated with a particular working group, you get a different mix of people, be it instrument and control system designers, plant system designers, operational people, new plants, operating plants; depending upon the technical issue associated with it. Or, of course, PRA folks.

CHAIRMAN APOSTOLAKIS: They are everywhere.

MEMBER STETKAR: To follow up on Dennis' question, have you had much interaction with the international community? Because, you know, these systems are installed and operating much more extensively overseas than they are in the U.S.

MR. GROBE: Yes. We've had extensive interaction internationally.

MEMBER STETKAR: With operations folks also from plants that have had several years of operating experience with the systems?

MR. GROBE: There's been a variety of interaction. Some of it has been attendance of specific topic focused counterpart meetings. And some of it has been visiting sites. Some of it has been attending professional meetings, international professional meetings. So it's been a variety of interactions, but there's been extensive interaction.

Probably six or eight months ago we provided the ACRS with a compendium of all the interactions that we had engaged in. And in recent months there's been an additional level of interaction.

One of the interactions is part of what's referred as the MDEP program, the multinational design evaluation program where I think it's the AP1000 and the EPR, we're looking at leveraging international engineering activities to be more efficient in the review of those two designs. And that includes digital as well as a variety of other areas.

So there's been extensive international interaction, both here in the United States as well as elsewhere.

About six months ago we hosted a meeting particularly on common cause failure. And we had, I think, seven countries come.

MEMBER SIEBER: Are you making an attempt to have an international consensus of ground rules for various phases?

MR. GROBE: That's part of the MDEP initiative. MDEP has two kind of legs to it, and really Gary Hollahan from New Reactors is a better person to talk about this. But one of the strands of MDEP is to try to get the international standard setting organizations, whether it's mechanical which would be ASME and different organizations in Europe and Japan, as well as other standard setting organizations to try to define a standard for a certain particular attribute and then identify the differences and try to see if a consensus could be developed.

This particularly affects component manufacturers. Because if you're manufacturing large forging, for a U.S. reactor you have to be ASME code, for a French reactor it's a different code, for a Japanese reactor it's a different code. And now that we've become very global in our component manufacturing, it would be much more efficient to have a standard international set of standards.

MEMBER SIEBER: Okay. Well, the codes for pressure vehicles and piping are similar internationally. But for computers, data processing, digital instrument control there are so many branches that you can take, I would think that achieving some kind of consensus would be more difficult.

MR. GROBE: Our goal is to not attempt that. That's part of what's ongoing with MDEP, and it's going to take many years.

MEMBER SIEBER: Well, you need to keep in mind that people may want to buy designs that are outside the United States.

MR. GROBE: Right. And one of the challenges that we're going to have, and we are already having, is whether the designs that are used at operating reactors in the United States in particular meet our standards. And if they don't meet our standards, then the review becomes more complicated.

MEMBER SIEBER: Yes.

MR. GROBE: But the goal of the Digital Instrumentation and Control Steering Committee does not include international standardization of standards. That's a many year project. It's not a short term activity.

MEMBER SIEBER: It's good to start off on the same diving board, so to speak.

MR. GROBE: Right.

MR. ARNDT: Just to amplify that a little bit. As Jack mentioned, that's not the particular goal of this particular activity although the NRC does actively participate in both U.S. and international standard setting bodies in this area. In this area it's primarily IEEE, a little bit ISA in the U.S. And it's the International Electric Congress international Electrotechnical Commission internationally, IEC, which we have representatives on. They have a special section for nuclear I&C.

And we also occasionally participate in EU and OECD and IAEA bodies that don't set standards, but set criteria and try and bring things into a standardization.

But it's a significantly more challenging area, as you pointed out, than mechanical. Because both the structure of the regulations and the specific regulations are fairly significantly different between the various countries.

MEMBER SIEBER: Thank you.

MR. GROBE: It was part of Chairman Diaz' vision to integrate standards internationally. And had we been sufficiently clairvoyant to anticipate the nuclear renaissance, we would have started this about a decade ago and we may have been prepared to have international standards at this point in time for this version of reactors that we're hoping to build over the next several years.

The standards alignment activity that's part of the MDEP I would anticipate could be in place for the next generation of reactors. I don't anticipate it's going to be in place for this generation.

MEMBER SIEBER: I may be wrong, but my

impression is that visual instrumentation is more in use in Europe, for example, than it is in the United States. And perhaps there is an opportunity to take advantage of some of the experience that is in Europe.

MR. GROBE: Yes.

CHAIRMAN APOSTOLAKIS: Let's go on.

MR. BAILEY: Okay. Where to start?

The steering committee is still working at breakneck speed, essentially. There are several ISGs that we will be completing in the near term, an interim staff guidance on the licensing process, one on operator actions. In October we will issue one of fuel cycle facilities. And February of 2009 we will revise the licensing process intern staff guidance to include the issues related with cyber security.

There may be other subsequent revisions to licensing process as these other task working groups finish up the results of those task groups as they effect licensing and the documentation, and the NRC's staff review would be factored in to the licensing process interim staff guidance.

You had asked previously about industry feedback. We are getting industry feedback at many levels, as you had heard. We continue to take it in task working groups and in the ISG development. And also as we use the interim staff guidance and we observe how effective they are, we accept that feedback and we can incorporate and revise the interim staff guidance as appropriate. And certainly there are public comments for when everything is incorporate into the regulatory infrastructure.

Next slide, please.

Again, to reiterate. We plan to retire the interim staff guidance by putting it into the regulatory infrastructure using our standard processes.

We are currently working on a tracking method, and this is to make sure that everything is done to our satisfaction. Because, as we've discussed, some of these actions will likely still be ongoing when we retire the steering committee. So we want to make sure that we have the appropriate tracking mechanisms for that.

MEMBER SIEBER: Do you anticipate the rulemaking may be required?

MR. BAILEY: There is at least one rulemaking that is going to be needed related to cyber security. I don't believe that we have identified any other potential rulemakings at this time.

MR. GROBE: There is one other. When we put the rule in place for the SPDS it uses the word "console" in the rule.

MR. BAILEY: Right.

MR. GROBE: And, of course, all of this is going to be integrated into a digital platform. There won't be a "console."

MEMBER SIEBER: Of some sort. Right.

MR. GROBE: So we need to fix that word in the rule.

MEMBER SIEBER: Thank you.

CHAIRMAN APOSTOLAKIS: Next year?

MR. GROBE: At least. Actually, there's a way to rapidly do that one, but it still takes time.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BAILEY: Well, that completes my talk. If there are no other questions, we will head into the next session on cyber security.

CHAIRMAN APOSTOLAKIS: All right.

MR. GARERI: Good morning. My name is Mario Gareri, Division of Engineering in NRO. And I'm the team lead for the cyber security TWG.

Okay. First slide, this is what I plan to cover. I'm going to have a few slides to cover the background so that it can give a pretty complete picture of what actually occurred before the ISG was issued. Then I'll have a couple of slides on the ISG itself. And one slide on the current status that we're at.

As you can see from the first bullet, the ISG was basically develop to provide clarification on cyber security guidance as it relates specifically to digital I&C safety systems. It was not intended to cover the entire cyber security program as we're trying to develop right now during the rulemaking.

The specific task for the TWG was to address a issue and concern as it relates to possibly inconsistencies and conflicts within two specific documents, which were Regulatory Guide 1.152 Rev 2 and NEI 05-04 Rev 1.

CHAIRMAN APOSTOLAKIS: Can you summarize, at least for me, what kinds of threats we're talking about? What is the issue here?

MR. GARERI: Okay. The issue is not directly at threats or cyber security as a threat assessment. It's we have two guidance documents that the industry found, one was Regulatory Guide 1.152 Rev 2, which has cyber security criteria in it for safety systems. And then there's an industry guidance document that was endorsed by the NRC which addresses cyber security as a problematic approach. And the industry felt that the two documents had inconsistence and conflicts within them.

CHAIRMAN APOSTOLAKIS: Forget about documents.

MR. GARERI: Okay.

CHAIRMAN APOSTOLAKIS: We are trying to protect the I&C from something.

MR. GARERI: Yes.

CHAIRMAN APOSTOLAKIS: What is that something?

MR. GARERI: The --

CHAIRMAN APOSTOLAKIS: Intruding from -- and manipulating it, I mean --

MR. GARERI: Well, there's several aspects of it. If you look at the design aspect, we're trying to prevent possible bugs or back doors being put into the software life cycle while we're developing the software.

And if you look at the programmatic approach, we're trying to prevent attackers from the outside getting into the systems through a cyber attack, the internet.

So there's two parts of it.

CHAIRMAN APOSTOLAKIS: Two parts.

MR. HECHT: Can I follow up on the next question. My name is Myron Hecht. I'm a consultant and we've not met before.

In the terms of a threat assessment, one thinks also about insider threats and you say from the internet. Well, there could be attacks from places other than the internet.

MR. GARERI: Sure.

MR. HECHT: And so one of the things I was looking for in this document was I was looking for a definition of cyber security so that you could have something to go on.

So, first of all, we need a definition of what cyber security is and then we need to probably have a threat assessment done and the vulnerabilities-- well, the vulnerability assessment comes after you've done the threat assessment.

It appears here from my not too in depth review, but it appeared that you were dealing primarily with access control and not with authentication, for example, and not with logging and the other aspects in auditing, which are the other aspects of generally computer security. And I don't know the difference between computer and cyber security.

But I'm just saying that in order to answer those questions about, for example, insiders or the types of authentication needed in addition to coming up with the pretty good guidance on the structured process and access control, which is covered here, that you would have to have that. And it might not be a public threat assessment, it might be classified. I don't know. Maybe such a document does exist.

MR. GARERI: It actually does. There's been a threat assessment, a NUREG that's been developed and it's sought security related information so it's not available to the public.

And those issues that you raise as far as whether it's insider or not insider, that is being addressed by the Office of NSIR through their draft guide that they're developing. And it's also addressed in the NEI 04-04 document. But like I said, the scope of this TWG was very limited. It was not to address cyber security as a whole.

So what you're asking is being addressed, it's just not in this particular document that we developed.

MR. HECHT: Well, if there are threats that are being addressed in other documents, how would they become part of staff guidance?

MR. GARERI: It's going to be covered by the draft guide 5022 that's being developed right now in NSIR and Research.

MR. HECHT: Okay. So that's not the same thing?

MR. GARERI: No. That's not the same thing as this. I'm going to get to that. That's going to be the later slides which we'll talk about.

MR. KEMPER: If I could just jump in here? This is Bill Kemper from NRR.

We are going to develop specific interim staff guidance for cyber security licensing criteria which is, as Mario said, is being produced via a generation of DG 5022. But that information will be put into the interim staff guidance for the licensing guidelines. And Stew showed you a slide on there. That's scheduled for later this year, actually, to complete that.

MR. HECHT: It doesn't have to be clear to me, but is it clear to the staff what the differences are between these two documents and how they fit together?

MR. KEMPER: Yes, yes. My staff and NSIR staff and NRO are all working collaboratively to sort that out.

CHAIRMAN APOSTOLAKIS: Okay.

MR. GARERI: Next slide.

Basically to determine what the possible inconsistences and conflicts may have been, what we did is we developed a gap analysis. And through that gap analysis what we found was actually, as the next bullet indicates, that there were no real inconsistency conflicts because the documents served a different purpose. And basically, they were actually complimentary to one another.

What we did then is the industry basically committed to revising NEI 04-04 Rev 1 to be able to capture some of those gaps and the differences that we found from Regulatory Guide 1.152 so that they could actually cover the same criteria in NEI 04-04 Rev 2 and use that in lieu of the Regulatory Guide itself.

MEMBER BLEY: Given you have those two documents that you're trying to reconcile, how does this new document fit within that framework?

MR. GARERI: The new document being the ISG or the draft guide?

MEMBER BLEY: The draft guidance, the interim guidance document.

MR. GARERI: The ISG that we're working on?

MEMBER BLEY: Yes.

MR. GARERI: The ISG what it does, is it basically gives a background on cyber security as a whole. But then what it does it speaks specifically to these two documents and addresses --

MEMBER BLEY: Marries them together?

MR. GARERI: Right. It provides clarification on how exactly the document is to be used and actually has attachments, which again I'm going to be talking to later on. It has a correlation table attached to it so that if you use NEI 04-04 Rev 2 in lieu of the Regulatory Guide, you can look at this correlation table and it will show, and I have an example in here in the slides, on where the criteria from the Regulatory Guide is found in the NEI document. So it makes it easier for review or to be able to make a determination if it's actually covered in that document. Okay? But I'll get to that. There's a specific example that you'll be able to see how it works out.

Let me see there. We're at the third

bullet, I guess. No, I covered that. Basically the industry revised Rev 1 to be up to capture the criteria within the Regulatory Guide.

And as Bill said, we worked together with the various offices and industry. A lot of public meetings and interaction and comments were, obviously, considered and incorporated when it was possible.

The cross-correlation table itself was developed mainly to be able to map the criteria from the Regulatory Guide to the NEI 04-04 Rev 2 document. Because as I said, initially the two documents served different purposes. So it was very difficult to take the NEI document and try to make a determination just basically on going through that document itself. So the table is really a tool to be able to do a quicker review and a more consistent review by various reviewers.

Training was provided to the staff at the, a DISG workshop along with the other ISGs that were also -- you know, during that training.

And I think that covers the background.

The ISG itself, which is the next slide. As I mentioned earlier, the ISG is basically to clarify the cyber security guidance as it relates specifically to the safety systems. Again, it was not intended to be a cyber security guidance document because, you know, it would have taken a lot more than this effort to do that. And that's being done also in NSIR.

MEMBER BLEY: I want to make sure I'm not missing something.

MR. GARERI: No, go ahead.

MEMBER BLEY: What it sounds to me like is this interim guidance is there to help the staff reviewer who is using the Regulatory Guide look at a submittal that was done in accordance with the NEI document and review it.

MR. GARERI: Exactly.

MEMBER BLEY: That's clearly the only purpose of this is --

MR. GARERI: Well, the purpose again is to provide additional clarification on the two documents themselves.

MEMBER BLEY: And anything beyond the Regulatory Guide?

MR. GARERI: And it talks a little bit beyond the Regulatory Guide itself because it speaks to the items that's coming our way in the rulemaking. But the focus of the ISG was, again, to provide additional clarification on questions that were out there from the industry and then address specifically, like you said, if they decide to use NEI 04-04 Rev 2 in lieu of the Regulatory Guide, it would make it easier to be able to use this cross-correlation table and see what exactly matches up.

MEMBER BLEY: Makes it work --

MR. GARERI: Exactly. Because the two documents, again, were structured differently. Because one is a programmatic approach, another one is for the design aspects.

MEMBER SIEBER: In other words, there's missing pieces if you used one or the other as opposed to using the combination?

MR. GARERI: I'm sorry, I didn't understand.

MEMBER SIEBER: There would be missing pieces. According to your explanation here there are gaps and overlaps. And so if you just use one document, you're going to run into --

MR. GARERI: No. That's not the case. Because during the process the way that the NEI document was revised was that they incorporate any missing pieces or gaps that we found and overlaps were, obviously, revised so that there would be consistency between the two documents. So that was actually addressed.

MEMBER SIEBER: That's okay. Thank you.

MEMBER BLEY: Have their purposes been brought together now are they still --

MR. GARERI: Again, the NEI document still serves a different purpose. But, again, the Rev 2 draft is going to incorporate what we wanted to look at for that particular part of the safety systems as it applies to safety systems.

MR. KEMPER: Yes. This is Bill Kemper again. If I can just expand a little bit.

MR. GARERI: Go ahead.

MR. KEMPER: Yes. Regulatory Guide 1.152 is a licensing document primarily. We use that to license new digital processes from a security standpoint, if you will, as well as many other things.

NEI 04-04 Rev 2, as Mario said, is a programmatic document but it didn't necessarily cover all of the licensing aspects for a new or modified systems. So that was really the task here was to compare the two documents and then embed the licensing aspects of information within 04-04. So now the industry can in fact use that one document to make submittals for all aspects of cyber security.

MR. GARERI: As that final bullet says there, it's basically as Bill just indicated. If they decide to NEI 04-04 Rev 2, the ISG will facilitate the licensing process.

The next slide is just a quick example of how the table is structured so that it basically maps the criteria from the Regulatory Guide to the NEI 04-04 Rev 2 document. As you can see, will tell you the specific section in the Regulatory Guide and then find the appropriate section within NEI 04-04 Rev 2 that basically matches that. And the reviewer will be able to see if its consistent and everything that needs to be covered is covered.

In this case the example we decided to pick out is intrusions, viruses, worms, Trojan horses and bomb codes. And as you can see, the wording in the second column is pretty similar to what's int he Regulatory Guide.

And, again, this is after revising the documents so that they do match up. And we did similar things with the other areas as well. So this is just one example on how the table -- the table itself, I want to indicate, is security related information that comes from NEI documents. So it's not publicly available. In this particular case, we showed a simple example.

CHAIRMAN APOSTOLAKIS: Safety systems includes what? In the previous slide you say power plant safety systems. This includes the support systems, I suppose?

MR. GARERI: Well, as far as the safety systems themselves, maybe Bill can be more specific on what exactly it includes, because it's from the Regulatory Guide itself.

MR. KEMPER: Yes. Again, Bill Kemper here.

The Regulatory Guide really addresses safety related systems per 10 CFR 50.2, I believe it is. So there are other systems that are certainly important safety, but they're outside our purview, if you will. So from a licensing perspective those are the systems that we deal with primarily from a licensing standpoint.

Now, NEI 04-04 Rev 2. though, is broader than that. 04-04 covers all of the critical digital assets, as we call it, in that document which could have an effect on the plant safety itself. If that answers your question.

CHAIRMAN APOSTOLAKIS: But you said that

there were other systems that were important to safety but are not included. That worries me a little bit.

MR. KEMPER: Right.

CHAIRMAN APOSTOLAKIS: What is important to safety that is not a safety system?

MR. KEMPER: Well, like feed water in a pressurized water reactor; that's typically not a class 1-E system, but it's certainly a system that's important to safety. It can invoke reactor trips, you know if it misbehaves and is used for post-trip cooling and that sort of thing. But in the classic sense of the definition of safety grade equipment, it doesn't meet the criteria.

CHAIRMAN APOSTOLAKIS: So, while we're waiting, why not include those systems? I mean, anything that comes close to the reactor? Is it a legal constraint that you have?

MR. KEMPER: Yes. Our statutory purview really is over safety systems.

CHAIRMAN APOSTOLAKIS: Safety related.

MR. KEMPER: Right. So there are lots of digital systems that are installed in non-safety systems throughout the commercial nuclear industry. But, you know we don't see those applications. They would process those under a 10 CFR 5059 and screen them out because they don't meet the criteria for the staff review.

MR. BOWERS: Wes Bowers from Exelon.

I've been involved as an industry representative to the TWG on cyber security.

To answer a couple of the questions, NEI 04-04 Rev 2 covers nuclear significant systems. So that includes safety related, important to safety, security and emergency response. And then the utilities have made a commitment to also include continuity of power. So the NEI 04-04 Rev 2 assessments that have been done or some of them have been done and the rest are committed by the industry to be done by May 1st, include that whole set of systems. Much broader than safety systems.

So safety systems that Bill was talking about and that the Regulatory Guide deals with are only those that meet the definition that safety system is given in IEEE 603 or its intents in 10 CFR 50.49, the EQ rule. It's exactly the same in the IEEE standard or in the 10 CFR 50.

So that safety systems which includes safety support systems or auxiliary supporting features, a couple of different definitions that have occasionally been thrown around, but it's all those under 10 CFR 50 Appendix B QA program

Cyber security in NEI 04-04 Rev 2 is much broader than the limited scope of safety system equipment.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BOWERS: And one other comment just to address Mario's comment. Also the programmatic things in NEI 04-04 Rev 2 are much broader than the limited scope of what's in Regulatory Guide 1.152. So Regulatory Guide 1.152 set out to endorse IEEE 74432, which is only for applications of digital equipment to safety systems. So there is a difference in scope of what's covered by the Regulatory Guide versus NEI 04-04 Rev 2.

MR. GARERI: Jack?

MR. GROBE: Jack Grobe.

Just a little bit broader perspective. While these systems are not covered by specific regulation if you're talking about balance of plant systems, those that are important to the safety of the plant, like feed water, are addressed through two mechanisms. One is the probabilistic risk assessment in the sense that if there's substantial problems with the systems, you can consider those problems within the context of the PRA, but also through the maintenance rule. All of those systems that could contribute to an initiating event, like reactor trip, are covered by the maintenance rule. And the reliability of those systems is tracked and monitored through the maintenance rule and actions are required if the reliability of the systems declines.

So while it doesn't specifically address things like cyber security if that was a problem in those systems it would show up in the reliability of the systems and would be addressed through the maintenance rule.

MR. GARERI: Okay. The next slide would be basically the status. If nobody has any other questions on that example.

MEMBER STETKAR: Let me just follow up a little bit.

MR. GARERI: Okay.

MEMBER STETKAR: Going through the examples, I recognize we don't have time to do that because we're over time already, but if you look at the guidance examples in your Appendix B or NEI 04-04 Rev 2 there is, as was mentioned, a reliance on the PRA to identify important systems, important functions and so forth.

One thing to keep in mind, I don't know how heavily the guidance relies on the PRA right now to identify those safety, or whatever we want to call them; systems important to safety from the perspective of the instrument and control systems. One thing to keep in mind is that traditionally instrumentation and control systems in PRAs have been modeled at a very, very high and simplistic level. What we found is that when you go in and do a detailed fire analysis, for example, where you're worried about fires either failing particular signals or initiating other signals, spurious signals, we often need to add a lot of detail to the PRA even to capture those impacts.

So if you rely solely on existing simplified PRAs to identify important interactions between instrumentation and control signals and other systems, you may not capture the full range of things.  Because the PRA is probably not developed to a sufficient level of detail to find those.

So the message here is do rely on the PRA because they're useful, but don't rely solely on the PRA or things like risk importance measures to say okay this is a ranking of the interfaces between our instrumentation and control systems and the plant systems.

That was one point. Second point, quickly, is if you go through the details, there is a bit of a lack of sensitivity to interfaces between digital instrumentation and control systems and support systems.

For example if you look at the physical protection guidance, physical protection guidance primarily is focused on barriers to physical intrusions; rooms, locations, things like that. In the early part of the guidance you mentioned the right things about -- also things about support systems like AC/DC power supplies for the control systems themselves; ventilation and room cooling things which are an interface issue. But those issues are lost when you get to the detailed guidance.

So just a comment to keep those things in mind because we're talking about not the instrumentation and control system in isolation. It's integrated with the rest of the plant. And any guidance on recognizing this is cyber security but it's really security of the systems themselves, the equipment, the hardware and intrusions that would disable, for example, DC power or ventilation could thwart your whole purpose.

MR. HECHT: Again, just a follow up on that comment.

One technique which is used is just dependency diagnose. In other words, in NEI 04-04 Rev 2 it speaks about a concept or an entity called the critical digital asset. And the critical digital assets, of course, I assume are those that are related to controlling, in this case safety systems. But then those CDAs depend on infrastructure, depend on power, HVAC, a number of other things, maintenance and along with maintenance tamper protection.

So those types of things can be identified through this dependency analysis as a technique. And perhaps that should be more closely reflected in staff guidance. I didn't see that term in there. It might be there, but I didn't see it.

MR. GARERI: Okay. Just one general comment. One of the reasons why we're developing the draft guide to support the proposed rule is to make sure that we have more complete cyber security guidance. If these documents did the entire thing perfectly, then we would just transfer them over. So the new guidance, hopefully,m will address some of the concerns that you have. But, again, it's going to be out for comments, hopefully by the end of this month.

But this guidance document does not address everything complete for cyber security.

CHAIRMAN APOSTOLAKIS: Is that in answer to what Myron said? Is anybody using those dependencies? Do they appear in the NEI document?

MR. HECHT: I didn't see it.

MR. GARERI: No.

MEMBER STETKAR: They don't. The NEI document in the introduction, kind of up front in the document, discusses a lot of these things. However, if you get back to the details of the -- I forgot. I don't have it in front of me here. But there are details in Appendix B of the ISG or the NEI document that actually give point-by-point comparisons of what you should consider. And those types of interactions seem to get lost in the details of the point-by-point comparisons so that the early part of the document says the right things, but I suspect as most guidance documents people who use it are going to look back in the details and check off the boxes to make sure that everything meets all of the detailed information in it.

It does get lost.

CHAIRMAN APOSTOLAKIS: Okay. I expect

you will come before the full ACRS soon with these issues, and the Committee will write a letter. Is that the plan, Jack?

MR. GROBE: The answer is we'll be coming before the ACRS in probably the context of the Regulatory Guide necessary to implement the new 73.55. Is that right, Mario?

MR. GARERI: Yes.

MR. GROBE: Yes. Now the soon question is you anticipate that will be mid-year?

MR. GARERI: I believe so, but maybe Scott Morris can address that better.

MR. GROBE: Yes, I don't have those dates at the tip of my fingers. But there is a Regulatory Guide being developed that is a companion to the new rule 73.55(m), I think it is, and that will come to the ACRS in the development of the Regulatory Guide. And I think that's scheduled for June.

MR. GARERI: It is scheduled for June. But, like I say, I don't have the --

CHAIRMAN APOSTOLAKIS: How about the ISGs, they're a part of the guide or what?

MR. GROBE: No. The ISGs don't come to the Committee, the full Committee.

CHAIRMAN APOSTOLAKIS: Okay.

MR. GROBE: The ISGs will be incorporated into some form of formal regulatory infrastructure. And that document, whether it's a regulatory Guide or Standard Review Plan or a NUREG, whatever it might be, that will come to the Committee for consideration. The full Committee.

CHAIRMAN APOSTOLAKIS: But last time I thought we reviewed the ISG with a 30 minute window.

MR. GROBE: You did. You did.

CHAIRMAN APOSTOLAKIS: And the Committee wrote a letter? Didn't we write a letter on that?

MR. GROBE: Who remembers?

CHAIRMAN APOSTOLAKIS: Yes, we wrote a letter.

MR. ARNDT: The letter you wrote, basically said you had looked at three ISGs that we had previously briefed you on and that you were comfortable with the issuance and use of those ISGs.

When we originally talked to you a year ago, the arrangement was that we would brief you on a regular basis on the status of various things that either had recently been finished or would recently be available, and you provide an input on the acceptability of those guidance and any additional recommendations for future work.

In a letter that you wrote in November you basically endorsed the issuance of the three ISGs and provided additional guidance on areas that we might want to look at before we made them a formal document.

CHAIRMAN APOSTOLAKIS: So are we going to do the same thing with this?

MR. ARNDT: That would be the expectation.

CHAIRMAN APOSTOLAKIS: And that will happen in June?

MR. GROBE: Well, was that a letter from the full Committee?

MR. ARNDT: Full Committee, yes.

CHAIRMAN APOSTOLAKIS: Full Committee, yes.

MR. ARNDT: There are two different things.

The ISGs are interim guidance that will eventually be turned into staff guidance.

CHAIRMAN APOSTOLAKIS: Right.

MR. ARNDT: The guidance you have in front of you in the slide right there is a separate guidance that is related to the ISG. That will come to you formally June/July, whatever it is, for normal process review.

MR. GROBE: Now, George, I don't think we're answering your question.

The official process does not require a letter from the ACRS.

CHAIRMAN APOSTOLAKIS: Right.

MR. GROBE: If you desire to send us a letter, we're certainly interested in whatever insights you have. If we need to come back and meet with the full Committee to precipitate a letter, we'd be glad to do that. We look for your insights as to how to proceed. But our processes and the ACRS's procedures don't require a letter for interim staff guidance.

CHAIRMAN APOSTOLAKIS: But since we did it last time and Steve said it useful, maybe we should do it again.

MR. GROBE: Insights from the ACRS are always useful.

CHAIRMAN APOSTOLAKIS: Always useful.

MR. GROBE: And we appreciate every insight.

CHAIRMAN APOSTOLAKIS: Yes?

MR. SHUKLA: Yes. This is Girija Shukla, Senior Program Manager for the ACRS.

Yes, we did write letter on three ISGs last time, and we'll probably do it again. But the problem is that only one ISG is complete at this time.

And I have scheduled full Committee meeting in April, April 10th to 12th for this ISG.

CHAIRMAN APOSTOLAKIS: So we'll discuss the three ISGs that we're discussing today.

MR. SHUKLA: But they're not ready, I guess.

CHAIRMAN APOSTOLAKIS: What do you mean "they're not ready"?

MR. GROBE: Well, only one is ready today.

MR. ARNDT: The one that we just reviewed has been issued. The one that we will review shortly on licensing process is not yet in final form, but it's working towards that. An ISG on Part 52 PRA reviews is all but done. It's finished. It's gone through OGC review and it's currently under final review by the steering committee.

CHAIRMAN APOSTOLAKIS: So if we are to have an impact on the final product, then we should meet in April?

MR. ARNDT: Yes, sir.

CHAIRMAN APOSTOLAKIS: Okay. So you did the right thing.

MR. MORRIS: Just briefly. Scott Morris, I'm the Deputy Director for Reactor Security. I'm also on the I&C steering committee with Jack.

The issue here with this ISG for cyber security, I don't anticipate this ISG will have a lifespan beyond the end of this year, maybe early next year. Because the Regulatory Guide that we're writing to support the rulemaking in Part 73, which is the new programmatic requirements for cyber security, as has been mentioned here there is a separate Regulatory Guide. It's been developed. It's been through several levels of staff review. By the end of this month it should be out on the street for our stakeholders. It's not a publicly available document, but it will be out for their comment. It will capture the whole range of cyber security from a programmatic standpoint, it will roll in some of these specific issues that Bill is interested from the standpoint of licensing safety related systems. It's soup to nuts.

CHAIRMAN APOSTOLAKIS: When would be a good time for us to review that particular document?

MR. MORRIS: We're going to put the draft guide out for a 45 day comment period. We're probably going to meet with the industry at least once. So I would say we'll have the benefit of industry comments and be able to fold those in probably by the end of May, June. But the Regulatory Guide itself won't go final probably until the rule's effected, which is early next year.

MR. GROBE: Go ahead, Bill.

MR. KEMPER: Since it is a Regulatory Guide, process-wise of course you know you have the opportunity to review it before it goes out for public comments. Typically ACRS declines and waits until we get those comments. So it's your choose. You could actually see it very soon in raw form without the benefit of industry feedback.

CHAIRMAN APOSTOLAKIS: Well, it's usually better to review it after the industry comments. So probably July or September.

MR. MORRIS: This is a reflection -- it'll be our own guidance, but the industry has also asked if we would include an endorsement of the latest version of NEI 04-04 as part of the guidance. So rather than just one option, which would be the staff methodology, the industry's asked well how about putting two options in the Regulatory Guide which includes NEI 04-04 Rev 2 or 3 or whatever it is.

CHAIRMAN APOSTOLAKIS: This is all on the cyber security?

MR. MORRIS: Right. Yes.

CHAIRMAN APOSTOLAKIS: Well, we have two more ISGs today?

MR. GROBE: Yes.

MR. GARERI: I think I'm over my time.

MR. GROBE: Well, you got lots of help, Mario.

CHAIRMAN APOSTOLAKIS: Well, that's because you're very slow.

I mean, we can have a meeting with the full Committee in April. You discuss this, you give us this programmatic information. And if we write a letter, which is not clear, we'll take all these things into account.

It's usually a good idea to write a letter and document the advice of the Committee.

MR. GROBE: Yes.

CHAIRMAN APOSTOLAKIS: Of course, you can always go back to the transcript and see what we are saying today.

MR. GROBE: Yes.

CHAIRMAN APOSTOLAKIS: But I think it's much easier and better.

MR. GROBE: What I would ask is that Stew work with Bridgett and figure out exactly what we can accomplish at various points in time and get those things scheduled.

CHAIRMAN APOSTOLAKIS: I think that's a good idea.

MR. MORRIS: And ordinarily with security we don't get you all too involved. But this is a unique issues and I, personally, would appreciate a little bit of extra insight on cyber. And I would just also add there is a whole new rule being created, safety security interface. And somehow that gets wrapped up into this, too.

So there's lots of very interesting issues associated with this.

CHAIRMAN APOSTOLAKIS: Very good. Okay. So we will have a meeting in April.

Thank you very much.

And the next one is on licensing process, Mr. Bailey.

MR. BAILEY: Actually, I think I'll just do a quick turnover to Mr. Loeser.

CHAIRMAN APOSTOLAKIS: Okay.

MR. LOESER: Thank you. My name is Paul Loeser. I'm in the Division of Engineering in NRR. I'm one of the digital reviewers.

The question came up on what is the process to go through for licensing, what documentation needs to be issued, needs to be submitted by the licensees or the vendors, and that type of thing.

Chapter 7 provides our review procedures when reviewing any I&C, BTP 14 goes specifically into software and things like this.

When we do these reviews they are somewhat unique in that we not only depend on testing, but we also depend on a well defined life cycle and a high quality process. The reason for this is the end product of a complex digital system is, in fact, very complex and we can't just review the code and see if it's good. It's too much. So we depend upon the licensee and the V&V team to do the detailed review and we sample this.

We take a look at a typical waterfall life cycle as defined in IEEE 1074. We look at the concepts, the requirements, the design, the implementation the tests, check out an installation; all of those things and the various inputs that go into these life cycles and the outputs and the processes.

In a typical staff review we look at the system specifications and how that system's specification is translated into hardware and software specs.

We look at the design procedures and the V&V program that is used to verify and validate those design procedures.

Next slide, please.

We review any information that may be available on hardware and software history.

Specific plant applications we do a thread audit where we sample various plant parameters or select various plant parameters.  And walk through the development process of how that particular parameter works.

Look at the coding standards that were used.

Then look at the hardware/software system, look for interfaces, timing problems.

And a great deal of this in the thread audit we may pick out of half a dozen out of 8,000 different specifications. So we only do a very small sample of this, but we're looking at the process that was used for the licensee to do it.

When we do a review, we --

MEMBER BLEY: Can I ask you a question about the process?

MR. LOESER: Certainly.

MEMBER BLEY: I know when you do the V&V they look to make sure the systems perform the way they ought to for the primary areas of interest. Some of the really funny failure modes that have happened out there are when input goes outside of the expected range of parameter values.

Do you see if there's any testing to look what happens with these systems if inputs drift outside of the normally expected range?

MR. LOESER: Absolutely. Not only outside of normal range. If communications between one software unit passing of parameters goes out of whack for some reason, you either pass an incorrect parameter, we make sure that the various units are compatible. We take a look at any communications issues between various parts. We take a look at the timing analysis that was done on the hardware. We may trace things through the schematics.

But remember, we're doing this on a very small percentage of the overall system. Where you're taking five or six or maybe as many as ten individual specification items out of thousands.

What we're really looking for here is the process that was used by the V&V people and by the licensee to assure ourselves that they did this on everything.

MEMBER BLEY: Very good. Thanks.

MR. LOESER: We obviously don't have time to do it all, otherwise we'd need ten reviewers for years.

MEMBER BLEY: My question was aimed at the process.

MR. LOESER: Yes. And we look to see that the process does these things. But we basically ask four questions:

What's going to be done?

How will it be done?

Was it done correctly?

And what were the results?

For the first question: What's to be done? We look at the various plans that are going to be used. What planning documents are being used for the configuration management? What's being done for software quality assurance? How is V&V being handled?

For how it will be done, we get down then into some of the procedures. What method will be used?

It's fairly easy to write a plan that says, oh, we're going to do all these grand things, but then are they actually being done.

The third thing, was it done --

MEMBER SIEBER: How do you assure that?

MR. LOESER: Well, we do it in two steps. (1), we look at the procedures, the methods that are going to be used and see if they using those procedures will actually accomplish the concepts within the plan.

The second thing we do is during the thread audit where we look at what was actually done, we then take these sample parameters, go through it and see that the various processes were actually used and used correctly.

MEMBER SIEBER: But there's thousands of elements?

MR. LOESER: That's correct. And we can only --

MEMBER SIEBER: So your audit is not going to cover thousands of elements?

MR. LOESER: No. We look at a sample. We look at a sample to make sure that we have reasonable assurance that the V&V team and the plant and the vendor did all of these things. If we start finding problems with it, then of course we would go into much deeper detail and potentially turn down the application.

MEMBER SIEBER: That's a very difficult process, though.

MR. LOESER: Yes, it is.

MEMBER SIEBER: Because there's a multitude of elements that are involved in that. And the sample size is typically for audits are so small that you really can't ascribe probability to that.

MR. LOESER: That's correct. We looked one time --

MEMBER SIEBER: I guess -- what else you can do.

MR. LOESER: Yes. The alternative would be to do our own independent V&V.

MEMBER SIEBER: Right.

MR. LOESER: Or do a full design verification. And this would be so complex --

MEMBER SIEBER: And time consuming.

MR. LOESER: And time consuming that we would basically have to send several experienced auditors on site and do the independent V&V

ourselves.

So while this is complex, it's less complex than the alternative.

And then, of course, finally we look at the results of the final V&V report, the testing reports and things like that to assure ourselves that the overall specification items have in fact been met.

MEMBER SIEBER: Now you actually have done licensing work on what, 30 or so systems? Not full systems, but parts of systems.

MR. LOESER: Myself only a half a dozen or so.

MEMBER SIEBER: Yes.

MR. LOESER: But the NRC --

MEMBER SIEBER: But what the staff in total has done?

MR. LOESER: Yes, probably. Somewhere like that.

MEMBER SIEBER: Is it 30?

Have you determined anyplace where your review led you to the more positive conclusion than actually existed in the plant and discovered through failures months or years later, or would you say that your process is pretty reliable to determine the reliability of the licensee's product?

MR. LOESER: I think our process is reasonably reliable. There are, of course, always possibilities that something can fall through. I can think of one area or one particular review that we did where we came to the conclusion everything work, and it did but it turned out that there was a software change later on that was not fully tested. This is after we had done our review and after it had been installed in the plant. And that eventually caused a problem.

But we believe that our process is reasonably thorough and will lead us to a conclusion of reasonable assurance, but not 100 percent confidence.

MEMBER SIEBER: So you're relying on examination of the process --

MR. LOESER: Yes.

MEMBER SIEBER: -- as opposed to the individual examinations of output?

MR. LOESER: That's correct.

MEMBER SIEBER: Okay. Thank you.

MEMBER BLEY: Paul, you've raised a really interesting issue there. How does the process work after the initial approval such that as software patches and software changes come along that they get a thorough V&V? And do you folks monitor that after the initial installation?

MR. LOESER: One of the things we look at during the initial review is what the process will be: That is what is the configuration control process both at the vendor who is likely to be doing the software changes; what level of regression testing is required; what level of V&V and also; at the plant how do they control their configuration, how do they know that what they are receiving as a change is in fact appropriate, has been appropriately test. And we approve that.

However, changes that are made at a later date after the fact are no longer in the licensing process. They're now in the maintenance phase, and this is handled by the regions. We make sure the planning is correct, but the region and local inspectors make sure the performance is correct.

MEMBER SIEBER: And some of these could be done under 50.59?

MR. LOESER: Actually, a significant number of them are.

MR. KEMPER: This is Bill Kemper.

If I could just tag on to what Paul's

saying. The majority of these changes, of course, are made under 50.59. If a change is such that it invalidates the assumptions by which the SER was approved in, then that would require a re-submittal to headquarters to be re-reviewed.

MEMBER SIEBER: But you would not know about it unless some inspector in his sampling process came across it?

MR. LOESER: That is correct.

MR. KEMPER: Well, no. Actually the licensee's 50.59 process should divulge that information. In other words, you know they're very trained. There's NEI guidance out there that covers this in detail. So they have processes within their infrastructures to make that determination of which the change that they're making has not been reviewed previously by the NRC. In which case, that would turn into a license amendment request.

MEMBER BLEY: Is there reason to believe that as software upgrades come out, they'll be applied across the board or are they likely to be plant specific or even plant system specific?

MR. LOESER: They're very likely to be plant specific, particular at this time when individual plants are making individual changes.

For example, Oconee is replacing their entire RPS and ESF system. Wolf Creek is only replacing their main steam isolation system. So somebody may use the same platform that say, Oconee is using, the TELEPERM XS but have different kinds of changes they're making, apply it to different safety functions, fewer or more, and therefore a code change may not be appropriate.

If it's, for example, in the base code of the system, the operating system, then it would probably be applicable to everyone. But if it's in the application specific, it would be by plant unless there happened to be two plants that are sufficiently identical and they're using the same applications code.

CHAIRMAN APOSTOLAKIS: Are you done?

MEMBER BLEY: I'm just nervous, that's all, how that process plays out in the long term. In other industries I've seen cases where the wrong uprate gets to the wrong place, and that whole process of QA is one that's going to be real interesting I think.

MR. LOESER: That's why we pay very close attention to quality assurance, configuration management and the V&V process.

CHAIRMAN APOSTOLAKIS: There has been quite a lot of work that this agency has sponsored at Brookhaven and Ohio State University under the umbrella of developing PRA methods for software. But really if you look at what they have been doing, a lot of the effort has been spent on developing methods for identifying failure modes.

Is any of that work, is it useful to you? Do you think you can use it at this point, or wait for a while, or --

MR. LOESER: There are two answers to that. As far as useful, yes it's useful for general information to make us more aware of problems and things to look for. But with the specificity needed for specific plant or vendor reviews, no it has not gotten to the point yet where we can actually incorporate these lessons into our review guidance. We're hoping though, however, as this goes on. Plus there's some efforts going on in University of Virginia and University of Maryland for things like fault injection and classification that we have hopes for. However, it hasn't gotten to the point yet where we can actually use it.

CHAIRMAN APOSTOLAKIS: Well, regarding specificity, what one of the drawbacks if you will of these methods is that they're very labor intensive. I mean, precisely because they model specific systems. You have to invest quite a lot of time to develop a particular model that will allow you to identify failure modes. So they are, in fact, very system specific.

But I'm wondering what it would take for those methods to become sort of routine so people like you who are really the decision maker can find them useful?

MR. LOESER: Well, one of the things that's being done is Research has, and I'm not sure which one of the universities they're working through, acquired some of the systems that we have approved. A Tricon system, for example, or a TELEPERM and they're going through and investigating the design details and exactly how it works and exactly how the software works to try to develop better models so we could plug in some application specific software and do this. However, we haven't gotten to the stage yet where this is a routine or even right now I don't know whether it's possible. I'm afraid Research would have to give a better explanation of exactly where they are at this time. However, all of this research has been started based on NRR or NRO prompting and user needs. And to be honest, I'd love to be able to make my job similar and easy.

CHAIRMAN APOSTOLAKIS: Are you being consulted or briefed?

MR. LOESER: Yes. We are briefed. We get to read the interim reports. They are sent over to us for review, concurrence for suggestions of future things.

CHAIRMAN APOSTOLAKIS: Okay.

MR. LOESER: And I do in fact read them. Either myself or some other qualified reviewer reads them. In general, I read them all, but I don't always write the comments.

Yes, we are kept quite informed. What we're not kept informed on is the interim things, that is in between reports. But --

CHAIRMAN APOSTOLAKIS: But you do have influence on what they are doing?

MR. LOESER: Of course.

MR. KEMPER: Yes. This is Bill Kemper. If I can just tag onto this.

Yes. As you know, the Office of Research has a five year dataline research program plan which has been developed with quite a bit of interaction with NRR as well as NRO. And so, yes, the office, as everybody knows, is a support office to the other one -- to NRR and NRO. And so they depend very heavily on our inputs in prioritization of the projects, if you will.

And so if I could just kind of expound on the fault injection project I think is going on down at the University of Virginia that the Office of Research is still managing. We're looking forward to that producing perhaps some very, very useful results for us to use in licensing new applications.

I don't know when's the last time you had a discussion from Research on that, but that's a project that we have high hopes to very fruitful to identify really the reliability, to be able to assess the reliability in a clinical means, okay, empirically rather than just estimating and that sort of thing.

CHAIRMAN APOSTOLAKIS: Well, again, but there are two parts to it. One is the identification of failure modes.

MR. KEMPER: Yes.

CHAIRMAN APOSTOLAKIS: And as the other is the reliability.

MR. KEMPER: Yes.

CHAIRMAN APOSTOLAKIS: And even at that time, and I think to this day at least some members of this Committee have serious doubts about the reliability part. But the failure modes, I think the work is very useful. And ultimately I think what will happen is that you will have a number of tools and each one will give you different insights. I mean, I can see the value of fault injection. Should I rely only on that? Absolutely not.

MR. LOESER: No, I don't think we can rely on any one tool.

CHAIRMAN APOSTOLAKIS: Exactly.

MR. LOESER: We need a preponderance of evidence.

CHAIRMAN APOSTOLAKIS: But the other thing is that I think the staff should make a very clear distinction between the qualification part and the structural part, right, to figure what failure modes exist. And in my personal view, we don't speak on behalf of the Committee of course, it's the first one, the structural analysis, the failure modes that would be very useful, at least in the foreseeable future.

MR. LOESER: Well, in particularly when it comes to us doing our thread audits if we knew with a reasonable degree of confidence what the real threat was, what was the most likely failures are, we could tailor our thread audit to make sure that kind of thing was among the things we looked for to try to just improve our odds of finding any problems. But as of yet we have not yet gotten the reports in that level of specificity to be able to do this. We are hoping that this will occur in the future.

CHAIRMAN APOSTOLAKIS: Okay.

MR. HECHT: Could I ask a question?

MR. LOESER: Certainly.

MR. HECHT: I'm clear as to what the scope of your activities are. There's one part of it which I thought it was, which was just dealing with the process which is basically there's a plan, the plan is conformance with 1074. You verify that they've followed the plan.

Then there's another part of it which is how they might do their plan. And specifically, I guess, the last part of the discussion was testing oriented toward failure modes.

And do you consider the scope of your activities to say not only that they did testing, but what techniques were used and whether those techniques were adequate? Is that part of the scope of your job or it's just that they said they were going to do testing and --

MR. LOESER: No, no. We have to make the testing is adequate to prove their point. For example, there's a different level of testing. There's a unit testing where they start putting the software together. There's integration testing where they integrate it in with the hardware. Those are looking for individual problems, communications errors, early problems of, I don't know, misnaming the very constance or whether you're using a global or local variable or, you know details like that. Are you passing the correct parameters? Does the receiving unit get what it expects; that type of thing.

Then there is the factory acceptance test where now you are beyond just the individual parts and you're looking for does the system overall meet its specification.

So different levels of tests are trying to perform different things. And we look at first the test plan to make sure that they are planning to do all of this and what the direction is. Then we look at the procedures to see do these procedures if they follow these procedures, will they prove what the plan says it's supposed to do. Then during the thread audit we follow, after we've followed the development of it, we look at how was it tested, what were the test results, let me see the particular test sequence and what was done and who signed it off. In some cases if the equipments really still there, we may ask them to repeat one of the tests. You know, out of three weeks we want to see one 20 minute segment or something like this for this particular specification. It varies, sort of depending on whether the equipment is still on sight, how integrated it is, how set up it is, how complex it is a major issue.

Are we having something with 15 or 20 different cabinets with a total of 300 microprocessors or is this one simple function, like Wolf Creek using FPGAs, not even a microprocessor, that's going to be much simpler to follow the testing.

And we have to tailor it each time in accordance with what the system is, what it's supposed to do and what the testing philosophy of the plant is. Are they doing this all manually? Are they using a software tool to do all the testing? Does the software tool actually perform the testing that they want it to?

These are all decisions that have to be made. This is not an easy thing for a staff reviewer to do. It takes a lot of experience. A lot of knowledge. Fortunately in past lives I have been a software designer, I've worked in factories, I have built things and stuff like this so I have some knowledge. Granted, it's somewhat outdated. We didn't have FPGAs in those days and the microprocessors were much simpler, but the same concepts still hold. But that's one of the reasons why we have problems finding enough people to do this because it's not a simple task.

MR. HECHT: Can I try to clarify the question?

MR. LOESER: Sure. Maybe I'm off on a tangent.

MR. HECHT: Yes.

We spoke, for example, about fault injection testing.

MR. LOESER: Yes.

MR. HECHT: Which, incidentally, I have a different view of than maybe some of the other people here because I've seen it not work.

As opposed, for example, another kind of testing do you feel that if a licensee were to present you with a plan that said we're going to do fault injection or that didn't have fault injection testing in the plan and you felt on the basis of the results you'd seen from the work done by Research that fault injection testing should be in there, is that part of your authority to say we think that you should do this and include that?

MR. LOESER: Actually not. We're not allowed, really, to tell the licensee exactly what they ought to do.

MR. HECHT: I see. Okay. So --

MR. LOESER: What we do is we judge what they do. We tell them our overall expectations.

MR. HECHT: Okay.

MR. LOESER: That is, this is what the end result needs to be and then we look at what they do to see if they've reached that end result. We can't be prescriptive on exactly what tests we want them to do.

MR. HECHT: Okay.

MR. LOESER: We can say that if you do it this way, we have reviewed it in the past and we think it will be acceptable.

MR. HECHT: All right. I just wanted to

be clear on that point.

So the results coming from some of the advanced, not only testing techniques but for example their static analysis technique or -- I don't know. Say even some kind of earlier techniques in terms of specifications. That's not something you could prescribe, but that you only might say might be recommended, but is really at the discretion of the licensee?

MR. LOESER: That's correct. What we can do is we have various Regulatory Guides. And, say, for example if you follow a particular standard, we think that standard's good enough and we'll come up with a method. But we can't tell them that if you don't use this standard, we won't approve it. We have to look at whatever they did do and then determine if they reached an equivalent level of safety, an equivalent level of protection. And if they did, we need to approve it. If for some reason they didn't, then we have to look at what possible compensating measures were done, other things like this, then reach this determination.

But in the long run, the only thing we can really do is say was what the licensee did good enough or not.

MR. HECHT: Okay. If I could just make one final recommendation rather than a question on part of the Research plan that I did find interesting was was the operating experience. And I would suggest that as pat of that operating experience if analysis were properly done on failures that were discovered in the past with respect to the causes, that that might be useful in other words to say how much of it was due, for example, to configuration management issues or how much of it was due to inadequate traceability or how much of it was due to just poor coding standards.

CHAIRMAN APOSTOLAKIS: Yes, we have to follow the --

MR. LOESER: We agree with you entirely and you're getting a presentation on that this afternoon.

CHAIRMAN APOSTOLAKIS: Yes, you're getting a presentation next.

MR. HECHT: Okay.

MR. GROBE: Let me just make an observation. Paul is on slide 5 of 15.

We've been dealing with many very difficult technical issues. Those are easy as compared with this question, and that is what is necessary to achieve reasonable assurance.

CHAIRMAN APOSTOLAKIS: Yes.

MR. GROBE: Nobody knows what reasonable assurance means. I hesitate to say, it's a bit like pornography: When you see it, you can understand it. But reasonable assurance is somewhat of an elusive concept.

We've done a number of very successful digital I&C platform reforms. The difficulty from the industry's perspective with those has been that each review has gone different directions and there's a bit of an unpredictability in the level of detail that we got into because of various problems with those applications and technologies.

And the goal of this interim staff guidance is to provide a predictable level of review consistent with the standards of the Regulatory Guides and the Standard Review Plan and the interim staff guidance of what documentation we expect to review, how we expect to perform audits. And then the component that hasn't yet been defined well is the inspection piece in the field once the equipment is begun to be installed and before it goes into operation.

Similar to steam generator replacements, we have a comprehensive inspection program after the licensing staff does their piece.

We have the Oconee application for a major retrofit in house right now. We've got a draft interim staff guide on the licensing process. We're continuing to refine it.  What we're planning on doing is using that draft ISG in the Oconee review. And as we go through that review, I would suggest that would be an outstanding time to come back to the Subcommittee and describe how that's going, what kind of work we're doing, what we're finding and we're developing reasonable assurance.

So I'd suggest we let Paul get on with his presentation and then schedule some time to come back as the Oconee review is proceeding.

CHAIRMAN APOSTOLAKIS:  And I suggest that maybe if we have discussed some of the slides, you could skip them or go over them very quickly.

MR. LOESER:  Okay.  I'll try to go through it quickly.  The real problem here is that the review I've been discussing takes a significant amount of documentation. And  the question is do we really need all of this?  The licensees would prefer to submit less.  So the task working group looked at several different times.

One is level of detail. How much detail do we need?

What is the application of Chapter 7 in digital reviews?

Provide some clear protocols for developing this application and clear guidance for licensing on cyber security.

On slide number 6. In order to address this our working group tried to come up with a listing and a reason for the documentation that needs to be delivered to the staff. At what phase this licensee documentation is needed. Which of this documentation needs to be on the docket, and which does not be on the docket but needs to be available for the staff during an audit visit.

We've had considerable input from the industry. We have come up with a draft version of interim staff guidance. This staff guidance is based on, so far, the most complex review. That is a new platform and a new application and at the moment is only applicable to existing plants. We plan to expand this later to cover new plants. But the process is somewhat different.

Slide 8 we say that these guidelines do not modify or exceed the existing regulations. We've used Branch Technical Position 14. We have made one change. We have divided up the review into licensing and operational issues and things like the software maintenance planning and the software training planning are considered operational issues. So we are going to de-emphasize those.

Slide 0--

MEMBER BLEY: When you say you're going to de-emphasize those, they come up later on --

MR. LOESER: Oh, we are shifting the emphasis of these from the headquarters staff doing the review to the regional staff. And we're in the process of writing an inspection procedure for the regional staff to use. What they need to look at in these various things to determine that it is adequate.

MEMBER BLEY: Have you said anything about how the regional staffs are coming up to speed on digital I&C?

MR. LOESER: I have had no --

MEMBER BLEY: An input where the regional staff all have to leave that up to other people?

MR. KEMPER: Yes. Bill Kemper again.

Yes. We've developed some training curriculum specifically aimed at digital I&C

technology. It's called E1-14. TTC has worked with us and we've conducted two sessions of that so far. And the regions have sent quite a bit of their folks to those to start getting involved with that.

And also they're looking at other resources on their own to enhance the training for their own folks.

MEMBER BLEY: Thank you.

MR. LOESER: Anyway, some of the basic approaches. We assumed that by the time we get a license amendment request that the planning stage for the modifications have already been done. They've already written the specification. They've already written the V&V plan. They've already written the software quality assurance plan, that type of thing. And that all of these planning documents will be available at the time of submittal.

They may not have finished the final design yet. They may not have finished all of their V&V. They may not have done any of the detailed design yet at this point. But we expect that the design documentation should be available sometime in the neighborhood of six months after we do the acceptance review, and this is somewhat negotiable depending on the review schedule.

Some of the detailed design documents, for example individual code listings and individual schematics, we don't need here as long as they're available on site when we got to the vendor site, for example, to do the thread audit.

And, of course, some of them can't be done prior to our review. For example, installation testing. They can't possibly have completed installation testing before our approval.  So that has to be available for regional staff review for startup testing or whatever the regional staff looks at.

The ISG also specifically looks at the information needed for an acceptance review. And when we do an acceptance review we have to see that there's enough information available that the system is planned well enough that we see a clear path to success to acceptance and review of this.

For example, if they're not planning on doing V&V.  Well, fairly obviously we can't accept that, so we won't even accept it for review.

If there's other problems, we may not accept it for review.  If they just come to us and say we'd like to buy one of these, we'll install it, we'll do really good stuff. We say what kind of good stuff. We haven't decided yet. That's too early for us to do the review. So we probably wouldn't accept that.

Generally we look at the systems specification, the system requirements, the system description down to a block diagram level, hardware and software, dedication. If they're using commercial parts or commercial system, the commercial grade dedication plan. And then the V&V planning, quality assurance planning and defense-in-depth are all quite important. We sort of expect to see those up front.

MEMBER SIEBER: Have you given any thought to things like certified designs?

MR. LOESER: Yes. We take a look at what certified designs there are. We have reviewed three of them so far. We have reviewed the Triconex PLC triple redundant. We have looked at the TELEPERM XS. And we have reviewed the Westinghouse Common Q. All of those have been approved. When we do a review now, we would only look at the plant specific application.

MEMBER SIEBER: Right.

MR. LOESER: And anything that may have been changed in the design. As an example, the TELEPERM XS is using a different microprocessor than we originally reviewed, which is a different board. So we would have to look, for example, at the temperature and humidity and EMI qualifications; have they changed, is that any different now. But if they've used the same design process, if they've used the same V&V process and all of that, we would not go back at any of that.

This is discussed in a slide a little bit further on. There's no reason to review something that's already been reviewed. Why should we look at it twice?

MEMBER SIEBER: Right.

MR. LOESER: We don't have the time or the people.

We've based our list of documentations on things we found in our Standard Review Plan. For example, Appendix A, the review process for digital I&C, see the conference to IEEE 603 conformance to 7432, Chapter 18 on human factors, Branch Technical Position 7 on software reviews and on Regulatory Guide 1.152 for cyber security requirements.

MEMBER BLEY: Let me sneak a question in on you.

MR. LOESER: Sure.

MEMBER BLEY: If there's a hardware

change or a software change --

MR. LOESER: Yes.

MEMBER BLEY: -- are the V&V requirements they have to meet greatly reduced to look at only what they think has been effected or do they have to still be fairly broad to see if they've introduced new interactions and problems?

MR. LOESER: I would expect it to be fairly broad. I would expect, for example, a full range of regression testing. I would expect the V&V to look very carefully at this, look at all the interfaces.

Well, the design team, first of all, should look at all the interfaces, make sure that none of any timing changes have been accounted for, any differences in signal trajectory have been taken care of; this type of thing.

It very much depends on what the change is and the scope of the change. In some cases if a resistor manufacturer goes out of business and they're using a different brand of resistors, it's virtually nothing. As a matter of fact, that would probably be about as much review as it would get, what I just said.

If they switch from a 386 to a Pentium 5, it may be a fairly significant amount of information. And once again, we spot check this. We try to make sure that the design team and the V&V team looked at all of this, but we don't have time or people to look at it all ourselves. We spot check it. We want to make sure we do enough to give ourselves a reasonable assurance that they did all of this already.

MEMBER BLEY: One last question in this area. Does the Regulatory Guide, the SRPs, the Branch Technical Positions distinguish between initial V&V and V&V on upgrades of one way or another.

MR. LOESER: Not at the moment.

MEMBER BLEY: I'm sorry, that begs another question. Is it in the mill?

MR. LOESER: We're planning upgrades. I'm not sure that this is one of the things we have currently planned. Basically an upgrade like this requires a certain amount of knowledge and experience on the part of the reviewer to decide what they have to look at. And, of course, management guidance has to -- you know, if you try to get too deep into it, they sort of pull the chain a little bit and pull us back to try to keep it reasonable.

MR. HECHT: We got this shipped to us.

It's a document entitled "Documents Needed for Reviews of Different Complexities," which I reinterpreted as basically experience levels, whether it's existing, modified or new. Are you using this?

MR. LOESER: Yes. This is part of the overall ISG. That's Appendix 2 or something like this. I can go into a little bit of the format of the ISG, and I was planning to actually starting this slide.

MR. HECHT: Okay. All right. But the ISG is not the Regulatory Guide, and that's why --

MR. LOESER: That's correct. However, we expect that eventually all of the ISGs will be incorporated into a Regulatory Guide or the Standard Review Plan or some other more formal not interim guidance.

But we have table 1 where we show the review criteria, where we show which are the applicable SRP sections, what are the requirements or the standards that are associated with these particular documents, how the requirements are met or referenced in the license amendment request. And then columns 4 through 7 shows at what stage we expect to have this document, whether it's with the original review -- with the original submittal, whether it's supplied later on during the process of the review, whether it's available for audit or available on site for the region.

The second set of tables are what you were referring to there. We actually have three of them. One of them shows a digital platform which was previously reviewed and is being used in the same format as was reviewed. There haven't been any changes to the basic platform, but the application that it is being used in is new. So it's plant specific, in which case we wouldn't look at any of the stuff having to do with the platform itself, just the application and the manner in which the application software was developed, that type of thing.

Attachment two shows one where we have a previously reviewed one, but they have made some changes to it. an example of this is the Oconee review we're doing at the moment where they have made some changes. And there we point out that only the items that have changed will require a review. The things that are still the same, process documentation and things like that that has not changed, does not have to be re-reviewed.

And then attachment three shows a full

blown -- this is a new application with a new platform. We haven't seen any of it before so we basically have to review everything.

We have a pilot project going on where we're trying to look at the possibility of having fewer things initially docketed. Where we are saying at the moment the ones that are the most important, the ones that will offer us the level of confidence is what will be initially reviewed. And there may be some backup documentation that will not be initially docketed, but in the process of our review if we determine we need these, we would then ask for them and get those on the docket. Or, if for example, we go on site, we're down to the local offices and read them there and say oh, this one is important. We would then say to them this one needs to go on the docket.

This is still a pilot. We're trying to see how it's working. We're using it right now with Oconee. And it's still very much trial and error. We're still working our way through it.

I mean, we have some stuff written on it, but nothing's set in concrete yet.

MEMBER BLEY: The criteria that leads you to decide what goes on the docket and not, you've just hinted if it's important. But does it affect the requirements of what people have to do to make the change if it's on the docket?

MR. LOESER: No. No. What they need to make the change, what the vendor uses and what the licensee uses basically is what good engineering practice says they should be doing, what various standards do. If you're dealing with high reliability software, you obviously can't go out and buy at a Radio Shack. You have to have a pedigree for it, you have to do configuration management, quality control.

For example, all your inputs and outputs from the various design phases under configuration management so somebody can't just arbitrarily go in and make a change, I think this would be a good thing.

What we're talking about is the documentation that we need to review to reach a determination of reasonable confidence. So we don't need all the design details. We may need some of them, but exactly what is needed is still up in the air.

We'll probably need all the plans that show finding to the right things. We may need some of the procedures. We may need some of the tests. But like I said, we're still working our way through it.

We've gotten about eight or ten of the major documents on the docket so far from Oconee and we're still doing our acceptance review. We have not yet started the heart, the meat of the thing. So we're seeing how this is working.

And I'm sure there are going to be things that we don't initially ask for that we're going to end up needing.  And we just don't know exactly yet what they are. And the list may be very different for different reviews of different complexities and different scope.

MEMBER STETKAR:  To come back to the international part of this thing. I'm familiar with a couple of plants in Europe that have, indeed, done the same thing that Oconee is doing with in fact the same platform. Have you had any interaction with international regulatory agencies to see what types of reviews and audits they've been doing or have done?  Because they have already implemented.

MR. LOESER:  Yes.

MEMBER STETKAR:  They're working at the plants.  Just to kind of gain some insights from lessons learned from what they've done.

MR. LOESER: Yes. For example, there's the difference between the review strategies and the final results between the Finn's review of the TSX and the French review of TSX where the Finns were significantly more picky.

We got a briefing a couple of days ago or last week from the Germans on what they consider are some of the requirements for safety systems, and it's quite different from ours.

We do talk to these people. I used to be a member of the IEC Committee on Nuclear Instrumentation and attended a number of the meetings.

so we do interface with them. But we have to remember the difference in regulatory requirements between them and us and sort of take this into account when we look at what we did. But, yes.

MEMBER STETKAR: I understand. It's just a matter of people have gone through this process, and learned a little bit based on --

MR. KEMPER: Bill Kemper again.

Yes, I looked into that myself also. And what I found is that the difference in the regulatory infrastructure, though, that exists between the various  country's regulatory process, if you will, lends itself to quite a bit of variability in actually what they reviewed, the level of reviews. Like EDF serves the French regulatory agency. GRS advises the German regulatory agency. Whereas, we do most of that stuff ourselves and we use our own internal Office of Research for some of those things.

So it really makes for a complex issue trying to read some kind of continuity in what's reviewed and the timing for the reviews and the level of detail that we need.

MEMBER STETKAR:  Thank you.

CHAIRMAN APOSTOLAKIS:  But you still can ask yourselves why are these people reviewing this particular aspect that we are not?

MR. LOESER:  Of course.

CHAIRMAN APOSTOLAKIS:  I mean, that's a kind of insight that's useful.

MR. LOESER:  And we do that. If you get right down to it, in the long run they review a lot of a similar stuff.

The Germans, for example, may ask TUV to do a much higher level of V&V than we do.

We have had a number of other various regulators come over here for a period of time, and

I've gotten to know them. And when we get told by a utility that the French said this or the French said that, I know a guy in France that I can call up and ask.  And this interpersonal relationships as well as the official relationships, we have official meetings --

CHAIRMAN APOSTOLAKIS:  Yes.

MR. LOESER:  -- on regular basis on a variety of levels, everything from the reviewers to Commission staff or Commissioners' meeting. Yes, we have a fair amount of interaction with the international.

CHAIRMAN APOSTOLAKIS:  Can we wrap it up now?

MR. LOESER:  We're done.  Any additional questions?

The last slide just says "Comments/Questions?"

CHAIRMAN APOSTOLAKIS:  Okay.  So we are done.

We'll talk about the schedule a little later, but we are planning to have a Subcommittee meeting dedicated on item 6 Review of Current Status of Traditional Methods Digital Reliability Modeling Research.  Because we were hit with a NUREG report that had 17 plus appendices; an exaggeration, but -- so I don't think it's fair to review that in two hours. And we may add other things as well. So that's why I'm a bit relaxed about the schedule.

You guys From Brookhaven probably will not have much of an opportunity today to present your work.

Steve?

MR. ARNDT: What we can do at the end. We've put together five or ten minutes at the end to talk specifically about schedule, both in terms of the Subcommittee and --

CHAIRMAN APOSTOLAKIS: Yes, we should this. Yes.

MR. ARNDT: -- talk to those issues.

CHAIRMAN APOSTOLAKIS: Because I really don't want to review such a massive amount of work in two hours. Okay.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: All right. So we will break now for coffee or whatever. Coming back at 10:40.

(Whereupon, at 10:29 a.m. a recess until 10:49 a.m.)

CHAIRMAN APOSTOLAKIS: Okay. We're back

in session. And now we are having?

MR. ARNDT: Glenn's going to give the primary presentation. We're now going to give you a presentation on the soon to be issued review guidance for new reactor digital I&C PRA.

CHAIRMAN APOSTOLAKIS: Okay.

MR. KELLY: And my name is Glenn Kelly. I'm with NRO. I'm in the Probability Risk Assessment Branch there.

And I just wanted to express my thanks to Cliff and Steven, the real experts in digital I&C. So if you have any hard questions, they'll be happy to answer them for you.

Just a little bit of background about Task 3 Working Group. As you know, NRC and industry currently are using a deterministic approach for handling the review of digital I&C systems to determine if they're acceptable. This has turned out to be very, very resource intensive. And the Commission has, through various means, indicated that it wanted the staff to evaluate whether or not to what extent it can risk-inform the process. And as part of that, they're seeking to provide early on better guidance for how to perform risk assessments for the new reactors in the area of digital I&C. And we've been told, following the June 7th Commission meeting, that we should be looking at operating experience and taking that into account in what we're doing.

The next slide.

In looking at risk-informing digital I&C, there are a number of significant challenges that we look forward to, hopefully, overcoming over time. One of them is the lack of consensus about how to perform modeling of digital I&C systems. In particular, common cause failures.

There is just not a lot of robust data from our standpoint, the staff's standpoint about digital I&C systems faults and common cause failures. Part of this is due to the fact that software keeps changing and so you don't have a long track record. Like, you don't have a piece of hardware that's been out there for 20 years and its been exercised so many times. Every time people make major modifications to the software, in essence you've got a new piece of software involved there.

Also, you have a lot of different applications being used and you reasonably that with each different application you have the potential for different common cause failures. Therefore, it's not clear that you can lump together lots of different applications and say this provides you with a good data source about common cause failures.

So we have uncertainties associated with modeling of these associated with the reliability of the systems. There some issues once you perform the additional I&C risk assessment, how you kind of stick that back in with the rest of the PRA, determine what to do with it.

And the Commission has said to us they want us in risk-informing to take into account the process of risk-informed decision making laid out in Regulatory Guide 1.174, the five principles and some of the other guidance there that's laid out there that's very important.

MEMBER STETKAR: Can I ask a question? I've had some confusion in my mind.

Could you in a nutshell identify the fundamental differences between the digital I&C system and a traditional analog I&C system and how the approach for modeling those things would differ in a PRA?

MR. ARNDT: There's been a number of different articulations --

CHAIRMAN APOSTOLAKIS: Microphone.

MR. ARNDT: I'm sorry. Okay.

There's a number of different articulations associated with that, and you can find those in some of the NUREGs that we've published, as well as other things. But in a nutshell the failure modes, if you will, are different or potentially be significantly different.

You have software which has different kinds of failure modes. You have more challenges associated with identifying failure modes.

You have issues associated with hardware/software interface.

You have, in some cases, timing issues, both internal and external timing issues as to how they interface with the different systems.

You have the fact that, for the most part, analog systems can be not necessarily or always are definitively tested or definitively established have a deterministic process by which you can predict their operation.

The other big issue from a reliability modeling standpoint is analog systems usually fail as associated with wearout mechanisms and things like that which have a fairly well established theoretical basis in reliability analysis. In terms of software driven systems, that's a much more challenging area and there's still a significant amount of debate as to whether or not you can even analyze digital systems in a way that you decompose software and hardware and hardware/software interfaces into separate components, if you will, or whether or not it doesn't make sense to do that and you actually have to do a more system based analytical process.

I don't know if I touched on all the --

MEMBER STETKAR: You kind of addressed a few things. And the point that I'm trying to make is having modeled analog instrumentation control systems for 25 years, most of the problems that you raised are precisely analogous in the analog system modeling world.

Identification of failure modes is something you struggle with. You worry about failure to operate, fails as is, fails high, fails low. Too much, too little.

MR. ARNDT: Yes.

MEMBER STETKAR: Failure causes is a different issue. We need to be careful between the difference between failure causes and failure modes.

Hardware, defining hardware, component boundaries and the interface between what we define as a thing, and I'll leave it at that, a hardware and the applicable data for that is something that we struggled with for 25 years in analog systems.

Those are not new problems. Those are not unique problems to digital I&C.  They're problems that we face and we have criteria and guidelines that tell us how to do that.

Something that is unique to digital I&C systems is software. And you've mentioned software many, many times. And I think it's really, really important when we start to talk about digital I&C PRA that we keep that differentiation in mind.

Are we talking really about the problems in digital I&C PRA?  Are they 99 percent related to the fact that we don't know how to do a reliability assessment of software or are they equally split between the hardware part of it, which is something that's wired together and in fact faces the same problems that we do in analog systems; that by the way we don't model very well these days anyway.

MR. ARNDT:  Right.

MEMBER STETKAR:  And that's what I'm trying to get an elaboration from you as far as where you see the distinction between digital I&C versus analog I&C.  Because I hear a lot of problems about this is a very complex topic, we have to have a lot of details, we don't know what we're doing. And I'd like to see a little bit more clarification where the real problems are in terms of methods and modeling approaches, if nothing else.

MR. ARNDT: Okay. You'll hear a little bit more about that this afternoon.

MEMBER STETKAR: Okay.

MR. ARNDT: In the Research aspect. To give you the 30 second answer, it's basically, at least the way I think of it is the primary issue is the software.

MEMBER STETKAR: Okay.

MR. ARNDT: But because you have the software/hardware interface, you run into a lot of secondary and tertiary issues associated with that.

Glenn mentioned it becomes that more difficult to do the data analysis because understanding how and if you can aggregate data when you have software and software changes and software interfaces is that much more difficult. When you try and do your deconvolution of systems it's that much more difficult to break hardware and software apart, if you can even do it.

So software is the big issue, as you have pointed out, is probably the majority of the issue. But it's also a problem associated with the secondary and tertiary issues associated with that.

MEMBER STETKAR: Thanks.

MEMBER SIEBER: The reliability part of the basic structure. For example, you have transducers which the failure rates of digital transducers about the same as analog transducers.

You have operators, which is about the same. The part that's different is the controller function. And one of the issues there is does a failure in some transducer someplace introducer a problem in the software that takes unexpected things out of service or puts them in a mode that is a failure mode. And that's what's different.

MEMBER STETKAR: That's right. But you're looking at inputs and outputs from software not as the focus of your reliability or risk assessment rather than looking at subdividing that transducer down into its piece parts and saying I don't have any data for those piece parts.

MEMBER SIEBER: Yes, right.

MR. ARNDT: And depending upon who you ask there is a more holistic challenge in that because of the nature of software it's that much more difficult to decompose systems. And this is something Professor Apostolakis --

MEMBER SIEBER: Right.

MR. ARNDT: -- and I and others have weighed in on extensively over the last couple of years.

MEMBER SIEBER: Okay. You can actually have a failure in part of your system and have the software good enough to cover it up if you're weakened at that point and your risk is laid out.

MR. ARNDT: Correct. And you can also have the converse. The software performed perfectly and you still have a system failure because --

MEMBER SIEBER: Right.

MR. ARNDT: -- of the design aspects of the software.

MEMBER SIEBER: Right.

CHAIRMAN APOSTOLAKIS: But we're now discussing the ISG.

MR. ARNDT: Yes. We're trying to.

MR. KELLY: Regarding the ISG, I did want to take one second to talk about the Regulatory Guide 1.174 process and some of the areas under that that are an issue --

CHAIRMAN APOSTOLAKIS: Now which slide

are you on?

MR. KELLY: This is slide 3 last bullet.

CHAIRMAN APOSTOLAKIS: Yes.

MR. KELLY: The purpose of the working group, I heard you were very knowledgeable in that area.

CHAIRMAN APOSTOLAKIS: True.

MR. KELLY: Yes. The purpose of the working group was to evaluate the feasibility of risk-informing digital system evaluation with the intent on improving the effectiveness and efficiency of digital system review. And, again, taking into account those five principles from Regulatory Guide--

CHAIRMAN APOSTOLAKIS: Your purpose was to evaluate the feasibility.

MR. KELLY: Right. Well--

CHAIRMAN APOSTOLAKIS: The answer is?

MR. KELLY: My answer would be that you can at this point, given where we are with modeling and data, you can evaluate at a high level the digital I&C systems and get a general overall appreciation of the level of risk that's associated with it, given the assumptions that you're making about the data failure rates.

CHAIRMAN APOSTOLAKIS: You seem to be a very nice fellow. I would say no.

MR. KELLY: Well, that's what I was coming to, but I was saying it nicely. Yes.

I mean, in essence, the answer is that at this point you have very high level risk insights and you can use it for much.

CHAIRMAN APOSTOLAKIS: You probably can draw insights for what's in there, but that's about it.

MR. KELLY: That's --

CHAIRMAN APOSTOLAKIS: Again, I'm speaking as a member of this Committee who will do his best to carry the information.

MR. KELLY: Well, this is an area where, apparently, we and industry differ significantly about this. And I'll let industry speak for themselves.

CHAIRMAN APOSTOLAKIS: I mean, you're going to come to that, right?

MR. KELLY: Yes. sir.

CHAIRMAN APOSTOLAKIS: The guidance of plain sensitivity.

MR. KELLY: Right. And we have NRO/NRR, Research people involved in knowing

CHAIRMAN APOSTOLAKIS: I do appreciate your problem though. Don't misunderstand me. I do appreciate you have a very difficult problem in front of you and you are trying very hard to do something reasonable about it.

MR. KELLY: We've quite a few public meetings. We've worked with industry attempting to really deal with this issue. They've provided us with white papers and we've had a lot of different discussions on things that we can do.

Our Task Working Group identified three major issues that we wanted to deal with, and these became problem statements 1, 2 and 3.

One of them is what we currently talked about, which is how to use current methods to model digital I&C for Part 52 PRAs.

Where possible, use risk-insights to improve operating reactor digital I&C reviews, that's task two.

And task three is see if you need to enhance the state-of-the-art.

So for Problem Statement 1, you know it was felt that there was not enough clarity out there about how to do the reviews.

CHAIRMAN APOSTOLAKIS: Well, I think if

we go back to slide 5, the last bullet: "Determine if it is necessary to enhance the state-of-the-art so that a comprehensive, risk-informed decision-=making process." Enhance the state-of-the-art, you include in this developing some sort of a method to quantify -- okay. Yes. Yes.

MR. ARNDT: Rephrase, it's basically --

CHAIRMAN APOSTOLAKIS: Yes, that's good. Yeah.

MR. ARNDT: -- what can we do in terms of the required PRAs in Part 52. Given the current state-of-the-art is there anything additionally we can do in terms of risk-informing. And then the last part is if you want to do a comprehensive review what more, if any, additional state-of-the-art improvements.

CHAIRMAN APOSTOLAKIS: Right. So you felt like adding a bullet that it is very easy to answer? Yes, good.

MR. KELLY: It was felt that the existing guidance didn't provide a lot of clarity. And so what we basically did is we took the work that had been done, in particular, on AP1000 and ABWR digital I&C PRA reviews and we incorporated that into this ISG. That information was also informed by additional work that's happened in the--

CHAIRMAN APOSTOLAKIS:  So you went back to the ABWR, you say?

MR. KELLY:  AP1000. It was really primarily from AP1000.  But also I did the ABWR.

CHAIRMAN APOSTOLAKIS:  Did you understand what the -- I mean I went back very quickly myself. And --

MR. KELLY:  Well, I talked to the gentleman who did the review.

CHAIRMAN APOSTOLAKIS:  Yes.

MR. KELLY:  And he explained it to me.  I didn't try to go back and read it.

CHAIRMAN APOSTOLAKIS:  Is this appropriate time to give you one number that I found there or later?

MR. KELLY:  This is fine.

CHAIRMAN APOSTOLAKIS:  In Chapter 26.5.4, well I have to tell you what it is, they say software common cause failure is 1.2 times ten to the minus six failures per demand and then quote "For software failures that would manifest themselves across all types of software modules derived from the same basic designed program in all applications."

I admit I didn't spend a lot of time

looking for the justification of this number, but it--

MEMBER BLEY: But that's not far from what I've seen for watchdog circuits.

CHAIRMAN APOSTOLAKIS: For what?

MEMBER BLEY: For watchdog circuits, the timing circuit failure, which does fail everything across the board if it fails. Within a factor of ten, that's what I've seen.

CHAIRMAN APOSTOLAKIS: But is there any justification for this number?

MEMBER BLEY: If that's what it's for, I think.

CHAIRMAN APOSTOLAKIS: There is? In your opinion or what?

MR. KELLY: In my opinion at this point the number is an educated estimate.

CHAIRMAN APOSTOLAKIS: Well, it says: "manifests themselves across all types of software modules derived from the same basic designed program in all applications." And one point two ten to the minus six failure per demand.

I mean, it seems to me numbers like that should be justified given some arguments. And the only thing I could find was a table where the number was listed.

MR. KELLY: I spoke to the gentleman who performed the review. And he said that he had gone to Westinghouse and spent about a week up there going over some of these things in detail with them.

I don't remember specifically discussing this number, and I appreciate that particularly with the specificity of the 1.2.

CHAIRMAN APOSTOLAKIS: We may have some enlightenment.

MR. BLANCHARD: Well, I'm not sure that I will enlighten things.

CHAIRMAN APOSTOLAKIS: Identify yourself, please.

MR. BLANCHARD: My name is Dave Blanchard. I'm from AREI. I'm working with the industry on this task work group.

I guess I would more like to ask a question. I understand your skepticism about a 1.2--

CHAIRMAN APOSTOLAKIS: No, it's not the .2 that bothers me.

MR. BLANCHARD: I think an equally important question is how important is that particular value to the results? How sensitive are the results to that value? Depending on the defense-in-depth and diversity that's in the systems, the plant systems in which that particular software application may be installed you may be able to vary that value orders of magnitude in either direction and have almost no impact on the results. So --

CHAIRMAN APOSTOLAKIS: I can see some value to that.

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: But, again, I don't even have to start with this. I can say, you know, what kind of a number would in this particular case lead to core damage? And you find the number, you well this is unreasonable. It's too high.

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: It couldn't be that high. I mean where engineers were careful and so on. But my fundamental problem is that these numbers are all over the place. And I don't know -- first of all, I don't know that I can take each one of them and start changing them. There is no basis for them as far as I can tell based on also the work that NRC has sponsored in various places.

So to go to an ISG that fundamentally asks you to do sensitivities studies, I'm having a problem with that. I would rather try to draw some insights, as much as I can, maybe doing nothing. This particular number would have to be .8 to do real damage, and we all know it can't be .8. That probably is a reasonable insight. But I do think the fundamental problem here, which comes back also to John's question and everything, is that we have a problem identifying the various failure modes. And if the PRA has done some work on that, then more power to it. We'll use that.

MEMBER STETKAR: Yes. That's what I was going to -- unfortunately, I don't have the experience. I haven't seen the AP1000 PRA, haven't been through that process so I'm totally clueless about what is in there and what is not in there.

One of the fundamental questions I had before we get into the sensitivity, the numbers part of the game, is backing up. Because I don't have that experience and you said that you're using the AP1000 experience as at least some input to your process.

How thorough was the AP1000 analysis process in the area of identifying failure modes? For example, I see a lot of things written about failure of the protection system to trip the reactor. Okay. That's an important function and failure to trip the reactor is an important failure mode.

If it's an integrated I&C system that in addition to tripping the reactor it does other things, did the AP1000 PRA systematically look at other types of failure modes, in particular spurious signals? Not failure to do the thing it was supposed to do, but doing other things that it could do unexpectedly; did it look at that? Because that I think is a key to what George -- that's my bigger concern in terms of the holistic picture of how you scope out one of these analysis.

I don't care so much about the details of the numbers, that tends to fall out.

CHAIRMAN APOSTOLAKIS: I don't remember whether they actually looked at spurious signals. I can give you the PRA for it, But the fundamental approach was fault trees.

MR. KELLY: Yes.

MR. KELLY: Yes. And they did it at a very high level. It basically was a top level thing and they said common cause failure, boom, I'm not. That's it.

CHAIRMAN APOSTOLAKIS: Okay. That's okay.

MEMBER STETKAR: Fault trees, I mean if I can identify a spurious failure mode, I can build a fault tree to do that. If I don't try to identify the spurious failure mode, then I don't build a fault. The fault tree will not identify it for me.

In terms of the staff guidance, getting back to kind of high level things what do you look for, I think that this is an important area of the risk assessment process that the staff should be -- probably more important than is 1.2e to the minus six or 1e to the minus five for a particular number in there. And is there a systematic and relatively comprehensive methodology employed to identify failure modes?

We do that theoretically with analog I&C systems. I say "theoretically" because what we find, again, when we do fire analysis we suddenly need to think about, oh, these spurious signals that the traditional analog I&C models have not thought about because they've wished away because they're insignificantly small.

So in terms of guidance for staff review, I didn't read very much in this document at that level to say has the PRA essentially scoped--

MR. KELLY: There's two places. I'll tell you -- a good question.

The review guidance aspect of the ISG is broke up into two sections. The first is a section the expectation of where if I'm doing a more focused review. Because understanding that I came into this with a lot of PRA experience and very little digital I&C experience. It took me a lot of time to understand what was going on and where the issues were.

Part of this document is there to help provide the reviewers with a better understanding about what are some of the issues that digital I&C can bring up. But this is broken down into two review areas. In essence if I have a more focused review and then if I have time to do a more detailed review.

So under the focused review number 11, which is somewhere around page 10 on your copy, it says --

MR. ARNDT: Background material, not slides.

MR. KELLY: Yes. In the ISG itself it says "Examine the applicant's documentation to ensure that the dominate failure modes of the risk assessment are documented and described in..." That just says make sure that they put down dominant failure modes.

Now when you go back, if you have more time because this is something that takes a lot of time to do.

CHAIRMAN APOSTOLAKIS: That's number 11?

MR. KELLY: Yes.

MR. ARNDT: That's number 11.

CHAIRMAN APOSTOLAKIS: and I have a comment. Right there. How are there determined?

MR. ARNDT: There you go.

MR. KELLY: Right. Well, that's --

CHAIRMAN APOSTOLAKIS: This is the heart of the problem and that's why we're scheduling a separate Subcommittee meeting to meet with Brookhaven.

MR. KELLY: Right.

CHAIRMAN APOSTOLAKIS: And I see Brookhaven already wants to say something. Is it okay to let say now?

MR. KELLY: Sure. Sure.

CHAIRMAN APOSTOLAKIS: Okay.

MR. MARTINEZ: My name is Gerardo Martinez. I work for Brookhaven National Lab.

As part of our project I looked at the PRA modeling of some digital I&C systems of the

AP1000. And something that I found again and again is that many of the values, many of the arguments that they do are based on documents which are not included in the PRAs.

CHAIRMAN APOSTOLAKIS: Yes, I noticed that.

MR. MARTINEZ: They refer to other proprietary documents and so on. So for somebody who doesn't have access to those documents, as far as I can tell, it's practically impossible to tell what is the basis for those --

MEMBER BLEY: I take it you did not have access to those?

MR. MARTINEZ: I didn't have access.

And another important aspect, shortly before you were talking about failure modes and the ports defined for your modes. In AP1000 PRA they say that they did a failure modes and effects analysis. But the FMA itself is not included, as far as I remember, in the PRA.

I suppose that the NRC staff who reviewed the PRA had access, but otherwise it's practically impossible to tell.

CHAIRMAN APOSTOLAKIS: Okay.

MEMBER STETKAR: I hope you're going to

get to number 1 in your detailed review. If you're not --

CHAIRMAN APOSTOLAKIS: Number 1 you mean of the 11?

MEMBER STETKAR: On page 11.

MR. KELLY: Yes. Okay. And that's --

CHAIRMAN APOSTOLAKIS: Wait a minute. There's an additional comment.

MR. BLANCHARD: Yes. Just excuse me one additional thing.

CHAIRMAN APOSTOLAKIS: But, first, repeat your identification.

MR. BLANCHARD: This is Dave Blanchard. I'm from AREI.

The main differences between analog and digital systems is the software and its failure modes. And the uncertainties are not only in the probabilities, but they're also in the failure modes.

CHAIRMAN APOSTOLAKIS: Sure.

MR. BLANCHARD: And to the extent that you don't understand all of the failure modes, we need to keep in mind the software by itself does not do anything in terms of mitigating plant accidents and transients. It has to actuate a equipment.

We do know the failure modes that we are concerned about in the plant equipment that the digital I&C controls. And to the extent that we're uncertain about the effects of the failure modes of the digital I&C, we can make sure that we have provisions in the plant design to address the failure modes of the mechanical and electrical equipment that we're concerned about.

CHAIRMAN APOSTOLAKIS: But isn't that were another activity of the staff looking at operational experience comes into the picture?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: To confirm or modify your statement. And the staff is doing a lot of work on that, and we have a presentation.

MR. BLANCHARD: And so is EPRI.

CHAIRMAN APOSTOLAKIS: So is EPRI? Okay.

MR. BLANCHARD: All right. But we got to recognize there's not only uncertainties in the probabilities. There's also uncertainly in the failure modes. And you could design your digital systems and the diverse actuation systems in a way that address those uncertainties such that understanding the precise numbers isn't particularly important, and understanding the precise details of the failure modes may also not be very important.

MEMBER STETKAR: I'm not sure about the second part of that.

MR. BLANCHARD: All right.

MEMBER STETKAR: Because I think understanding the precise details of the failure modes is absolutely important. That's a whole challenge. I don't care if it's complicated, PRA is not a simple process.

MR. BLANCHARD: Right.

MEMBER STETKAR: We started developing PRAs back 30 years ago or more and everybody said this is such a complicated process you can't do it. Well, the fact of the matter is you can. But what we've learned is that a clear delineation of the possible -- possible, not most likely, possible failure modes is essential.

MR. BLANCHARD: But remember you can translate those failure modes --

MEMBER STETKAR: That's right.

MR. BLANCHARD: -- of the digital I&C system into mechanical and electrical equipment --

MEMBER STETKAR: That's right.

MR. BLANCHARD: -- that you're controlling, and that is already modeled in the PRA.

MEMBER STETKAR: If it is modeled in the PRA; that's my whole point. If you've modeled a flow control valve that is supposed to open in response to the safety signal failure to open --

MR. BLANCHARD: Yes.

MEMBER STETKAR: -- suppose that the digital signal closes it? Have you modeled the spurious closure in the PRA to allow you to quantify the likelihood that that occurs across the board?

MR. BLANCHARD: And your analogy to the spurious actuation scenarios that we're having to deal with in the fire PRA today is very appropriate.

MEMBER STETKAR: It's totally analogous. A fire is performing the surrogate of that smart--

CHAIRMAN APOSTOLAKIS: I think this is getting to be too detailed now. It's very instructive, but we will come back to this. Don't worry.

MEMBER BLEY: I would just like to ask a simple question. I know we have AP1000, what other PRAs of digital systems are out there that you know about and have had a chance to look at?

MR. KELLY: Well, we have the ABWRs.

CHAIRMAN APOSTOLAKIS: ABWRS.

MR. KELLY: Which I reviewed, which was

very high level and basically said come back when we build it and we'll let you know --

MEMBER BLEY: Okay. That's wasn't very helpful.

MR. KELLY: No. And --

CHAIRMAN APOSTOLAKIS: The ASBWR now.

MR. KELLY: ESBWR has more detail, I understand. That it's the most detailed one that's come in so far.

We had a C-SAR AD Plus, which was at a fairly high level, similar to AP1000, maybe a little bit less. But those are the only one --

CHAIRMAN APOSTOLAKIS: I think the two that have been certified are the ABWR and the AP1000. I don't know whether system 80 plus, had digital. Does anybody know?

MR. KELLY: Yes, it did.

CHAIRMAN APOSTOLAKIS: Okay.

MEMBER BLEY: He said it was very high level.

CHAIRMAN APOSTOLAKIS: Okay. But these are the three have been successful.

MR. ARNDT: There has also been a number of PRAs that have attempted to analyze digital systems in foreign plants. And we've looked at some of them. Again, most of those were done at a fairly high level.

MEMBER BLEY: It sounds like that's kind of the picture.

MR. ARNDT: Yes.

MEMBER BLEY: So far they've all been done at a fairly high level.

MEMBER STETKAR: George --

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: But there are certain exceptions.

MEMBER STETKAR: Can we get back to the -- I'm assuming you're going to talk about that item 1.

CHAIRMAN APOSTOLAKIS: Well, the whole list, I hope.

MEMBER STETKAR: Well, we will. But this is a good example of --

CHAIRMAN APOSTOLAKIS: Okay.

MEMBER STETKAR: It's kind of relevant.

MR. KELLY: Okay. Further in the slides there is a listing, just to let you know, of kind of general review areas.

CHAIRMAN APOSTOLAKIS: Where are you? Which slide?

MR. KELLY: I'm starting on slide 10. We're on slide 6 right now.

CHAIRMAN APOSTOLAKIS: And I'm looking at the guidance itself that says on page something that to ensure the risk contributions -- ah. The review should consider the following steps, and then it's 1, 2, 3 --

MR. KELLY: There's 14.

CHAIRMAN APOSTOLAKIS: Fourteen. Are you going to go over them? I think you're referring to step 1, aren't you?

MEMBER STETKAR: Well, no.

MR. ARNDT: He's gone to the next level.

MEMBER STETKAR: Let me just get through this so we can get back to the slides.

CHAIRMAN APOSTOLAKIS: Okay. Okay.

MEMBER STETKAR: Number one, items number 1 on the additional steps, which you said are applicable only -- only if you're going to do a very, very detailed review.

MR. KELLY: Right.

MEMBER STETKAR: Number 1 says the modeling of digital I&C should include -- should include the identification of how digital I&C systems can fail and what their failure can effect, and then it goes on.

MR. KELLY: Right.

MEMBER STETKAR: Now why is that reserved to a detailed review? That's a fundamental element of any type of review, and as are many of these things pulled out in the detailed review.

One of my problems was, and I don't know if you're going to address it later and if you are, stop me and we'll talk about it then. Is that many of the 14 big ticket items that would be done in any review are very, very strong -- are too simplistic compared to the detailed review. And I recognize that you won't have the resources at the time to go into excruciating detail.

MR. KELLY: Right.

MEMBER STETKAR: But as a fundamental element of the high level review identifying the completeness of modeling failure mode --

MR. KELLY: When I did ABWR we took three years. Every six weeks I was flying out to General Electric to --

MEMBER STETKAR: And, obviously, you can't do that.

MR. KELLY: Right. Yes.

CHAIRMAN APOSTOLAKIS: Mr. Hossein?

MR. HAMZEEHEE: Yes, Hossein Hamzeehee, Chief PRA Branch in Office of New Reactors.

Well, I just want to make sure because there has been a lot of work in this area and a lot of issues that may or may not be related really to how we put together interim staff guidance for review of the new reactors digital I&C PRAs.

Now when we do review these things, we have scope of our review. We're not going to do a detailed review of every single line item of the PRAs because by the new ruling Part 52 we're expecting the industry to follow the standards that exist or will exist prior to the initial fuel load.

so, in other words, if there is an ASME standard that says how to do level 1 PRA and the licensee or the applicant says I followed the guidelines in the ASME standard, then we're just going to do spot check.

CHAIRMAN APOSTOLAKIS: But there is no standard on I&C?

MR. HAMZEEHEE: No, I understand now. In the way back, not to digital I&C, then there are issues in the digital I&C that have not been resolved yet. And the PRA practitioner in the NRC that is reviewing that portion is going to have a lot of challenges in front of him, and he's not going to be given unlimited amount of time just to focus on digital I&C portion of the whole PRA status.

So what we try to accomplish in this I&C is to see how the best to spend his time focusing on what is important in digital I&C within his limitation of time and resources.

CHAIRMAN APOSTOLAKIS: That's good --

MEMBER STETKAR: I understand that, Hossein. And let me give you a couple of analogies.

At your high level if somebody presented to you a level 1 PRA and had a list of initiating events and had no LOCAs in that list of initiating events, you would say that's a fundamental deficiency?

MR. HAMZEEHEE: Correct.

MEMBER STETKAR: If somebody presented to you, recognizing there aren't formal standards yet, but if somebody presented to you a PRA of fire events and did not address the issue of hot shorts, you would probably say that that was deficiency?

MR. HAMZEEHEE: An issue, yes.

MEMBER STETKAR: My whole point is that without a detailed reviewed of the models if someone presents to you a PRA that includes digital instrumentation and control systems and it has not addressed a comprehensive treatment of the possible failure modes, not looking at details for a particular valve or a particular pump, but to tell you the process by which they identified that failure modes to show you that process, that seems to me to be a deficiency. Because we know that there are interactions between software and hardware that can excite --

MR. HAMZEEHEE: Yes.

MEMBER STETKAR: -- a variety of failure modes.

MR. HAMZEEHEE: Correct.

MEMBER STETKAR: Not necessarily within the details of the digital I&C. Because recognizing the industry comments that these failure modes are only important as they're reflected through the operated equipment.

MR. HAMZEEHEE: Correct.

MEMBER STETKAR: So that's my point. I recognize the problems that you're facing, but in terms of scoping your review and providing guidance for what a reviewer should be sensitive to --

MR. HAMZEEHEE: Yes. However, for instance, what I would like to say I completely agree with you. But if you go to page 10 of the ISG number 11 at the high level that is enough for the reviewer to make sure that they have done that.

Now, if he finds problems, then he should go into more detail and find out --

MR. KENYON: No, it's not. Because 11 says: "Examine the applicant documentation to assure the dominate failure modes are documented."

CHAIRMAN APOSTOLAKIS: How the hell do you know? You don't know.

MEMBER STETKAR: Well if I put into my model failed to start, and that comes up as important, that is a dominant failure mode. If it does not come up as important, it is not a dominate failure mode.

If I do not insert in my model failed to run at all, it will never appear as a dominant failure mode.

MR. HAMZEEHEE: Correct.

MEMBER STETKAR: Perhaps it is the dominate failure mode, I just didn't put it in my model.

MR. HAMZEEHEE: No, but you --

MEMBER STETKAR: So how do you know by looking at risk importance measures or cut sets or whatever, how do you know that the model has completely addressed the possible failure modes?

MR. HAMZEEHEE: Correct. But what I --

CHAIRMAN APOSTOLAKIS: In question here is since there is a serious question regarding the validity of the numbers, how can we talk about dominant numbers?

I think we're on the same page here. We do want to have something that is sufficient --

MR. HAMZEEHEE: Correct.

CHAIRMAN APOSTOLAKIS: -- and reasonable. It's a matter of emphasis. And, you know, those 17 -- is it 14?

MR. KELLY: Fourteen.

CHAIRMAN APOSTOLAKIS: Fourteen items and the ten that follow, perhaps there ought to be some rearrangement.

MR. ARNDT: Sure.

CHAIRMAN APOSTOLAKIS: That's all we're saying.

MR. HAMZEEHEE: All right.

MEMBER STETKAR: The ten, by the way, I think are great.

CHAIRMAN APOSTOLAKIS: But they're greater than 14 or not.

MEMBER STETKAR: Well, the 14 are too truncated, basically.

CHAIRMAN APOSTOLAKIS: I think we should let Glenn resume and interrupt him 10 seconds.

Okay, Glenn. You have presented before the ACRS before, right?

MR. KELLY: A lot of times.

CHAIRMAN APOSTOLAKIS: So you know. He's a veteran. You get the special treatment today.

MR. KELLY: I appreciate it.

CHAIRMAN APOSTOLAKIS: Well, the other two ISGs were sort of dull. This is really interesting.

MR. KELLY: I know.

CHAIRMAN APOSTOLAKIS: They were just straightforward.

MR. KELLY: I just want to go back again because we broke this up into two parts. And I want to have an appreciation for why we did this. And I understand why you're saying that, and if I had an unlimited or virtually unlimited amount of time, that's what I would do. Because when you come down to it, it's driven by the bottom line. The bottom line is I don't know that the numbers are any good and I don't know that I've got the failure modes.

Okay? That's the reality of the situation right now.

CHAIRMAN APOSTOLAKIS: That's very good.

MR. KELLY: Okay. So if I spent a little bit of time or I spent a lot of time on it, I'm not necessarily going to know much more about the risk associated with a digital I&C system. So I looked at this and I said what is it that you can get out of this? I said I'm going to run these sensitivity studies. And the sensitivity studies are going to help me to understand what is it about my system, hopefully, that I got semi-decent modeling at least there that it's going to tell me that I want to make sure that I'm capturing this maybe in my RAP program or my maintenance rule, or someplace that I'm going to be picking this up and making sure that this is getting covered under some treatment. Because I can't trust the numbers that come out --

CHAIRMAN APOSTOLAKIS: Well, let me tell you what the problem with that is. First of all, there's a practical problem. The moment you guys start playing with these numbers, indirectly you're blessing them. And I don't like that.

The second is that kind of approach really assumes that there is a piece of component here that's called software and it has a failure rate. And I play with it, and if I have two of them, I have a common cause failure rate. The problem with that is that if you don't understand the failure modes, you know, you can't really say that the software is a separate component. It's embedded everywhere.

MR. KELLY: I know.

CHAIRMAN APOSTOLAKIS: And it can do all sorts of crazy things if it goes wrong. So that we miss.

So what I think we should do in the remaining time is to go over the 14 and then the ten and get the Committee's views, the individual member's views. And then you decide what to do with those, rather than go with the slides which I believe are fairly high level.

So I would start with number one of the 14.

MR. KELLY: Okay.

CHAIRMAN APOSTOLAKIS: I mean this is the heart of the matter, right; the 14 plus the 10?

MR. KELLY: Yes. I mean that's what people are going to --

CHAIRMAN APOSTOLAKIS: Yes. And that's why we have Subcommittee meetings.

MR. KELLY: Okay.

CHAIRMAN APOSTOLAKIS: To give you pleasure.

MR. KELLY: Number 1.

CHAIRMAN APOSTOLAKIS: Number 1.

MR. KELLY: Number 1 basically don't do this all by itself. This is part of your overall PRA and you should take into account the details and other things of your regular PRA, the level of review. And this is the other aspect down here. The level of review should be proportional to the use that the applicant plans on using the additional I&C system's insights. Digital I&C system risk assessment insights. I didn't say that very clearly.

But if the applicant comes in and says look, I want to use this, I'm going to use that on the 6059, I'm going to use it under a whole bunch of different places. And I'm going to say now my digital I&C system because my risk assessment says I don't need this because it's not important or it's very important, or whatever, these are things that now I want to look at and I'm going to say okay now this makes -- as a reviewer it's incumbent on me to put more attention to that review if I'm going to use it for theses kind of risk-informed decision than if

I'm saying I'm just getting some general high level insights. I'm making sure that I meet the safety goals, et cetera.

CHAIRMAN APOSTOLAKIS: So this is it fair to say that number 1 really requires the reviewer to familiarize himself or herself with what has been done, what does the licensee say about the digital I&C and so on.

MR. KELLY: Right.

CHAIRMAN APOSTOLAKIS: So it's a fairly innocuous thing?

MR. KELLY: That's correct.

CHAIRMAN APOSTOLAKIS: Is there any objection to it?

MR. KELLY: Right.

MEMBER STETKAR: And it's more than innocuous. I mean, it says you have to look at it as an integrated part. That's the important part of this. You can't just look at, like we used to in auxiliary feed water system --

CHAIRMAN APOSTOLAKIS: No, that's fine. That's fine. Okay.

Do we move on to number 2?

MR. KELLY: Right. Let me also note here --

CHAIRMAN APOSTOLAKIS: Okay.

MR. KELLY: -- In doing this review, this is a review that is a review, in essence, Chapter 18 review. This is not a Chapter 7 review. This is not saying whether the digital I&C system is good enough to meet the regulations under Chapter 7. It's saying are we seeing anything here that's going on here that's going to affect the safety goals or things like that; that's primarily what we're looking at right here.

CHAIRMAN APOSTOLAKIS: Now, moving on to number 2. My view is, and I'm sure others will give you their views, I would completely believe it and I would take number 1 from the ten items and make it number 2 here.

In other words, jump into the failure mode issue as a second item.

MEMBER BLEY: I certainly liked elevating that one to number 2 here, deleting everything that's here I'm maybe not --

CHAIRMAN APOSTOLAKIS: Okay. So there are two motions. There are two motions. One is to move item 1 from the list of ten and make it number 2 here, which really essentially says look for failure modes and then we'll think about the current 2.

MR. HECHT: Can I ask a question?

CHAIRMAN APOSTOLAKIS: You can always ask.

MR. HECHT: Ask of the Distinguished Chairman, Subcommittee.

Let's just say that we have a standard platform, you know the Triconex, TMSR was mentioned, a number of others that might come in. If we had one of those and the applicant was planning on using that, would you still say that it's necessary to go into the depth of review?

CHAIRMAN APOSTOLAKIS: Yes. Because -- go ahead.

MEMBER STETKAR: I think it's important to differentiate between internal failures of the digital I&C system if you want to call that a box and how that interacts with the rest of the plant.

I don't particularly care in a risk assessment what happens inside that box, whatever you call it, as long as the effects of those malfunctions are not important to the operation of my power plant.

So if that pre-approved design are recognized, you may not need to go look at the details of the internals of that. But the actual application of that and the particular failure modes that it may cause within the system, valves opening/valves closing, pumps starting/pumps stopping, displays in the control room going high, low, staying the same may be very, very different from application-to-application.

MR. HECHT: Right.

MEMBER STETKAR: Unless you have a standard plant design.

MR. HECHT: I guess the point is is that when we speak about failure modes and effects, an effect at a low level becomes a failure mode at a higher level, you know.

When we speak about computers the failure modes that I use, at least, are stop, hang, crash, late result, early result, incorrect result; things like that. And those are pretty general. And I would propose that those are the failure modes that may be common across all applications that are using a single platform. And that if we know those, that that be defined. And I thought that was the intention of point 11 when it was first discussed. I mean, I thought the point was is that you knew something about the platform that you were running on.

MR. ARNDT: The concern here is that the

review from a deterministic standpoint of the acceptable of a platform basically is against whether or not it is we have an adequate assurance that the system will perform.  That may or may not get to all the different failure modes.

The idea of the deterministic review is to evaluate possible failures and ensure that there's a low likelihood that will happen.

As was pointed out by John, is there is a number of different kinds of failure modes depending upon what kind of system it is being used for.

MR. HECHT:  Right. So we're talking about a top down analysis, basically what you're saying.

MR. ARNDT:  Yes. Yes.

MR. HECHT:  So I guess my point is is that when we speak about digital I&Cs -- I mean computers.  Let me just talk about computers. There's an awful lot about computers that crosses systems, crosses domains, crosses a lot of things.

MR. ARNDT:  Correct.

MR. HECHT:  And that when we start thinking about those, just as we think about a resistor having two failure modes, open/short and then we propagate that up, that we have to I think abstract the computer part of the digital I&C system and also the network part of the I&C system. People aren't talking about smart sensors and data highways, or whatever they call them in this field, field buses, whatever they call them here, in that as well. And if we can abstract that part of it and then move those into the appropriate level of the fault tree, that we might be better off.

CHAIRMAN APOSTOLAKIS: So let me understand what you're saying here. If there is a platform that has been reviewed by the NRC, right? You have done that to two or three of them?

MR. KELLY: Yes.

CHAIRMAN APOSTOLAKIS: And it has been approved, then I get a design of a new reactor and they say we are using for the digital I&C this platform, what exactly are you saying? That in identifying the failure modes I don't have to worry about the platform itself because it has been approved already?

MR. HECHT: No. No.

CHAIRMAN APOSTOLAKIS: Or should I revisit the platform? I'm trying to understand what you're saying.

MR. HECHT: This is perhaps the biggest difference. I would call it a modularization, if you will.

CHAIRMAN APOSTOLAKIS: Okay.

MR. HECHT: Okay. We have to think about how we break the problem up differently in digital than analog. So the issue is that we still have to do the fault tree, we still have to address the system impacts and when we think about failure of a system for example to actuate, we have to break it down. But when we say "a computer doesn't work" or "a control system doesn't work," then that's when we have to think about the ORgates that have all of those failure modes in them. And at that point those ORgates and that part of it might be standard.

CHAIRMAN APOSTOLAKIS: I see.

MEMBER STETKAR: Yes. And that's one of the things that when we ever have the meeting on the NUREG that I wanted to bring up. Because back, again, 25 years ago and to some extent still we're struggling on what is a diesel generator. I can subdivide a diesel generator into thousands of different piece parts, all of which if I do enough searching, I can find numbers for and develop a huge fault tree for just failure of a diesel generator to start. However, what we've done in the industry over 25 years is with reasonable success we've identified a diesel generator; what is within the component boundary of a diesel generator. We mean that it includes all of these things. People who compile the failure data are cognizant of that component boundary so that when we compile the data and model this module that we call a diesel generator, we have reasonable assurance that we've captured all of this equipment.

And I think what you're talking about in terms of modularizing the internals, if that's possible of a preapproved design, is worth a lot of miracles. It will save a lot of this developing a huge fault tree for a thousand different piece parts of a diesel engine.

MR. HECHT: Right. Right.

MR. KELLY: And I would note that that's a wonderful thing --

MEMBER STETKAR: But that's not necessarily--

MR. KELLY: -- but would not go in this ISG. Because this is for current, you know based on what we know today, what we have today, where we are today. And we're not at that point today for these modules.

MEMBER SIEBER: I see.

MEMBER STETKAR: That's right. But what I was talking about earlier at a failure mode an effects analysis is at a higher level.

MR. KELLY: Right.

MEMBER STETKAR: In other words, I don't care about the level of detail of modeling of the diesel generator. I care does the diesel generator fail to start, does it fail to run, if it's applicable does it start spuriously, if it's applicable does it deliver half of the output voltage if that's an applicable failure mode. It's a high level of completeness in the failure mode.

MEMBER BLEY: Yes. I have a question. If I followed everything you said, it seems to me for certified designs we should already have known and identified those large level failure modes.

MR. HECHT: If it has been done, if it has been broken up so that the computer is separated from the system.

MEMBER BLEY: And I don't know if that's true.

CHAIRMAN APOSTOLAKIS: I don't know either.

MEMBER BLEY: Because I haven't looked through any of those factors.

CHAIRMAN APOSTOLAKIS: Steve probably knows.

MR. ARNDT: It was not the intent of the review.

CHAIRMAN APOSTOLAKIS: Which review now?

MR. ARNDT: The review to approve a visual platform.

CHAIRMAN APOSTOLAKIS: So we don't have then a set of potential failure modes --

CHAIRMAN APOSTOLAKIS: We looked at the potential failure modes associated with the system, but the intent of the review was not to identify failure modes and put them into categories for review. The intent of the review was to determine whether or not it was an acceptable platform and we had a reasonable assurance that met our safety --

CHAIRMAN APOSTOLAKIS: Which is fine, because at that time you were not thinking in terms of future applications. But my question now is it looks like this is a very important area.

MR. ARNDT: It is.

CHAIRMAN APOSTOLAKIS: Should the agency have a research task someplace to try to pull all this together?

MR. ARNDT: Some of that information will be derived from some of the ongoing research. It's not specifically focused towards that particular task. But if you look at the work that is ongoing in the reliability area at Brookhaven, OSU and the work on testing methodologies that is ongoing at the University of Virginia some of that is focused toward a better understanding of how it can fail and it cannot fail.

CHAIRMAN APOSTOLAKIS: I understand that. And there will be a lot of insights and partial twos for doing certain things. But what I'm thinking is that maybe we need somebody to take the pattern failure modes that, say, Brookhaven is doing, the other one that Virginia is doing, the other one that OSU or ASCA, or whatever and create a package bringing the best features of these diverse methodologies, a package that will help Glenn in his work.

MEMBER BLEY: Best in terms of future use.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: Yes. Yes. Because, again, I mean if you read any one of these reports the investigators really want to get down to estimating probabilities. They're doing a good job on the failure modes, but that's not their focus. They really want to get the Nobel Prize on probabilities. So you need somebody who focuses on the failure modes and also really does a critical evaluation of how good is this particular approach. Can this other method supplement it? Are they doing the same thing? Are they doing slightly different things?

Because the issue of failure modes, I think it's developing into a consensus, is really a very critical one here both in the PRA efforts but also in regulatory space where you have to make some decisions interim or long term.

So I would strongly suggest that you guys think about that. You know, to have somebody that pulls everything together.

MR. ARNDT: We will discuss that with our regulatory brethren, or rather our Research brethren.

CHAIRMAN APOSTOLAKIS: I never expected to get a definitive answer in a public meeting. I've been on this Committee for too long. But as long as you guys say that you will think about it, I'll be happy. Okay?

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: All right. So we

all agree then that item 1 from the list of ten should be moved up. I know that you are --

MR. KELLY: No, I didn't -- the problem -- I mean as a reviewer I looked there and I said there's no standard list --

CHAIRMAN APOSTOLAKIS: There is not. That's correct.

MR. KELLY: -- for failure.

CHAIRMAN APOSTOLAKIS: That's right.

MR. KELLY: If I take one of those PRA reviewers off the street, you know they're all out there, and you pull them in and you say okay, name me the failure modes for this particular model, the guy has no clue.

CHAIRMAN APOSTOLAKIS: Of course not.

MR. KELLY: He's not going to understand. It's going to take  a lot of time for that reviewer. And these reviewers don't have a lot of time available.

MEMBER BLEY: Well, I think this fits into the mode we were talking earlier with the people who -- you know, we're going to have QA people out in the regions who are going to have to come up to speed on I&C to be able to do their job in the future. And that's going to be true for the PRA people as well.

Maybe it's not within the next three months, but it should be in the plan to work those things out and have that kind of training available.

CHAIRMAN APOSTOLAKIS: By the way, just a clarification. When I say "move this there," that doesn't mean that some appropriate wordsmithing will not take place. I don't mean verbatim. It's the idea--

MR. KELLY: Right.

CHAIRMAN APOSTOLAKIS: -- of failure modes. Now you may want to think again about what this means, what this and that -- we can work --

MR. ARNDT: We understand.

CHAIRMAN APOSTOLAKIS: Yes. Yes. Okay.

John?

MEMBER STETKAR: I think more what I was talking about, recognizing you have limited time but again at a high level. If I'm doing a review of a current PRA, somebody has a systematic process of identifying for example initiating events. Let's separate this from digital I&C for the moment. And they have a list of 150 possible detailed initiating events. Well, I don't have the time to look at each one of those. I don't have the time to think about the plant and the design to know if they should have had 151 and of 150. However, I can look at their process and see how they grouped them together, see whether the general list seems to make sense from my experience and from the guidelines that I have available. Have they looked at LOCAs, have they looked at transients, have they looked at support system failures, what types of support system failures, for example.

At that level of review in terms of looking at failure modes, it's incumbent upon the people doing the PRA to convince you that they've had a systematic process to identify the possible failure modes and if they've coalesced them, if they've simplified them the process by which they've done that. Does that process at least exist and can you convince yourself that it seems reasonably completed based on what I know.

Granted, you don't have time to go in and look to see if there are 15 different possible failure modes for some software element.

MR. KELLY: Okay.

MEMBER STETKAR: It's their job to do that.

CHAIRMAN APOSTOLAKIS: Okay. Shall we move on then to the second part of my motion?

MR. KELLY: Okay. And I would just note also that these numbers like 1 through 14 and 1 through 10, it's not like number 1 is the most important, number 2. They're just listed in there.

CHAIRMAN APOSTOLAKIS: Okay. So my second recommendation is that this number 2 of the 14 which plays games with the probabilities should be either deleted completely or replaced by a sentence that is appropriately vague and talks about possible insights that one might draw and having a very strong statement that the state-of-the-art is very fluent there and we really don't have good methods justifying numbers like this.

MR. HECHT: Can I offer an insight?

In the part of the world that I work in we have this process --

CHAIRMAN APOSTOLAKIS: Which is?

MR. HECHT: Well, aerospace and defense and things that kill people.

CHAIRMAN APOSTOLAKIS: As opposed to --

MR. HECHT: In the reliability discipline what we have is a process called allocation, reliability allocation or probability allocation. And I think that's what you're trying to get to here.

You're trying to say given a certain top event or certain set of events of concern, what is the maximum probability that you can tolerate. And while you may not be able to predict the probability of a specific system, you can certainly do a better job of saying whether or not you're at or below that limit.

CHAIRMAN APOSTOLAKIS: This is similar to what we were discussing earlier with that gentleman that the probability should be point date --

MR. HECHT: Right. Right.

CHAIRMAN APOSTOLAKIS: -- but you know it's not point date.

MR. HECHT: Right. I wanted to make the point at that time, but I couldn't.

CHAIRMAN APOSTOLAKIS: Right. But is this, though -- first of all, I think this is something to be explored. But the question is whether this belongs to the ISG or to the research projects that are trying to quantify.

When we have a Subcommittee meeting discussing, for example, the Brookhaven work where they really try to come up with probabilities, then maybe we can raise that issue again.

MR. HECHT: I would say that it's perhaps both. And the reason is is that the applicant has a specific system or system or subsystem that does certain things.

CHAIRMAN APOSTOLAKIS: I can agree with that, yes.

MR. HECHT: And the idea is that ultimately you're talking about a core damage frequency or a probability of a release at the boundary, or whatever it is you're looking at and at that point it should be related to that.

MR. ARNDT: Yes. At the risk of extending this beyond where it needs to be, it's a little more than just allocation, though. Because by doing this you're trying to understand not only how important it is in a generic sense, but how important it is compared to other systems or compared to the safety goal or things like that. It's a little bit more you're trying to get insights associated with if you put more defense-in-depth in, is it going to make it less of a problem or if you put other systems in, or how does it relate to other systems and things like that.

CHAIRMAN APOSTOLAKIS: You spoke the magic words "defense-in-depth." The way I see this this is guidance that we'll utilize whatever insights we can get from the PRA in this area to make sure that our defense-in-depth measures are appropriate. This is really the ultimate goal. Because we know we cannot truly risk-inform this process. So, you know it's a risk-informed process in some sense, but not so much based on the numbers that these people are producing.

So especially, you know, 2A, 2B increases software failure probabilities, I would take all this stuff out.

MEMBER STETKAR: Well, there's even some guidance. I had a real problem with 2D.

I tend to agree with George. I'm not sure --

CHAIRMAN APOSTOLAKIS: 2D?

MEMBER STETKAR: 2D.

CHAIRMAN APOSTOLAKIS: Ensure the effect?

MEMBER STETKAR: Ensure the effects of digital I&C system common cause failure assumptions--

CHAIRMAN APOSTOLAKIS: Yes.

MEMBER STETKAR: -- properly reflects a system architecture connections and hardware and/or software failure modes if it does not increase the common cause scope. Well, if the models don't capture the integration and the potential failure modes, that's an error in the models. You can't just play numbers games as a surrogate or fundamental errors in the models. And that's some of my concerns about specific guidance was saying that --

MEMBER BLEY: I didn't know what that last sentence -- I didn't know what it said.

MEMBER STETKAR: I didn't know that it changed the numbers. No, it said --

MR. KELLY: It was a recommendation to sit down and discuss with your counterpart in industry the value of improving your models in that area.

MEMBER BLEY: I think that's what you were after.

MR. KELLY: Yes.

MEMBER STETKAR: But I wouldn't call that a sensitivity study. The problem is when you delineate, I have six particular sensitivity study scenarios that now people are going to go out and say, okay, the staff told us we have to do this and a reviewer is going to say okay, they did that and everything is fine, you know. That's, like it or not, regardless of what the high level intent of this that's the way it's going to be implemented.

MR. KELLY: Right. But the other side is

that you have somebody if they come in and they haven't had a lot of training in digital I&C systems and understanding the kind of routes that are going to come up here.  Maybe the licensee performs a sensitivity study and they think that's good enough because they have nothing to base it on. And that was, in part -- I mean, actually I expanded on the ones that had been done in AP1000 in order to -- there's some other ones that I thought might have been useful. And industry was happy when I gave them these. I was surprised.

MEMBER STETKAR:  Industry is happy because it's easy to play numbers games. It's easy to vary parameters within the scope of a predefined model.  That's something, I mean it takes five minutes to do that. That's nothing.

MR. KELLY:  Right.

MEMBER STETKAR:  And that's why it's easy to do.

It's not necessarily the thing that ought to be done.

CHAIRMAN APOSTOLAKIS:  I think your first seven recommendations in the list of ten are very good and they should be moved up.  And everything else that refers to numbers should be downgraded.  We can't do it in real time here. But if you look at the 7, I mean verify that physical and logical dependencies were captured, ensure that spurious actuations of diverse backup systems or functions are evaluated, common cause failures can occur in areas and so on; all that stuff is very useful. And, again, I appreciate your concern that you stated earlier that you really don't have time to go into the same detail. All I'm saying is you can wordsmith this to make that the reviewer understands what the spirit is. But the top 14 don't impress me that much.

MR. KELLY: So one of the few things that the regulations actually tell you you have to do here is compared to the safety goal. So, in part, that's what I was trying to --

CHAIRMAN APOSTOLAKIS: I know.

MR. KELLY: You don't like the numbers, but --

CHAIRMAN APOSTOLAKIS: This is not the place to bring the safety goals. No. Let's leave the safety goals.

But look at that number 8, for example, of the fourteen.

MEMBER BLEY: Which number?

CHAIRMAN APOSTOLAKIS: Page 9. Ensure that common cause failure events are identified and modeled properly and that CCF probabilities are estimated based on an evaluation of coupling mechanisms combined with an evaluation of design feature, blah, blah, blah, blah. And I have a little comment here when I read it. If it's so easy to do, why don't we make this a general methodology? I mean, then we don't need Brookhaven or anybody else to work on anything if that can be done.

So you're asking the poor reviewer to really advance the state-of-the-art a hell of a lot.

MEMBER STETKAR: And this is the simply thing to do. This sounded pretty detailed to me, that's why I got confused between --

MEMBER BLEY: Yes, I guess that's --

MR. KENYON: -- the top 14 and the bottom 10.

MEMBER BLEY: -- to me you're looking at the failure modes, while it's not trivial, it's really important. This one, while it might be important, how do you do it?

CHAIRMAN APOSTOLAKIS: How do it?

MEMBER BLEY: It's a real tough one.

CHAIRMAN APOSTOLAKIS: That's the real

issue.

MEMBER BLEY: Just because somebody --

CHAIRMAN APOSTOLAKIS: It's stated as if it's something that anybody could do. And we all know it's tough.

MR. KELLY: Right. And in part, you know, try again. Coming into this it seems to me that --

CHAIRMAN APOSTOLAKIS: Oh, my comments don't necessarily mean you have to justify it.

MR. KELLY: Right. Okay.

CHAIRMAN APOSTOLAKIS: But if you want to, go ahead.

MR. KELLY: No. Well, I was looking that one of the insights that has tended to come out of the early PRAs that were performed over digital I&C systems, and understanding that these may be wrong, but at least the insight that did come was that failures of individual components, individual modules, whatever, tended not to be risk significant. It was common cause failures that drove you to really have problems. And for that reason I felt that -- I realize that this long and complicated and stuff like that. But that potentially common cause failures if you're going to spend time looking at anything, you want to spend time looking at common cause failures.

CHAIRMAN APOSTOLAKIS: Yes.

MR. KELLY: And trying to understand what they did and did they say, you know, basically I can only have this little tiny set of common cause failures or could it be across trains, where did they put the boundaries? What did they put in the same category that says, okay, all of these things can fail in a common cause failures. Those to me were the most important decisions that were going to be made there.

And I probably --

CHAIRMAN APOSTOLAKIS: I think the way you just said, I wouldn't have much of a problem. But when you say "an modeled properly," and "that CCF probabilities are estimated based" blah, blah,blah I think you are asking for too much here.

MEMBER BLEY: And there is another piece of it. It almost is sounding like doing a common cause failure for a bunch of valves. If you really dig in, and I'll admit you have to correct me on this, and look at how these I&C systems -- systems fail, look at the failure modes, some of those failure modes in fact have common cause impact on the other things. So when you understand the failure modes, the real key is to the common cause failures coming out of these systems I think probably fall out of that, where this makes it sound like you can go in and do a multiple Greek letter mix of six different things.  And I don't think that's the way this is going to check out.

MEMBER STETKAR:  I think there's two parts to this.  Is that internally if I call the digital I&C system with its software a box --

MEMBER BLEY:  And firmware and hardware.

MEMBER STETKAR:  And firmware and hardware and everything a box for the moment, part of the message is that within that box if you have four levels of redundant trains of things, you need to look at.  And, you know, and the vendor claims that each one is completely independent and you need to look at common cause within the box in terms of software, that's getting at this.

The other is the --

MEMBER BLEY:  That's a failure mode.

MEMBER STETKAR:  That's a failure mode.

The other is that particular combinations of unexpected outputs from that box can, indeed, have important common cause failures throughout the integrated plant. That's a different level.  That's linking the outputs the digital I&C with the rest of the plant, which --

MR. ARNDT: Yes. And we try to address some of that in the details of the verbiage associated with software-to-software in terms of the hardware and component-to-component and things like that.

And the point here was to try and articulate things that a reviewer would hopefully see in a common cause failure analysis.

MEMBER STETKAR: I think what you hear us saying is that certainly common cause failures, the scope --

MEMBER BLEY: Level.

MEMBER STETKAR: Not necessarily level of detail for the moment, but scope; the types of things that you want to look for, just what you fellas have been discussing, is certainly an important topic that should be examined during the review. An equally important are the failure modes and their impacts throughout the rest of the plant model that should be reviewed at a high level model. Not specific details. Not this level of detail for how did I think about modeling each common cause failure mode and what sort of methodology did I use; that is probably too detailed.

MR. KELLY: I think probably more than any other area of a PRA today, this at least at NRC this is an area where you're going to have more interface between digital I&C reviewer and the PRA reviewer. You know, usually now the PRA reviewers understand the systems well enough that they don't need to have the auxiliary feed water guy in their back pocket all the time telling them how to do things. But here realistically if you don't have one of these experts talking to you, you're going to get lost fairly quick.

MR. HECHT: Can I suggest that within the digital I&C part of this that we also have to be a little bit more specific on exactly what we mean by a common cause failure. I'll give you an example.

I can use a Triconex system which I believe is running in lockstep, and any failure that's caused by a timing or buffer overflow or something like that is going to happen on all three channels at the same time.

I use another system perhaps where I'm running my processors loosely coupled or more loosely coupled and I synchronize every so often. That what takes down one channel, a particular sequence of events, may not happen on the other channel.

So the computer architecture also has to be considered when we speak about common cause events. Because otherwise you will end up in a situation.

There are some software failures, and I think the kinds that are addressed in the traditional, I call it a quality  or antiprocess, but what I've seen discussed earlier in terms of the design review that are geared primarily to discover omissions, errors that one can see in the source code that will persist.  There are another class of things that occur due to timing, due to combinations of strange events, due to interactions with the hardware, sometimes the hardware has some noise in it, that are not evident in the source code.  And that we have to consider those separately. And once again the degree of isolation or the degree of commonly and the redundancy of the architecture would affect those common cause failure modes.

CHAIRMAN APOSTOLAKIS:  Shall we go on?  I mean, you got the picture here.

Item 10 of 14, again, my comment is -- let me see what I wrote here.  How is this to be done?

Item 11 the dominate failure modes, how is this to be done?

So I would change these completely. And the recent method, as I say, the safety goals I wouldn't go there.

Yes, go ahead.

MEMBER STETKAR: Item 11 is fine. I didn't care about the word "dominant." But the message there that I got was you have to look at the whole sequence of, you know, why was it dominate.

CHAIRMAN APOSTOLAKIS: Yes, take out "dominate."

MEMBER STETKAR: Yes. Well, okay.

CHAIRMAN APOSTOLAKIS: Because dominate in our business means something specific. I mean, you have probabilities or frequencies and, you know, that kind of stuff.

As I say, the wordsmithing is something I'm not addressing right now. I'm addressing content.

I do like, as I said, the first seven of the ten with appropriate wordsmithing, again.

Now why don't I like eight? Because it refers again to data. And that I don't know that it's the reviewer's business to get into that.

Nine refers to data.

And 10 raises the issue of dynamic interactions. Yes, that's good. That's important.

So 8 and 9 I would change drastically.

And, let me see. I think that covers pretty much everything I want to --

MR. ARNDT: In terms of your concern over 8 and 9 and data, what exactly is your concern? Is it that the review of the failure data and the failure rates and where they came from and what their pedigree is less important than other things or what exactly is your concern?

CHAIRMAN APOSTOLAKIS: No. I think advice like "determine if the manner in which basic event probabilities were established is acceptable," for example. That's pretty good. But I know the answer; it will be unacceptable. So --

MEMBER STETKAR: Let me interrupt for a minute. This ISG --

CHAIRMAN APOSTOLAKIS: Subtlety is not my strong suit, you know --

MEMBER BLEY: That's hard to believe.

CHAIRMAN APOSTOLAKIS: I'm sorry.

MEMBER BLEY: Always being such a nice guy.

MEMBER STETKAR: This particular ISG

focuses on digital I&C systems. Reading through this I think it's important to not be too sensitive to the fact that a digital I&C system is a cow and we're used to evaluating nuclear power plants. A digital I&C system has many different features that we need to address. Some of the things that we were talking about; software failures, completeness of failure modes, modeling of common cause failures. Yes, indeed, where do I get the data. But indeed many of the available guidelines, Regulatory Guide 1.200 and ASME, PRA standards apply equally well to modeling and quantifying the models for digital I&C as well as anything else. I don't think we need to repeat those things.

So a lot of I think, George, what you're saying in terms of 8 and 9, I didn't see anything in there that wasn't already covered by other things that we normally look at in terms of the quality or completeness of a risk assessment. You're just saying make sure that it's also satisfied for this particular application.

MR. ARNDT: Well, yes --

MEMBER STETKAR: But I need to do that for diesel generators and valves and pumps.

MR. ARNDT: But more importantly, there

is a number of techniques that are used in the industry or being proposed to be used in the industry for development of data in the digitals area.

For example, the use of defensive measure, which is referenced in an IEC standard that are unique to the nuclear I&C data analysis.

There's the issue associated that we talked about earlier about how challenging it is because of the software components and the changing aspects of systems over time that make data analysis a little bit more challenging.  So we we're trying to at least include some of that flavor in 8 and 9 so the analyst realizes that, yes, it's important, it's the same level of importance as it would be for any other component. But how the licensee might develop the data is different and you need to understand those assumptions as they effect the rest of the analysis.

MEMBER STETKAR:  Right. But we do have guidance on how -- not on the details of how derive data, but on consistency between the data that are developed --

MR. ARNDT:  Right.

MEMBER STETKAR:  -- and how they're applied in the model for everything else.  For example, now how do I derive a common cause failure parameter for failure of 13 out of 16 relief valves. That's a very, very difficult problem, but we don't highlight that as something that's unique.

MR. ARNDT: My whole point is that a lot of the things in terms of -- yes, it's in terms of data analysis and how the data parameters are derived, how the uncertainties are quantified and the applicability of the data to the particular model at hand are not unique to digital I&C systems. The same types of concerns apply throughout the whole PRA process.

I don't necessarily want to highlight data, data, data as a uniquely important element of digital I&C systems or that it should be considered any differently as a challenge in this particular area. Now other folks might not have this opinion.

MR. HECHT: Could I offer an alternative view? And that is because we are so concerned by the strange nature of software, particularly in the I&C system, that there may be some room for -- or that you need to have more experience gathered. And I'll give you just an example.

We're talking about common cause failures. Well, if we do our data collection in the right way, then we might be able to microprocessors from the automotive industry, for example. And we certainly have enough operating time each day to determine for very high level what the failure modes are.

MEMBER STETKAR: My only point is the existing guidance in a lot of the other documents addresses exactly that issue. It addresses the scope of generic data that are used, the pedigree of the generic data.

I have a particular valve in my power plant. You know, it's a 2 inch valve that has a certain motor operator with certain torque limits and limit switch limits. Well, I don't have very much data for that particular valve, but we have guidelines to say how I can use generic data to account for plant-specific experience and so forth. That exists. We're reasonably happy with that level of guidance.

My only question is do we need additional guidance specifically within the context of digital I&C systems for data? It's the same type of problem.

MEMBER BLEY: What you're talking about, the NRC now has a handbook for parameter estimation.

MR. HECHT: Right.

MEMBER BLEY: That goes through all of this. And the only thing I see looking through these that you wouldn't see there is the word --

MEMBER STETKAR: Yes, and they don't have numbers for particular boxes.

MEMBER BLEY: It doesn't have numbers. It tells you how to do the analysis and --

MR. HECHT: Yes, but isn't it worth saying in this guidance that it's possible to use that data?

I mean, you know there are two views of software. One view of software is what I call static view, which is as source code lying on the shelf or on the desk and you look at that. Then there's another view which is a dynamic view and these instructions are being executed at millions or hundreds of millions of times a second.

And in that latter view what we're talking about, the dynamic view, the software is very different. And to that extent it's worth -- at least I personally believe, and I've believed this since I'd actually had a contract for the NRC research area many years ago where we advocated that approach; is having that data and being able to say if you're going to use a certain component, hardware and software, and in combination that having that empirical basis might do something to maybe make George's earlier statement about it not being acceptable, a little bit less absolute.

MEMBER STETKAR: That's right. I think the only thing that I was trying to get apart if I look at item 9 out of ten on page 13, this is guidance for the review of digital I&C systems, digital I&C. "Confirm the data obtained from the operating experience of the same equipment as that being evaluated." Well, that's general guidance that applies to anything in a PRA. Sources for raw data or generic databases are provided; that's what I do whenever I review any PRA data analysis.

"Methods used in estimating parameters is documented." Well, of course, it must be documented. That's a basic principle of data analysis.

"If the system is being modeled is qualified in the environment, the data are not so subjective." All of these principles are principles that I apply whether I'm looking at a digital I&C system, hardware, microprocessor, if I'm looking a software, if I'm looking at in principle data for human error probabilities or human failure events. If I had a data, but I don't.

CHAIRMAN APOSTOLAKIS: Yes, because he doesn't.

MEMBER STETKAR: That's right. No, that's right, but I had to say it. You could find looking at data for diesel generator failure or anything, so it's not clear to me why I have to elaborate this and raise it as a particular item for digital I&C. Because digital I&C as an element of a PRA is going to be reviewed as an element of an integrated PRA. We're not talking about a stand alone digital I&C system analysis. At least I hope we're not.

CHAIRMAN APOSTOLAKIS: Let me, in light of where we are, I think you got a lot of advice on what to do with the list of 14 and the list of 10. But there is also an appendix that's very interesting. And I have some comments. Okay.

Appendix, the title is "Insights From Risk Assessments Performed for New Reactor of Digital I&C Systems."

The first insight says that the absolute value of the contribution to CDF and risk from failure of DI&C systems is low. The uncertainty of this insight is at the medium level.

And I'm a little perplexed now. How do

we know it's low?

MEMBER BLEY: That statement is up in the main report as well.

CHAIRMAN APOSTOLAKIS: Okay.

MR. KELLY: This is based on, again, new reactor digital I&C systems that we've already reviewed. So this is based on ABWR and AP1000 primarily.

CHAIRMAN APOSTOLAKIS: Using their numbers?

MR. KELLY: Using their numbers, right. These insights here are derived from AP100 and ABWR. Okay? And so you're taking it with that, you want to call it grain of salt or whatever it is.

CHAIRMAN APOSTOLAKIS: Can you put that grain of salt in the introductory statement? You say "The following are general insights drawn from previously reviewed new reactor."

MR. KELLY: Yes.

MEMBER STETKAR: It sounds like these are--

CHAIRMAN APOSTOLAKIS: These are real.

MEMBER STETKAR: Real.

CHAIRMAN APOSTOLAKIS: Yes. If you put a sentence there what you just said --

MEMBER BLEY: And no operating experience.

CHAIRMAN APOSTOLAKIS: And no operating.

Then the second one says --

MR. KELLY: No, there are ABWRs in Japan.

CHAIRMAN APOSTOLAKIS: -- "The estimate CDF is not --"

MEMBER STETKAR: How much data do you get from Japan.

MR. KELLY: Actually not --

MEMBER BLEY: How much data does the Japanese get from Japan? I'm sorry.

CHAIRMAN APOSTOLAKIS: "The estimated CDF is not very sensitive to reasonable changes in single digital I&C component failure probabilities or in initiating event frequencies." Question: Doesn't this depend a lot on what was modeled and how, which as been John's argument?

MR. KELLY: Yes.

CHAIRMAN APOSTOLAKIS: Okay. Let me see--

MEMBER STETKAR: By the way, oscillicity importance is not -- you can mischaracterize oscillicity importance, though. It's not for setting something. That risk reduction worth.

MR. KELLY: Yes.

MEMBER STETKAR: It's a subtle difference.

CHAIRMAN APOSTOLAKIS: Well. okay.

MEMBER STETKAR: You can kind of infer, but it's defined --

CHAIRMAN APOSTOLAKIS: Do any of the people sitting around the table have anymore comments?

MEMBER BLEY: Only one.

CHAIRMAN APOSTOLAKIS: Okay.

MEMBER BLEY: We've been pushing very hard. And, Glenn, the task you had set out is really a tough one and I think you've made a lot of progress. But I can still see a lot of difficulties. But, yes, it's really tough. At least I sympathize with the job you're trying to do.

MR. KELLY: Well, my boss told me I had until Friday to get it out.

MEMBER BLEY: Okay.

CHAIRMAN APOSTOLAKIS: John, do you do have anymore comments?

MEMBER STETKAR: Nothing new.

CHAIRMAN APOSTOLAKIS: Okay.

Jack? Myron? You'll have more

opportunities, don't worry.

Gentlemen from the staff, yes?

MR. ARNDT: WE just want to in closing, you can look at the last slide or just listen --

CHAIRMAN APOSTOLAKIS: We can look at the last slide?

MR. ARNDT: Yes. The big issue is: (1) This was not intended if you look at the actual introduction to the ISG, specifically not intended for general use. This is a guidance specifically for Part 52 PRA reviews.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: And the specific guidance or the intent of the design PRAs in Part 52 is very general, not specific for decision making, you know, Chapter 7 kind of sampling. So your discussion earlier in the meeting is very applicable.

We, the staff, are not at this point ready to use PRA for any regulatory decision making, and this is not -- specifically excludes that purpose.

CHAIRMAN APOSTOLAKIS: I second what Dennis just said. I mean, these are difficult problems.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: And the reason why we have such animated discussions is because the --

MR. ARNDT: Absolutely.

CHAIRMAN APOSTOLAKIS: -- development of these documents is at the early stages. So there's an opportunity to give ideas and so on.

MR. ARNDT: Absolutely. And the task working group has a more general charter.

CHAIRMAN APOSTOLAKIS: Right.

MR. ARNDT: And we're working with the industry on that for a longer term.

CHAIRMAN APOSTOLAKIS: I was informed by the ACRS staff that they were trying to set up a meeting with the full Committee with you guys on Friday of the April meeting.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: Two hours in the morning. So I'm sure they will contact you for approval.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: But you got our initial reaction to what we saw.

MR. ARNDT: Yes. And we'll go back and look at our processes --

CHAIRMAN APOSTOLAKIS: Right.

MR. ARNDT: -- and determine how much we're going to change and things like that.

CHAIRMAN APOSTOLAKIS: Very good.

so if there is nothing else to add to this subject, we'll recess for lunch until 1:30. And then we'll pick up the industry comments.

Very good.

(Whereupon, at 12:30 p.m. the meeting was adjourned, to reconvene this same day at 1:38 p.m.)

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

1:38 p.m.

CHAIRMAN APOSTOLAKIS: Okay. We're back in session.

The next item is industry comments on the ISGs. Mr. Gordon Clefton of NEI, please.

MR. CLEFTON: I am Gordon Clefton with NEI. My position assignment right now is to work with the industry to try and filter out some of the complications that Jack alluded to earlier this morning where we have a number of inputs from vendors, from suppliers, from utilities, from commercial interests that support the utilities. It's a task that's been challenging, to say the least.

We coordinate to have as many interfaces as we can. We try and get collaboration among ourselves so we speak with one voice to avoid confusion. We try and focus our communications through the digital projects so we have one voice speaking. We don't have a number of complications associated there.

I want to thank you for letting me speak for a few minutes this morning. If you notice on the schedule, our principle input today is a discussion on the operating experience. And that's of significance. I don't expect to take very much time to allow us to stay on schedule this afternoon and get the most that we can out of that presentation.

The overview slide that we have here is what I was going to run through today, basically summarizing. The advantage of speaking later in the day is that we've already covered a number of the topics on the TWGs, we don't need to go into further detail on them. But I wanted to express the position of the industry is working closely with the NRC. And I think this is a model that we can use in the future to see success. We've had cooperation between the interface of the industry and the staff members at TWG meetings, telephone conferences, webcasts and other associated methods.

We've had the benefit of allowing the NRC folks to come down to NEI and use our conference rooms when we couldn't get 35 people in a room designed for 20 people. We've had that working and we expect to continue that in the future.

As you can see in the slide here that we are working together. We now have seven task working groups.

We're pleased to see that nuclear fuel cycle one added to the list. There's discussions of other topics that we're working with in our own groups that we may have other issues that could come up to another task working group level, but they haven't at this time.

The steering committee has been very effective. We bring the leadership of both digital organizations, NRC and the industry together. And have effectively increased management review and increased the quality of the project management that we're doing.

We've got compliments associated with the working group organization and the steering committee. No problems at all there.

Project management, we've got a project plan. We've got a pilot project. And they're working and it gives us a chance to assign responsibilities, due dates and tasks accomplishments that we all have agreed to.

On the short term goals we're looking at the interim staff guidance, as you've heard from earlier today. We expect those to finish out this year and recognize that the last of the paperwork may spill into time periods beyond that.

Things we're looking for on that, and as an industry spokesman we're looking for them to be technically sound.

We're looking for them to be practical to apply, and that's both from the industry side and from the staff side. We want the staff to be able to review comfortably using the documents we've created and for our submitters to be able to have guidelines to put them in there.

We've shortened the appropriate regulatory reviews, but we can't dismiss those. The review comments periods and such is important to us.

In the long term, we're hoping that we'll have quality final staff guidance out there. And that we expect the ISGs to be revised and enhanced as we go along. Lessons learned with the pilot projects, more information gathered by reports, white papers and such as that so that ISGs are in as a good form as they go before they roll into the final guidance documents that we've discussed early, the SRP, the Regulatory Guides, et cetera.

One of the things that's working well I think is that we have the NRC endorse some of our industry guidance documents. That allows us to have more detail. It can be more voluble, changed as technology improves and changes, which prevents us having to take the time period to go all the way through the time delays of rulemaking, reg guide changes and such as that. So we've seen that in some of the TWGs. I think that's a new plan for TWG 5 on human factors is that they're expecting cascade some of our details down into our industry documents. We've seen that with NEI 04-04. We've enhanced to Rev 2 to match up with the Regulatory Guide, fill in the gaps that we had. We'd like to encourage that in the future as well.

On TWG 1, what I'm going to do now is just quickly run through the seven security items, or the 7 TWG items starting with the security one.

And you can see on there that we don't really have any issues and we're looking forward to the support and reviewed comments on the documents that are coming out.

It's ironic that cyber security was considered to be one of the open and closed TWG assignments with its problem statements. And it's turned out to be a challenge because of some of the things we discussed this morning. It's far reaching and it hits into each of the different TWGs.

The defense-in-depth, we have the ISG that was issued initially in September. We've been working closely with the staff to enhance that. We've recently submitted white papers, you can see on the list there. We've got some points that we're still working with the staff on in clarifying our joint understanding of the Point 4 and the BTP 7-19. And diverse actuation system is an issue that's heavily under discussion.

We've got TWG meetings happening almost every week. We have one scheduled tomorrow morning with the combined effort of TWG 2 and 3, which is our D3 group and our risk reliability, risk-informing organization. These are the agenda topics for tomorrow's meeting.

The risk-informing I think we covered pretty extensively this morning. We recognize that this one is going to come a little bit slower than the others because of the complexity of it and how we are applying it. And I think Steve Arndt suggested this morning that there's no regulatory decisions being used on this immediately, so we can appreciate that this will be a slower one developing. But as we saw in the RIC, perhaps you saw the presentation there that we're interested in risk applications.

CHAIRMAN APOSTOLAKIS: And what do you mean by COLs?

MR. CLEFTON: Combined operating

licenses.

CHAIRMAN APOSTOLAKIS: Yes, but what do you mean? I mean what's the issue?

MR. CLEFTON: The aspect there is this one we're focusing on the 10 CFR 52 type plant applications rather than existing plants right now.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: It was what we discussed this morning. The issue of what is the proper review guidance associated with the review of digital systems in PART 52 PRAs.

CHAIRMAN APOSTOLAKIS: Should it be at a COL stage or earlier, is that what you mean?

MR. ARNDT: No. I think what Gordon is trying to get at is simply the fact that the PART 52 reviews are required for design certain COLs.

CHAIRMAN APOSTOLAKIS: I can't hear you.

MR. ARNDT: I think what Gordon is just trying to point out is that modeling for PRAs in Part 52 are required for design cert and COLs. There's no additional meaning associated with that bullet.

MR. CLEFTON: So the intent is that the interim staff guidance will support those needs rather than what we have right now for existing plants and upgrades and modifications. It's focused right now for --

CHAIRMAN APOSTOLAKIS: Oh, okay.

MR. CLEFTON: -- new plants rather than existing plants.

CHAIRMAN APOSTOLAKIS: Yes. Right.

MEMBER STETKAR: You mentioned you're considering a pilot plant project. That would be in the contest of?

MR. CLEFTON: A risk application, that's correct.

MEMBER STETKAR: Of risk application?

MR. CLEFTON: Right.

MEMBER STETKAR: So, for example, the Oconee upgrade could be a candidate for that?

MR. CLEFTON: No. Our next slide -- we're getting there.

MEMBER STETKAR: Okay. Thanks. Never mind.

MR. CLEFTON: No. The Duke Oconee pilot project is principally to support the ISG supporting TWG 6 for licensing process. But it also wraps in communications, wraps in cyber security. The one it doesn't do currently is the risk or the number 7, which is for fuel aspects.

So we've identified that pilot project

that we've got when you get up here to TWG 6 is really going after demonstration of those ISGs that we have out there and with the lessons learned associated to it.

Back on track, number 5 is our human factors. WE had an all day public meeting yesterday at NEI with industry. And we worked with that on minimum inventory, computerized procedures and working on the methods for acceptable evaluations to determine manual operator actions and the time periods associated.

The nice thing about Mike Marshall and his human factors is he's picked up some of the tasks that were originally identified as a problem statements in other TWGs.  And so we've got a cross blending, if you will, between the resources for risk-informed with human factors with communications and with diversity.  So we're blending some of the staff.

When we talked about the numbers of people we have and the industry supporting it, I've probably a list of 150 people that are out there. And that includes everybody from operators to managers to vendors. A particular interest in representatives and numbers showing up from Westinghouse, Areva, General

Electric. So we have many of those represented in our industry side meetings, which most if they can and will attend are public meetings with the TWGs, but frequently are just telephone linked in or email communication.

But to answer your question earlier of how much industry support do we have, how much industry cooperation, we have a significant amount. The hard part is picking out the value in the single voice from the industry when we have a lot of noisy puppies in the litter. You can understand that situation.

So we get on to number 6 here which is where we do have our pilot project. The LAR from Oconee was submitted on the 31st of January, which is a real plus.

Industry has got a number of people looking at the success path on this. It's important for our project to be successful with it, to be able to keep this on a timely schedule so that we know what items we have in front of us. That we can resolve them quickly, not be stagnated for unnecessary problems or things that can't be resolved quickly.

We've had good success in the fact that

the steering committee members from the industry side as well as the NRC side are working together. They'll basically wear the referee shirts for this process as it goes through. We find an obstacle that's too big to surmount, we'll identify it, bring it up, if we can't resolve it it'll go to the steering committees to address whether we need to reset policy, we need to rewrite the ISG or we need to help a reviewer or help the submittal.  It's both sides that we need this to be successful.

And the picture when you step back from it is significant. Because the industry is holding several digital packages that could come to the NRC for approval based on the success in this.  The regulatory uncertainty has been significant in the past, it still exists. We want to see that this is handled as professionally as we can.

We've written and worked with the TWGs to put the best documents available out there for a guide for the reviewers and for the submitters.  We expect to follow that and then work on the delta between those if we discover one as the pilot project goes on.

We've allowed, perhaps, one year.  The acceptance-- well, we had a preliminary acceptance meeting this week and it appears that the acceptance is going to happen by the end of the month. We need a couple of schedule items to show when we're going to start answering the first the RAIs that are out there. But we're looking at about a 12 month period so that this can come back to at least a go/no go indication. And then we're working now with the industry and NRC to get a mutual schedule that we can live with that will meet Duke Power's time schedule to be able to put the first package in in the fall outage of '09, which with their schedules of freezing things before that we need a go/no go by about March of 2009.

So that gives us a year to work as a project to make sure that this package goes through. And as we identified earlier, it's a TXS RPS system.

Number 7 is a late start. We're working with Dave Rahn on that. He's doing a good job of refining his problem statements to what the real industry problem is. The meetings I've attended on that one are bringing in the vendors. They are anxious to put digital applications into the fuel cycle with, of course, the safety aspects leading the parade. But the economy and the effectiveness in there.

So we from NEI with Felix Killar are working actively to ensure that those steps are made with the input of the major vendors and our fuel supply channels and cycles and such.

With that, I'd be happy to answer any questions on a global picture. But I'd like to introduce, if we don't have questions, our presenters for the operating experience.

Well, we've been asked and talking about in cooperation with the industry and NRC is putting together as many digitally identified issues that occurred. And we started with an inventory of over 500. And what EPRI and supporting contracting companies and our TWGs have done is refined the analysis and the evaluation of that operating experience.

Now this goes back for almost 20 years. And so it's a significant pile of data to try and structure so that we can get value out of it at this level and be able to use those lessons learned.

So what I've got is Ray Torok from EPRI. He's come from California. And Bruce Geddes with him to be able to do the presentation. And I'll vacate the chair so they can get to it directly.

MR. TOROK: My name is Ray Torok. I'm

from the Electric Power Research Institute.

And I want to thank you for getting us onto the agenda here so we could come and talk to you about an ongoing project that we have where, as Gordon pointed out, we're looking at operating experience of digital systems in U.S. nuclear plants.

My co-presenters are Bruce Geddes from Southern Engineering Services who is the principal investigator for this EPRI project and Dave Blanchard from AREI who has been a consultant in dealing with the evaluations and so on.

Next slide, please.

Now we're very briefly going to explain the basis of the evaluation or investigation we did and the focus. What we did with the data to bin the various events, how we made our decisions. Also what the basic findings and conclusions were along with some interesting observations that I think are useful in terms of generating insights.

I view this as the first attempt we've made to answer the simple question what is the OE trying to tell us. So that's what it's about.

Next slide, please. Oh, there it is. Yes.

Okay. We have looked at or we have

evaluated 322 so called digital events over a period of about 20 years, both safety and nonsafety.

When I say "digital events," all of these involved something having to do with a digital system. In some cases the digital system was the cause of a problem, in other cases it just acted normally. There were things that appeared in various reports in NRC and INPO databases. Now of these 322, about half of them were also on a list that was developed by Mike Waterman of NRC Research over a number of years.

PARTICIPANT: (Off microphone.)

MR. TOROK: Pardon me? Well, no we can explain that. About half of them, that's right, were on Mike's list. Mike had been compiling a list over a number of years. And he shared that list with us. We went and looked for the reports on those events, and we couldn't find them all was the basic problem. We found about 106 --

CHAIRMAN APOSTOLAKIS: This is nuclear experience, right?

MR. TOROK: It's all U.S. nuclear experience.

CHAIRMAN APOSTOLAKIS: Okay. And you are saying it includes safety and nonsafety systems?

MR. TOROK: Safety and nonsafety, yes. Just digital system events.

CHAIRMAN APOSTOLAKIS: How many of these deal with safety systems.

MR. TOROK: Pardon me?

CHAIRMAN APOSTOLAKIS: How large is the experience with safety systems?

MR. TOROK: We'll show you that shortly.

CHAIRMAN APOSTOLAKIS: Okay.

MR. TOROK: It's a fraction of that.

Let's see. So we took the report from the OE, you know reports from INPO databases, LER reports and other reports from NRC databases.

Of course, we could only evaluate the events where we had reports. So that's what we're talking about here. And that's why we were unable to address some of the ones on Mike's list. We simply were unable to find the reports.

And in fact, at one point we went back to Mike and asked for help to find them. And we still couldn't find a lot of the reports on Mike's list.

CHAIRMAN APOSTOLAKIS: Did you make them up?

MR. TOROK: Pardon me?

CHAIRMAN APOSTOLAKIS: Did you make them

up?

PARTICIPANT: Took us a long time to do that.

MR. TOROK: That's a lot of dedication if he did that.

MR. GEDDES: It was very creative.

MR. TOROK: Yes.

Anyway, now one thing I wanted to point out here. As we say, we characterized this as OE, operating experience data. But really what we're looking at is things that involves some sort of misbehavior, typically. We're not looking systematically at the successful operating experience. I just wanted to make that clear.

Now, presumably, there's a lot more successful operating experience than there is negative operating experience. But that's not what we talked about.

MR. GEDDES: And it doesn't get reported.

MR. TOROK: That's right. Yes. The successful operating experience doesn't get reported in these databases. It's a lot more difficult to track down. Okay. Although, you know everyone has anecdotes about it, but in terms of a systematic approach to what's going on, it's not there.

So the focus then was on misbehaviors or potential misbehaviors, that sort of thing.

Now we were doing this work in support of the NEI working group on digital instrumentation control issues. This is the group, of course, that Gordon was talking about a few minutes ago. And specifically we were supporting the D3 effort, the defense-in-depth and diversity effort which means that for the purposes of what we were doing, the focus wanted to be on either actual or potential common cause failures and also with an emphasis on 1E systems, safety systems. Because that's where the D3 issue drives you.

So that's really what the focus of our presentation is today as opposed to on the broader class of all the safety and nonsafety issues.

Now, there's significant differences between looking at safety and nonsafety systems that really affect the way you do the evaluation. For example, in the safety systems there are extra rules on redundancy and separation, you know single failure criteria and so on that affect the susceptibility of the common cause failure. So comparing nonsafety to safety really is apples and oranges here. So the focus today is on 1E events in digital systems.

MEMBER BLEY: Are you saying the actual digital systems are that much different or just the way they're employed?

MR. TOROK: I suppose it's primarily the way they're employed in terms of the architectures and so on.

Now there are also additional QA type quality requirements that affect the safety systems, you know in terms of software development standards for example that would be applied to a safety system, but not a nonsafety.

MR. GROBE: Yes. I'm not sure I understand that comment.

This is Jack Grobe.

Does that mean that the chemical industry, the aerospace industry, NASA all of that other information that we can gain on digital control systems has no value whatsoever?

MR. CLEFTON: Oh, absolutely not.

MR. GROBE: Oh. So I don't understand your comment.

MR. TOROK: I'm saying for the purposes of what we were doing, looking at operating experience in the U.S. nuclear industry and in focusing on defense-in-depth and diversity and the potential common cause failure, the architecture of the system and other requirements like the single failure criterion and so on play into whether or not there will be a potential common cause failure vulnerability. And in essence, the safety systems and nonsafety systems are very different.

For example, nonsafety systems can have redundant trains that share a power supply, but you would never see that on a safety system.

So they're different in terms of common cause failure vulnerability. So that's why the focus today is on safety systems.   And as I said, potential or actual common cause failures.

MEMBER BLEY:  Now let me go back to what I asked you before, because I think I understand it. The actual digital control systems, maybe it's a PLC, that's not what you're saying has different QA on its software?  You're saying the integrated, the full instrument?

MR. TOROK:  Well, both could. compared to nonsafety.

MEMBER BLEY:  So they're not standard PLCs?  These are designed and programmed at their baselevel especially for nuclear safety systems?

MR. TOROK:  Well, there's some of both

really. There are platforms now being used in nuclear plants that were designed to be safety platforms for the petrochem industry, for example. So they have a lot, most if not all of the same features that you would find in a system designed for the nuclear industry. There's a lot of overlap there. Okay.

And did I answer your question?

MEMBER BLEY: Not quite. I guess I'm -- it sounds as if you're saying even though there were some that were designed with the same kind of safety standards, that we have individual digital systems that were designed and programmed specifically for nuclear safety applications. And that's what's going into all our safety systems?

MR. TOROK: No. Typically the platforms that were talked about earlier, the ones that have been reviewed by NRC --

MEMBER BLEY: Yes.

MR. TOROK: As an example, somebody had mentioned the Triconex triple modular redundant platform. It was designed, I don't know how many years ago now, for use in safety applications in the petrochem industry. Because they knew they were designing it for safety applications, they built in a lot of fault tolerance and redundancy and so on. It turns out that's real good in the nuclear industry as well.

MEMBER BLEY: I'll buy that. Okay.

MR. TOROK: Right?

MEMBER BLEY: Go ahead.

MR. TOROK: Okay. Let's see. So why are we doing this? Well, I don't think I need to really tell you guys, because in a way it was your idea. There was an ACRS letter last year recommending to the staff that they look at the operating experience data to generate insights that could be factored into the guidance for defense-in-depth and diversity.

Now, we're not the staff. But we recognized a good idea when we saw it and decided that we should get involved in this. And that's really --

CHAIRMAN APOSTOLAKIS: The staff is also doing it because they think it's a good idea.

MR. TOROK: Of course.

CHAIRMAN APOSTOLAKIS: Right?

MR. TOROK: Now, there are a lot of different kinds of insights that I wanted to mention that you can go after when you start doing this. And, for example, you can look at event causes. Were the events caused by hardware problems, software problems, process problems; that sort of thing. Also what types of corrective actions were used after the fact?  Same thing, hardware/software process.

We also looked at them to see which of them could become --

CHAIRMAN APOSTOLAKIS:  Excuse me. Is the database you have developed available to the staff?

MR. TOROK:  Not yet, although we have--

CHAIRMAN APOSTOLAKIS:  But it will be?

MR. TOROK:  Yes. Our intent is to share as much of it as we can with the staff.  A lot of it comes from INPO reports. They're very sensitive about giving complete data to the staff. But they have agreed that in case we should be able to share almost all of it with the staff.  So that's our intent.

And what we have to do is produce a sanitized version of our database where we strip out things like plant names, for example.

CHAIRMAN APOSTOLAKIS:  Well, that you can do. But, I mean --

MR. TOROK:  Well we don't care about the plant names, right.

CHAIRMAN APOSTOLAKIS:  -- the information, though, should be documented.

MR. TOROK:  That's right. The event

descriptions. Well what we can't, we EPRI, give anybody is the complete operating experience reports from INPO, right? So we have been already discussing with INPO the issue of what we can give to others, including the staff. Especially the staff, in fact. And we want to give them as much as we're allowed to. That's our plan here.

So meanwhile, let's see. One of the things we're looking at here in these events was was there potential for common cause failure or was this something that could only happen in a single channel, and if so why. That can generate some interesting insights.

What kinds of prevention and mitigation methods might have been affected. And here we get into discussion of things like what type of diversity strategy might have bene useful. What types of design measures might have been useful.

CHAIRMAN APOSTOLAKIS: Can you give me some idea of which safety systems are using digital I&C?

MR. GEDDES: There are some reactor protection systems, ESFAS systems and a number of auxiliary systems that manipulate the valves or actuate emergency ventilation. Probably among the 1E events, I would say about a third are related to RPS and ESFAS. You'll see more information on --

CHAIRMAN APOSTOLAKIS: So this actuation of safety --

MR. GEDDES: Yes.

CHAIRMAN APOSTOLAKIS: Not control?

MR. GEDDES: In some cases there is some control. In a few cases.

CHAIRMAN APOSTOLAKIS: Right.

MR. GEDDES: We do have selected events in some backup slides that we can share.

MR. TOROK: Right.

MR. GEDDES: Just a handful.

MR. TOROK: So let's see. Okay. So one of the things we looked at or asked ourselves a question of these events, what types of diversity might have been useful in avoiding it? What types of defensive measures, which means design features, in the platforms might have been useful? And sometimes we can look at the design features that were added after the fact. Now an example of this goes back to a question that was asked earlier today. Suppose the digital system gets data from a failed sensor and does the wrong thing with it.

What you typically see in the platforms

that are being used here in safety applications is data validation routines that would find that at flag half, because that's what they're for. And there are many other design features that the vendors incorporate into these platforms that provide protection again single channel failures and also common cause failures.

So we looked in these events what types of defensive measures might have been useful that maybe weren't there.

We also looked at how --

MR. HECHT: Can I ask a question? And that is, with respect to those things you called design failures.

MR. TOROK: Design failures?

MR. HECHT: Well, you just mentioned design failures and you used as an example the data input validation routine.

MR. TOROK: Well, they call that a defensive measure.

MR. HECHT: Okay.

MR. TOROK: And maybe I said the wrong--

MR. HECHT: Well, I was just going to ask you what you meant. Do you have a classification called software design as being --

MR. TOROK: Yes, and we'll get to that.

MR. GEDDES: Yes.

MR. TOROK: So hold that thought.

Oh, and by the way, I should have said please save the part questions for Bruce, right.

MR. GEDDES: And my colleague Dave to my left.

MR. TOROK: But we'll show you that in a few minutes. So hold that thought, okay?

MR. HECHT: Okay.

MR. TOROK: Let's see. One of the things we looked at that was interesting was how were these events discovered. In some cases they were defects that were discovered in recommissioning testing, for example, and never actually made it into the plant. But there was an OE report filed on it. So we have that in there.

Now, in that case yo wouldn't want to -- what should I say? You wouldn't want to penalize the utility for doing a good job with their V&V. But that type of thing can still --

CHAIRMAN APOSTOLAKIS: No. But over the years, though, much has been made of the software controlling the process.

MR. TOROK: Yes.

CHAIRMAN APOSTOLAKIS: So this is telling us that the process and controlling the process doesn't always work.

MR. TOROK: Well, that's true. It doesn't always work. It doesn't always work. And that's one of the reasons we looked at what the potential causes were, what the recorded causes were for the events, and also what the mitigation methods were. Sometimes it's a process element, sometimes it's a design issue and so on.

And it was interesting to look --

MR. HECHT: I would want to make a comment, though, that with respect to those things which in my world are called "escapes,"

MR. TOROK: Escapes?

MR. HECHT: Yes. In other words, defects that escape the phase at which they were intended to be caught and eliminated.

MR. TOROK: Oh, oh, oh.

MR. HECHT: Yes.

MR. TOROK: Okay.

MR. HECHT: That if they're only a handful in this many systems, that the process is doing a very good job.

MR. TOROK: Thank you.

MR. HECHT: Based on other experience.

MEMBER SIEBER: That could mean it didn't find it in a system.

MR. HECHT: It could be mean that, too.

MR. TOROK: It could mean you didn't find them. The other thing to keep in mind here is that relatively speaking the safety systems are really simple compared to what can be done with software. And that's got to be a factor here.

MR. GEDDES: And there's relatively fewer of them, too.

MR. TOROK: Yes.

Now, another thing we looked at here was the safety significance. You know, we talked about what happened and whether it was a potential common cause failure. It's a whole different question to ask was this important from a risk perspective, right? And so we looked at that, too.

Now as Bruce pointed out, we do have additional slides that show details for selected events. Because we thought you'd want to get into what actually happened in some of these things. And we'll get to that shortly.

CHAIRMAN APOSTOLAKIS: Do we have those slides?

MR. TOROK: You're about to.

MEMBER SIEBER: I think we have them in our book.

CHAIRMAN APOSTOLAKIS: We don't have --

MR. TOROK: They're not in the package because we were still working on them last night.

CHAIRMAN APOSTOLAKIS: You did what last night?

MR. TOROK: We were still working on these last night, which is why they're not in your package. Okay?

Now, these have more information on selected events in terms of what happened, how we bin it in our process, what the safety significance was and maybe some other insights. So we'll be getting to that shortly. Okay.

One thing I wanted to mention very briefly is that it was suggested early on that looking at this data might be useful in terms of generating reliability numbers for PRA.

CHAIRMAN APOSTOLAKIS: Who said that?

MR. TOROK: Who said that?

CHAIRMAN APOSTOLAKIS: Yes. We didn't say that.

MR. TOROK: Okay. And it turns out that

that's a more difficult problem. Because you end up having to talk about more than just what problems there were, also what was the successful for history, for example, that we didn't have a good handle on. Or it was much more difficult to get a good handle on.

Another problem here is that for the safety systems there really aren't that many demands on the safety systems. And the other factor here is that these safety systems are designed to be very, very reliable, which means failures on demand are hard to come by. So in terms of generating statistics it's not so easy. And so we did not go into that in detail in this effort. That's all I wanted to say about.

So let's see. Next slide.

CHAIRMAN APOSTOLAKIS: You're way behind.

MR. TOROK: Pardon me?

CHAIRMAN APOSTOLAKIS: You should be slide on what?

MR. TOROK: Four -- five.

CHAIRMAN APOSTOLAKIS: Five.

MR. TOROK: Three/four, I think.

CHAIRMAN APOSTOLAKIS: You just finished four?

MR. TOROK: I'm on four right now.

CHAIRMAN APOSTOLAKIS: You're on four right now. Okay.

MR. TOROK: Is that right? Yes.

So now we want to get onto the details and some of these things, but first I just wanted to very quickly summarize the findings and then we'll show you how we got there. That's where the hard questions come in.

First of all, there were no actual common cause failures that disabled safety functions in on demand situations in the 322 events.

MEMBER STETKAR: Let me stop you there. That's a very, very carefully worded lie. "There were no actual" that disabled a safety function. You mentioned 322, but you screened that 322 to look only at safety related?

MR. TOROK: Yes.

MEMBER STETKAR: So it wasn't 322. Yes, it could have been six.

MR. TOROK: Oh, I see what you mean. I see what you mean.

MEMBER STETKAR: Now let me dissect that line. What is an actual common cause failure? What is an actual common cause failure? What is the definition of an actual common cause failure?

MR. TOROK: It's a situation -- in this case we're talking about at the system level, too. Because I said --

MEMBER STETKAR: No, no, no. What's the definition of an actual common cause failure?

MR. TOROK: It means there's a valid demand system --

MR. GEDDES: We have it written down.

MEMBER STETKAR: If it's a difficult question, you said he could answer.

MR. TOROK: That's right. And I should have also indicated that there was in the handouts that you do have a list of terms at the end.

MR. GEDDES: Key terms.

MEMBER STETKAR: Oh, okay. I'm sorry.

MR. TOROK: Now we put that at the end because we didn't want to get stuck on it here.

MR. GEDDES: Page 9.

MEMBER STETKAR: Oh, okay. And the malfunction on demands that results in an incorrect response or loss of function across multiple redundancies at the same time.

Okay. So now I understand what an actual common cause failure --

CHAIRMAN APOSTOLAKIS: Yes.

MEMBER STETKAR: Disabled a safety function. Now out of the 322 total events that you had including safety/nonsafety, whatever experience were there any actual common cause failure events that disabled nonsafety functions like feed water control, turbine generator control that also used multi-channel digital protection and control systems? Because they're more standard in the feed water and turbine generator controls than they are in the safety systems?

MR. GEDDES: Yes.

MEMBER STETKAR: There were? Thank you.

CHAIRMAN APOSTOLAKIS: You had an example of those --

MEMBER STETKAR: Those were judged as not relevant simply because you were looking on one side of an administratively defined term rather than the other side of an administratively defined term?

MR. TOROK: Well, the defense-in-depth and diversity issue is driven by Branch Technical Position 10 which focused on RPS and ESFAS primarily.

MEMBER STETKAR: If I'm operating a nuclear power plant, I want my turbine generator and my feed water system to work really, really well.

MR. TOROK: Yes.

MEMBER STETKAR: So I would like that to be a very, very reliable protection --

MEMBER BLEY: Could we revisit this after he reviews it?

MEMBER STETKAR: Okay. Sure.

MEMBER BLEY: Because there's a few other charts. I'll telegraph it ahead. When you go through the details, I'm going to ask you if you looked at all 322, do you draw different conclusions about how things parse out.

MR. TOROK: Okay.

MEMBER BLEY: So go ahead with your talk.

MR. TOROK: Okay. So let me try to get through this quickly.

So we know what an actual common cause failure is now. And we know that we didn't see any of the disabled safety systems. Okay.

And you're right; 322 is the wrong number to associate with that. It's just the 1E ones.

MR. GEDDES: Forty-nine.

MR. TOROK: Forty-nine is the magic number. Okay.

Now, the other part of this is you'll see that we differentiate between what we called software events and nonsoftware events. So it's useful to explain what we mean there.

When we said "software," we were trying to isolate the things that are digital system specific. So a good example of a software problem would be a design defect in the software that causes the system to do the wrong thing. What that would not include would be an incorrect setpoint. Because an incorrect setpoint, be it in a digital system or an analog system, it's still a problem, right? So we were trying to isolate the ones that effect digital systems, not all systems. And part of that is because Branch Technical Position 19 is focused on helping protect against software common cause failures or digital common cause failures, some people say. These other potential causes like incorrect setpoints are covered by other processes that are already well developed and it's where utilities manage these things under Appendix B programs. So that was why we tried to make that separation between things we called software and nonsoftware.

MR. HECHT: Ray, could I suggest that there are other differences that you might want to consider in looking over those failures?

For example, timing considerations.

Software systems are sequential. They do things in a certain order and they do things one at a time. So there could be response time defects.

Another one is A to D issues.

MR. TOROK: That's true. We used the word software because most people think we're talking only about software common cause failures. And it's really broader than that, as you point out.

So if we saw an event that we would say this is characteristic of a digital system but not an analog system, even if it wasn't software specific, we would call it a software event here.

MR. HECHT: Can I suggest a term that might be useful, and that is "computer."

MR. TOROK: Okay. We'll look into that. Computer is also a very loaded term, I think.

MEMBER SIEBER: Yes. It could be a small part of it.

MR. TOROK: Yes. IT means a lot of different things to different people.

CHAIRMAN APOSTOLAKIS: What exactly do you mean, though?

MR. HECHT: What I'm trying to get to is that there are some parts of the system which, as Ray pointed out, are common between digital and analog.

If you have a short circuit, you can have a short circuit.

On the other part there are other parts of it which are unique to the computer -- I'm going to call it the computer -- that sequential state machine which does things and all of the underlying hardware infrastructure which supports that including, by the way, digital communication networks if they're there and especially including the multiplexing if it's there. I don't know if that's part of a safety system or not.

But those kinds of things are not necessarily in the "if, then else" part of the application software.

MR. TOROK: Yes. And it turns out that settling on terms to communicate this information proved to be very difficult for us. And we've had reviews with the NEI working group where we got pretty well wrapped around the axle on terms. And you can see how it is tough here.

Now one word that we have used a lot over the last couple of years for this kind of thing is just the word "digital." And a digital failure means it has certain characteristics. It's systematic in the sense that it comes from a design fault such that every time the system sees a certain set of circumstances it will behave in the same incorrect way.

And I wonder how that would do against the definition you're proposing.

MR. HECHT: No, it wouldn't. It wouldn't at all. Because I have lots of incidents and studies showing that you put the digital system in nominally the same operational environment, it will fail one day and it won't fail the next.

MR. TOROK: We should talk more about that.

MR. HECHT: And the reason is because you have certain combinations of events. You know, you can get a buffer overflow in one case, it doesn't come in the other case. In some cases there's a multitasking operating system so you do tasks in a different order.

MR. TOROK: Yes.

MR. HECHT: In some cases there's just certain noise in one of the vents that causes it to go one way or other. That same noise wouldn't affect the analog signal the same way, however there's other noise in analog signals that --

MR. TOROK: Yes. Another factor that may

be important to us here, too, is the restrictions that are on safety systems and so on that maybe make some of those mute. I'm not sure. But I think we probably need to broaden our discussion along the lines of what you're saying.

MR. HECHT: Yes. Well, so long as you add something to page 9, you can call it software and saying by software we actually mean the entire digital platform. That's fine.

MR. TOROK: Okay.

MR. HECHT: But I think we should know what it is that's meant here. And I think by coming up with the right term --

MR. TOROK: Okay. Now I hope everybody pretty much understands now what we mean by software and nonsoftware when we say for this purpose, right? So having said that --

MR. HECHT: No, I'm sorry. I don't. Does software include only the application software or does software include the parts of the system which might normally not be developed by the vendor?

MR. GEDDES: We include the operating system and the application code.

MR. HECHT: And the device drivers?

MR. TOROK: All, I guess.

MR. HECHT: And the board support package?

MR. GEDDES: Yes. Firmware, operating system, yes.

MR. HECHT: Okay. Even if it wasn't developed by the vendor?

MR. GEDDES: Correct.

MEMBER BLEY: And I would assume the kind of things Myron talked about like failures due to noise that you just don't know why they happen but they happen within that black box?

MR. GEDDES: We've seen more of what you're talking about in the nonsafety systems than the safety systems.

MEMBER BLEY: And in fact you've seen more of everything. You've got a lot more data on those.

MR. GEDDES: Well, the software failures that we have seen in the safety systems are at the application level, not the operating system level. Where we do see operating system problems, race conditions, timing conditions or for overflows we do have some of those events in a nonsafety population.

Now we didn't bring all the nonsafety information with us today. Because, quite frankly, we didn't feel like we'd have enough time to cover it. Our focus today is on the safety systems and the findings that we were able obtain.

MR. TOROK: We'd be happy to come back again sometime if you think that would be useful to talk about --

MR. GEDDES: We have a mountain of information.

MR. TOROK: Yes. But, anyways, like I said, we tried to focus on a useful subset here.

So now then moving on, if I'm allowed to say "software/nonsoftware," our bottom line here, one of them anyway, was that there were six of what we called potential common cause failures. And Bruce is going to show you lot more information on some of those.

One of them involved a software design defect, and that we would categorize as a software event. The other five involved other things where it had more to do with human performance, incorrect setpoints, incorrect parameters; that sort of thing, not software design issues.

Then the last thing there is based on this looking at the relative magnitude of the datasets for the software versus nonsoftware, the data seems to indicate that what's going on right now in terms of what the vendors are doing to protect against common cause failure in digital systems is working pretty well. And the kinds of things they're doing are, of course, they use various codes and standards in developing the software. They also have become pretty adept at implementing design features in their platforms to preclude or avoid or limit common cause failures. And that's what we call defensive measures.

And there are diversity attributes also that come into play here in making the nuclear plant systems -- that's what we're seeing. And with that, I think I'd like to turn it over to Bruce to talk about the details of how we handled the data.

MR. GEDDES: Okay. The next two slides cover a graphical illustration of the data that we were able to collect and some of the findings that we draw from that data.

Slide 5 is the software defect bucket that we just described. On the left hand side you see this pyramid structure. The 322 events at the top, 49 of which were discovered and reported on 1# systems, 274 on non-1E systems using just a very simple definition like you find in IEEE 603.

Out of those 49 1E events reported where we found the source documents, 27 of them reported a common defect of one kind or another. Okay. Twenty-two were single failures, and that's what you hope to find in 1E systems that the single failure criterion would protect against events. But there were 27 of these events that were due to some kind of a common default.

Out of those 27 common defects, four by this definition that we've proposed, were software related, 23 were nonsoftware related. And those would the life cycle management, human performance issues, operator error, maintenance error, bad procedures, configuration control or a bad requirement analysis --

MEMBER BLEY: Primarily human management, human maintenance kind of thing?

MR. GEDDES: Correct. Correct.

MR. TOROK: Is it clear what was meant by "common defect" there?

CHAIRMAN APOSTOLAKIS: No. You have an example of a single defect?

MR. GEDDES: A single defect?

CHAIRMAN APOSTOLAKIS: Yes.

MR. GEDDES: I have an example of a

common defect that resulted in a single channel failure. I don't have any examples of single failure.

CHAIRMAN APOSTOLAKIS: Well, how can one decide that the defect was a single defect?

MR. TOROK: Well, common defect means it happens in multiple redundancies in the safety system.

CHAIRMAN APOSTOLAKIS: I understand that.

MR. GEDDES: No, no, it means it's presence in multiple redundancies.

CHAIRMAN APOSTOLAKIS: If I see something in one channel and I don't see it another channel, what is it that tells me that next time around this will not be involved?

MR. GEDDES: Well, the examples -- and I apologize. I don't have one with me.

CHAIRMAN APOSTOLAKIS: Well, if you remember.

MR. GEDDES: But a real good example might be a module failure due to just a single random hardware module failure by the classical definition that we're used to. And I'm an I&C guy. I think deterministically. Dave's our PRA guy, okay. But from a single failure perspective under the IEEE single failure criterion, single random hardware failure is what is in those 22 events.

MEMBER BLEY: So one missing signal at an operator valve or something?

MR. GEDDES: Correct. A transmitter failure or a power supply failure.

MEMBER BLEY: Okay. The whole thing.

CHAIRMAN APOSTOLAKIS: You know, EPRI, NRC, I don't know who else, sponsored a major project on common cause failures for hardware back in the '80s or '90s. You were not with that? Okay.

MR. GEDDES: Yes.

CHAIRMAN APOSTOLAKIS: Okay. And they had these little diagrams, little pictures, right?

MR. GEDDES: Yes.

CHAIRMAN APOSTOLAKIS: That helped the analyst or the evaluator decide whether an observed failure on component A had the potential of not propagating, but appearing also on component B. And then they had an elaborate statistical method that assigned the probability of .1, .2 of this becoming a common cause failure.

So the message there was that it's really very hard to decide that if you see a defect here, you're not going to see them -- I mean you don't see it now, but it has the potential perhaps to go to the other side.

MEMBER BLEY: My understanding, and maybe I got this wrong, is that what they're showing us if they said "common," there were more than one effect. Not potentially there could be.

CHAIRMAN APOSTOLAKIS: But I'm addressing the potential that there was --

MEMBER BLEY: Potential mean you don't have to worry about.

CHAIRMAN APOSTOLAKIS: I know, but I mean in hardware EPRI does a report that says you have to worry about it.

MR. GEDDES: And in fact if we were modeling this in the PRA, we would model the hardware common cause failure potential as well as, perhaps --

CHAIRMAN APOSTOLAKIS: So you would take those 22 and have some sort of an evaluation?

MR. GEDDES: A beta factor, that sort of thing, yes, if we were modeling it in the PRA.

MR. HECHT: Can I suggest also that the next time you present these instead of using the word "common defect," defect implies a flaw. And I think you're talking about events here, aren't you?

MR. TOROK: No. We are talking about a

common defect or common fault --

MR. GEDDES: No. Let me clear. There are licensees that reported a defect without any system event, no failure. They discovered a flaw and reported it.

MR. HECHT: All right. But now is --

MR. GEDDES: And we have a definition that might be useful.

MR. HECHT: Yes. But here you're talking about actual CCFs. Actual common cause failures, failure or events.

MR. GEDDES: Okay.

MR. HECHT: All right.

MR. TOROK: Well, I was going to say, for a software event you need a software, a defect or a fault or a bug and it triggered to turn that into a --

MR. HECHT: So it was an event?

MR. TOROK: An event is anything that got reported in one of these reports. See, effectively, that's sort of a nuclear power industry definition.

MR. HECHT: I think we're mixing defects and events here. Because a single defect could cause many events, right?

MEMBER BLEY: No. I think we have a

language difference from industry's here.

MR. GEDDES: Yes. You're right.

Our approach -- in fact, in another report we take the time to report or define the term "event." Okay. I don't have it here. But if a system is inoperable due to a defect or passes the criteria for reporting and we have a single report of a defect in a system, we're calling that an event. If there's a reported issue in this context, whether there was a manifestation of that issue into a plant event or not, if there's a reported issue, we're calling that an event in this context.

MR. HECHT: Okay. I'll accept that definition. So I can use "report" and "event" basically as synonyms?

MR. GEDDES: Correct.

MR. HECHT: Okay. But then there is also a need to distinguish between flaws, if you will, in the design and things that happened.

MR. TOROK: It's here. And when we show some of these examples, I think it'll be clearer.

MR. HECHT: Okay. But that relates to the question that George was asking, and that is how can you have a common cause defect that affects only one channel?

MR. GEDDES: It has to do with the state of the channel. Okay. The state's required for the common defect to result on quality.

MR. HECHT: Okay. So that's why I'm saying that if you use the appropriate terminology, and I'm not hung up on the word "event," but if you use the appropriate terminology to distinguish something which is a persistent condition of the system which is not manifested itself into a failure which would cause somebody to write a report -- failure causing somebody to write a report as opposed to writing a report without the report, that that should probably be distinguished.

MR. GEDDES: Well, okay. That's good input.

There are cases where the discovery of a defect is reportable whether there's a failure or not.

MR. HECHT: I understand that.

MR. GEDDES: Okay.

MR. TOROK: The other thing to keep in mind is if you have a common defect, which means in multiple redundancies, it takes concurrent triggers in those redundancies --

MR. HECHT: Absolutely.

MR. TOROK: -- to make the common cause failure happen?

MR. GEDDES: Common state.

MR. HECHT: Yes. It's very important to know that. It's extremely important to know that.

MR. GEDDES: And we use that concept in differentiating how we bin these events.

MR. HECHT: Okay.

MR. TOROK: You'll see from some of the examples how we dealt with that.

MEMBER BLEY: I'd like to sneak in a question and a comment.

MR. GEDDES: Yes, sir.

MEMBER BLEY: The question is a simple one. You took the 49 events and you said out of those 49 events, 22 were single defect, 27 were common defects. Did you look at the 273 nonevents and do they break out in a similar fashion or were they dramatically different?

You know, the reason I'm asking this goes back to the question over here. If they're reasonably similar, then we have a much larger database from which to gather useful information about the digital system itself. Not everything connected to it.

MR. GEDDES: We do see common defects in

the non-1E events.  In some cases human performance procedures, operator error. We do see some of that in the non-1E systems. But to contrast the non-1E from the 1E, often non-1E systems share resources; power supplies, back plants, buses. And the defect might be common by the nature of the design of the system.

MEMBER BLEY:  Yes. Fair enough.

MR. GEDDES:  Okay.  So you know you lose that independence.  And what Ray's point was independence helps.  Now that doesn't mean there's a complete absence of common defects; of course not. But independence helps dramatically on the 1E sides.

MEMBER BLEY:  It's just that that leads me to another comment. There were a series of studies done by AEOD starting about ten or 15 years ago. They were called The Risk Studies. Idaho did them.  And they did something close to what John was talking about.  They went back and took different pieces of equipment.  It wasn't this kind of stuff. It was mechanical and electrical equipment.  And took it into different pieces and looked at the data on each of the pieces to see how -- you know, some data you gathered really only applies to this piece where somebody was applying it to the whole system.

And an approach like that might be useful here, that there are certain kinds of things that will apply to the non-safety and safety and other things are really peculiar to one or another. So we might be able to do much better on data.

MR. GEDDES: One of the extensions of this research that we're discussing is developing a lessons learned document from safety and nonsafety events. And the failure modes are very clear in the reports.

The most dominant failure mode of the non-1E systems is hardware module failures. And issues come into play like age related degradation mechanisms, terminations, loose wires sometimes initiate an event. And that's low-hanging fruit for licensees to go after. And I would echo your concern that as a licensee I've spent most of my career in plants, the turbine trip is a dramatic thing to happen on your watch, especially after a digital project.

If I can turn your attention to the next slide, then we'll come back and look at specific examples.

Again, the pyramid diagram on the left hand side is the same, and then you can see how we bin the various of the 23 nonsoftware defects. We do categorize by spurious actuation, potential common cause failure and actual common cause failure, like we've discussed.

And we differentiate the system, subsystem or channel level. The system level would be, for example, the entire RPS. The subsystem might be a trip channel like an OPRM, an oscillating power range monitor subsystem that's a member of the RPS. So we make that distinction.

If we can go back to slide 5, Ray?

MEMBER BLEY:  Let me just get the language clear.

MR. GEDDES:  Okay.

MEMBER BLEY:  Because I think I got it.

A common defect means there's something that's not right in multiple places associated with the digital system?  Common cause failure when you get over that, or single failure means including in all the attached material? So you can have a common defect but only a single failure out in the plant?

MR. GEDDES:  That's true.

MEMBER BLEY:  Okay.  That's the language?

MR. GEDDES:  Right.

MEMBER BLEY:  Thank you.

MR. GEDDES:  And our definition of defect is, if I can just read this: "A deficiency in characteristic, documentation or procedure." And we added on to that, "In software often referred to as 'fault' or 'bug.'" Okay. But it can be the characteristic of an item, a physical item, a hardware module or even a software module, or it could be in the documentation or the supporting operations, that means procedures that are used with the human in the loop to drive the plant.

I'd like to go to the potential common cause failure at the system level. There's an example here. And in your backup slide package, it's event 10. At event 10, the 10 is simply database entry number ten in the database.

This event occurred due to a common defect in a load sequencer, certainly a 1E system. It occurred in November of 1994.

The route cause, and I forget which Member differentiated between causes of events and failure modes, but that's a very important distinction. And on the right hand side you can see the causes of the events. And often there were multiple causes reported or root cause and then contributing causes.

In this case the root cause is inadequate software design. And the contributing cause reported by the licensee is inadequate software V&V.

The first corrective action was to fix the software, to actually change the logic in the software. And then they also focused on their software development process change.

The failure mode is in this case this load sequencer has four channels that operate asynchronously, and that's an important distinction. But the software logic defect was common in all four channels and under certain conditions, and it's a timing condition, the application logic can run -- at certain times they overlap to the point where it's simultaneous. Okay. And Dave did a back-of-the-envelop calculation and found that about ten percent of the normal operating time with this system in its automatic test mode had automatic test software that ran continuously in the background, so to speak, can prevent a valid safety injection signal from being passed through the sequencer and actuating safety injection.

MEMBER BLEY: Ten percent of the time?

MR. BLANCHARD: All four sequencer, right.

MR. GEDDES: Right. Ten percent of the

time.

MR. BLANCHARD: The revised software failure --

MR. GEDDES: All four sequencers overlap at the same time where this defect was common at the same time.

CHAIRMAN APOSTOLAKIS: How was this discovered?

MR. GEDDES: They were actually doing surveillance testing a couple of years after the modification was installed and they discovered it then. It's not clear to me reading the report what testing was done during surveillance that was not done during initial installation.

CHAIRMAN APOSTOLAKIS: Okay.

MR. GEDDES: But they happened to see the condition while they were doing the surveillance test.

MEMBER BLEY: Now, let me just to get the significance of this. That ten percent of the time the condition that would be calling for that actuation would be still there after this time cycle of overlap left, and then --

MR. BLANCHARD: Then the sequencer would--

MEMBER BLEY: So it would be a delay in safety injection rather than a complete failure?

MR. BLANCHARD: No.

MEMBER BLEY: No, it would be a failure?

MR. BLANCHARD: If you had the loss of coolant accident at the time all the sequencer were overlapping under this one condition, then the SI actuation signal would be permanently delayed.

MEMBER BLEY: And would not --

MR. BLANCHARD: And would have to be backed up by the operator.

MEMBER BLEY: Manually backed up.

MR. BLANCHARD: -- time it would have worked.

MR. WATERMAN: This is Mike Waterman in the Office of Research.

What it was was that the load sequencer had 11 sequences that it self tested, four of those sequences were safety injection actuation. And the way the testing worked out was that originally the testing happened continuously and they had a mechanical relay that would initiate each test. And none of us had done a mean time between failure on mechanical relay, and after about three months it wore out.

So they realized that they couldn't do continuous testing because they couldn't keep a relay running long enough. So then decided they would do one load sequence test per minute, and the rest of the minute after the test would be done, they just wouldn't do anything.

In the four high pressure safety injection sequence tests they locked out the high pressure injection pumps so they wouldn't start during the test.  And then the test was supposed to be reset by the next test.

When you run continuously, it happens really quick. When you wait for a minute, it doesn't happen so quick.

One of the units was operating, the other units was in refueling outage and they had to do a surveillance to see if one unit could use the HPI pumps from the other unit.  And so they ran the test, let's startup, for example, Unit 3's pumps on one unit.  And when they tried to do that, they couldn't start the pumps because they were locked out.

So that was the nature of how they discovered this defect was in place was it was actually a self testing thing where until you could actually unlock the pumps by doing the next self test, you see, you couldn't run the pumps.

Well, when a valid signal came in, you quit doing self testing. So during the 36 percent of the time that a particular sequencer was essentially making the HPI pumps inoperable, you wouldn't be able to get them back up. So that was the nature of the event.

And they actually found it fairly quickly when they discovered it. When the mechanical rely failed, they thought oh we got a software problem. Well, then they realized mechanical, no. And they went to modify the software in the load sequencer, they didn't really consider what would happen if a valid signal came in during one of those tests.

So anyway, that's the nature of the event.

MR. GEDDES: Thank you, Mike.

CHAIRMAN APOSTOLAKIS: So that was dormant for three years you said?

MR. BLANCHARD: Well, actually it was in automatic --

CHAIRMAN APOSTOLAKIS: Use your mic.

MR. BLANCHARD: Actually, I believe it was a year that they were in automatic test mode. They also had an option of manually testing. So during the two years that I think this situation was in place it was one year that it was in automatic test mode.

MR. GEDDES: And their immediate corrective action was to put it back in manual test mode, is that right, Mike?

MR. WATERMAN: Yes.

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: Can we speed it up a little bit?

MR. GEDDES: Yes.

MR. BLANCHARD: There was more thing that was done in reviewing each of these 1E events, and that was to take a look at its risk significant. And the way we did the risk significance determination was very similar to the significance of the termination process that's currently done under the Reactor Oversight Program.

In this particular instance we went ahead and put together the significance determination process stair step diagram and reviewed each one of the initiating events that is in the significance determination internal events process.

And the red X that you see for each initiating event reflects this ten percent of the time that the safety injection system would not have had an automatic signal for the small, medium, large LOCA. The steam generator tube ruptures, what you also see is credit for the operator backing up the safety injection signal in this particular significance determination analysis.

And so our determination on this particular one was that for most events we were still in the green area. There was one where it might be white, that was steam generator tube rupture, the white area being a little more risk significant than the green area. But on the other hand, had we gone on to a phase 3 significance determination analysis using their full scope PRA, we would have likely seen much more credit for the operator action for the steam generator tube rupture event than you get in the significance determination process.

And in fact the licensee, even though this was 1994 and they had just completed their IPE, did do a significance determination evaluation using their IPE and came up with very similar numbers to these with a little bit more credit for the operator in the small LOCA and the steam generator tube rupture events.

MEMBER BLEY: And this lockout definitely didn't lockout starting the pump manually?

MR. BLANCHARD: No, it didn't.

MR. GEDDES: Okay. Ray, if you can hit the back button there. We're back on slide 5. I'd like to show you another example. If we can look at one of the single failure. There you go.

This is event 1 it's on slide 11. This is a case of a common defect, a software design issue. Software version 6.1 in a core protection calculator was incorrect. The vendor discovered it and reported it to the licensee.

The defect manifests itself when there is a transmitter failure mode. In other words, an external device on a single failure can force the core protection calculator to substitute a last known value. In this case the requirements definition for the project or for the system, the specification for the system was complete and correct, it didn't get implemented properly in the code. Okay.

The requirement for this particular application is to trip a channel when there's a transmitter single failure that it shows up in two A to D processors are daisy chained together.

So in this case it's a common defect on a 1E system, but it can only manifest itself deterministically in a single failure mode.

MR. BLANCHARD: Now from a risk perspective here's where we recognize that there is a potential for common cause failure of the sensors. And in this particular case the software common cause failure would only manifest itself across a subsystem or the entire system if you had also at the same time a common cause failure of all the sensors.

And if you had the common cause failure of all the sensors, you've lost that subsystem anyway. So in this particular case, the software error in fact is subsumed by the sensor failures that have to occur in order for it to manifest itself.

MEMBER STETKAR: But if I understand what you just said, you're saying that if I have the trigger event of a single sensor failure, this particular condition will be manifested as a single channel failure?

MR. GEDDES: Yes, sir.

MEMBER STETKAR: However, if I had this type of -- I have to be careful with my terminology here -- fault existing in my software that had a different type of trigger event that was manifested in four channels, I would have all four channels failing?

MR. GEDDES: That's correct.

MEMBER STETKAR: Not in particular these sensor failures. But what I'm getting at is is this event in a broader sense evidence of the types of things that happen that have a potential to lead to problems in the plant?

Granted that each type of inherent fault will be manifested differently depending on the input trigger events and how it's wired into the plant, the output functions. So in terms of looking at operational experience as evidence of the types of things that happen in the world rather than literally looking at input triggers and output functions from that particular event, you might be led to different types of conclusions. Not with respect to safety, not with respect to counting events, not with respect to data but just in terms of what is the operational experience telling us about how often different types of faults occur.

MR. GEDDES: Ray, go back to --

MEMBER STETKAR: If you'll allow me to use the fault as an inherent --

MR. GEDDES: I think I understand. Go back to slide 5.

You can see the breakdown in the table of the four software events that were common defects due to software design, application design issues.  Two of them could only reveal themselves in a deterministic way.  Okay.  I'm using deterministic language here. In a single channel failure.  One of them resulted in a spurious actuation of a single channel and one had the potential to affect all four channels simultaneously due to the nature of the trigger and the software condition itself.

So three out of four of those events affect single channels.  And that may be some indication, again, to answer your question.

MEMBER STETKAR:  I'm not sure.  This event 1 that we're looking at here is one of the four on that slide 5, is that correct?

MR. GEDDES:  Yes, sir.

MEMBER STETKAR:  And in particular which --

MR. GEDDES:  It's one of those two in the upper right hand box.

MR. GEDDES:  In the upper right hand box?

MR. GEDDES:  Correct.

MEMBER STETKAR:  Okay.  However, if this same type of fault existed in a different plant and a different system what could be triggered by a common event? Let's say it was high pressure and real high pressure. I mean, pressure in the reactor vessel increases and it's across 357 channels because I have 357 channels. If this particular type of design error in the software existed, it would effect all of the output signals, is that correct?

I mean, I don't know if I'm interpreting the way these things --

MR. TOROK: If the pressure goes high and they're all supposed to react, that's not a failure, right?

MEMBER STETKAR: Yes. But this is a design error in the software. So the design error could prevent them from reacting, for example, under some -- I'm just trying to understand to see a layer deeper I get --

MR. TOROK: Well, you're right. That --

MEMBER BLEY: What kind of software error.

MR. TOROK: That would be, for example, an incorrect setpoint in multiple channels would do that, right? If the setpoints were all wrong, all the multiple redundancies wouldn't trip at the right time.

MEMBER STETKAR: I think we probably need to go on because --

MR. GEDDES: Okay.

MR. HECHT: Ultimately the cause was that the requirement wasn't implemented correctly, right?

MR. GEDDES: That's right.

MR. HECHT: Okay.

MR. GEDDES: And that's why we call it a software design issue.

MR. HECHT: So it could very well be that if a requirement is not implemented correctly, then it would affect a lot of things?

MEMBER STETKAR: Yes. My thinking is this particular event, whatever it is, is evidence of how often do software design errors occur.

MR. GEDDES: Errors occur. Yes.

MEMBER STETKAR: Now the effect of that in a particular application both in terms of the required trigger inputs and the functional impact on the output from the control system depends on the particular application. However, this particular event is evidence of a type of thing that can happen?

MR. GEDDES: Yes.

MEMBER STETKAR: Okay.

MR. GEDDES: Do we have time for a couple more examples?

CHAIRMAN APOSTOLAKIS: No.

MR. GEDDES: Okay.

MR. TOROK: You want to leave the actual comments up?

CHAIRMAN APOSTOLAKIS: I want to look at your actual reports sometimes soon.

MR. GEDDES: Okay.

CHAIRMAN APOSTOLAKIS: We would like to have your report whenever you feel it's ready.

DR. TOROK: Okay. And we'll --

CHAIRMAN APOSTOLAKIS: Because in real time we got a flavor of it.

MR. TOROK: Sure. We're basically preparing a white paper that puts the words around this presentation and we'll be submitting that through NEI over the next several weeks.

CHAIRMAN APOSTOLAKIS: I'd rather have actual data. Is that the --

MEMBER STETKAR: No. Don't say "data." Say event summaries.

CHAIRMAN APOSTOLAKIS: Event summaries.

MR. GEDDES: It will have event information. It will have this kind of information.

CHAIRMAN APOSTOLAKIS: But for all events?

MEMBER STETKAR: But not in any more narrative detail than this?

CHAIRMAN APOSTOLAKIS: I thought you were going to give the staff some report where you would take out the names of the plants.

MR. TOROK: Yes. Well we're --

CHAIRMAN APOSTOLAKIS: That's not a white paper?

MR. TOROK: No, no, no. Because the white paper is brief. It's the words around this presentation.

CHAIRMAN APOSTOLAKIS: Okay.

MR. TOROK: Then we'll be preparing a more extensive EPRI report with a lot more details in it. It'll be much thicker.

CHAIRMAN APOSTOLAKIS: Okay. And when will this be out?

MR. TOROK: Later in the year. Later in the year.

CHAIRMAN APOSTOLAKIS: Okay. WE would like to receive the documents as they are submitted.

MR. TOROK: And can we go to slide 7? Is it okay if we take a minute on wrapup?

CHAIRMAN APOSTOLAKIS: Sure. You can take more than a minute.

MR. TOROK: Wow. Okay.

CHAIRMAN APOSTOLAKIS: No more than two, though.

MR. TOROK: Okay. This is the recap here. Okay. In one line, I guess what the OE seems to be telling us is that the current methods that are used for protecting against software common cause failure have been good enough to make software a minor contributor to common cause failures and potential common cause failures. That's what we're seeing.

Now, we have some recommendations, though, which keep looking at the data. There's more data out there and this isn't a good time to stop. Hopefully, we can confirm the results we're seeing from other countries and other industries and continue to generate useful insights that we can factor into D3 guidance.

The other thing, though, is what we seem to be seeing is a need to refocus the current D3 guidance to credit the types of defensive measures and diversity attributes and so on that have proven effective. Because right now the D3 guidance doesn't do that. It pushes heavily for diversity, but it doesn't recognize defensive measures so much. But the defensive measures appear to be proving very successful here.

Now this is also a reference to a couple of reports that you've been hearing about earlier today, I guess. One of them is a white paper that we submitted recently. It was called "A Common Cause Failure Applicability." And it's about the use of defensive measures to protect against common cause failure.

CHAIRMAN APOSTOLAKIS: Do we have that, Ginija? Do we have this report?

(Off microphone comments.

CHAIRMAN APOSTOLAKIS: In the process of what? All I want is a copy.

MEMBER STETKAR: We don't need to review comment.

CHAIRMAN APOSTOLAKIS: Yes. We don't need to go review.

MR. TOROK: I'll give you one. And that's a white paper, it's brief. It explains what defensive measures are about and how we think they're useful in protecting against common cause failure.

Also for Mike Waterman, Oak Ridge has been doing work on diversity strategy. So we think it's a good idea to keep perusing that, and specifically the combination of diversity attributes and defensive measures to protect against common cause failure.  We think this is pretty important because it gets beyond the issue of just looking at process.  Process does not guarantee good design.  So we think it's important to be looking at the design attributes as well.

CHAIRMAN APOSTOLAKIS:  It seems to me that your recommendations --

MR. GEDDES:  We got a --

MR. TOROK:  Yes, we'd like on the record.

CHAIRMAN APOSTOLAKIS:  It seems to me that your conclusions and recommendations rely exclusively on the data that you have collected, which admittedly is not a very large database.

MR. TOROK:  Which is why we say keep looking.  That's right.

CHAIRMAN APOSTOLAKIS:  I mean, that doesn't seem to be any room for any other work that uses methods for identifying potential failure cause.

MR. GEDDES:  You mean go outside the U.S.

CHAIRMAN APOSTOLAKIS:  No.  I mean --

MEMBER STETKAR:  Well, outside the U.S. there should be more operational experience with safety.  Certainly with safety systems and probably an awful lot more with nonsafety systems.

CHAIRMAN APOSTOLAKIS: Well, we don't calculate the core damage frequency using operational experience. We do analysis, too. And there doesn't seem to be any room here for analysis. Is it because you are too excited by what you have done or is it an intentional thing to say NRC Research should drop all work that they're doing on trying to identify failure modes using methods?

MR. TOROK: No, there wasn't any attempt to say that.

CHAIRMAN APOSTOLAKIS: I hope you wouldn't.

MR. TOROK: No. But once --

CHAIRMAN APOSTOLAKIS: I mean, you're drawing conclusions here. You say recognize and endorse methods that have proven effective in protecting against software CCFs. Maybe they were effective protecting the CCFs you found. I don't know about the other CCFs.

MR. TOROK: Well, I think --

CHAIRMAN APOSTOLAKIS: We should be a little bit more cautious at this stage, Ray, do you agree?

MR. TOROK: Well, I think we should keep

looking at it. But the other thing that I think we're seeing here is that the digital platforms that are being used in safety applications are not ones that were designed yesterday. They have been designed and developed over decades and the designers have gotten pretty darn good at incorporating design measures that help protect against this kind of stuff. And I think that's what we're seeing.

These things aren't reliable by accident. They're designed to be reliable, and we're seeing that. And I think we should credit the design measures that are being used.

CHAIRMAN APOSTOLAKIS: I agree. I agree. I agree. On the other hand, I do remember -- it's nice that some of us stay on this Committee for a long time, you know. I remember when we first handled this issue in the late '90s that the staff was really enthusiastic about controlling the process of development of the software; nothing would go wrong. If we control the process, we are home free. And seven, eight years later, now we are changing our song, you know. And before Three Mile Island it was a heresy to say that the human error might occur in a nuclear plant. After that it was not a heresy anymore.

So it's our role to be cautious.

MR. TOROK: Sure.

CHAIRMAN APOSTOLAKIS: I thought you promised this was your last slide.

MEMBER STETKAR: You gave him an out. You told him he had two minutes and then you said something.

CHAIRMAN APOSTOLAKIS: Including, right.

MR. TOROK: I lied.

CHAIRMAN APOSTOLAKIS: Go ahead, Ray. Go ahead.

MR. TOROK: No. I just wanted to call your attention to the fact that there is a list of additional insights that appeared at the back. We knew we wouldn't have time to talk about all these things. And we wanted --

CHAIRMAN APOSTOLAKIS: We are looking forward to reading your white paper.

MR. TOROK: Okay. So just so they're there. And we'd be happy to come back and talk about any or all of it at your convenience.

CHAIRMAN APOSTOLAKIS: We really appreciate this. Because you are using real experience, and this is good and as you saw, the Subcommittee is very interested in this.

Thank you very much, gentlemen. We appreciate your coming here.

MR. GEDDES: Thank you.

CHAIRMAN APOSTOLAKIS: The NRC staff now will tell us about their work on operational experience review.

MEMBER STETKAR: Some of us are going to take a break.

CHAIRMAN APOSTOLAKIS: Oh, we want a break?

MEMBER STETKAR: Yes.

CHAIRMAN APOSTOLAKIS: Is it time for a break. Okay. We'll take a break. We'll take a break now, because I'm not sure there will be another presentation. Take a break for an unspecified period.

(Whereupon, at 3:04 p.m. a recess until 3:20 p.m.)

CHAIRMAN APOSTOLAKIS: Okay. We're back in session.

Now we're going to hear from the NRC staff, Mr. Waterman and Mr. Arndt, two old friends. they've been here many times.

MR. WATERMAN: I've gotten a lot of these Subcommittee meetings, to tell you the truth. I've thoroughly enjoyed them.

CHAIRMAN APOSTOLAKIS: Okay. Who is first.

MR. WATERMAN: I'm Mike Waterman with Office of Nuclear Regulatory Research, Division of Engineering. I'm in the Digital Instrumentation and Control Systems Branch. And today we're going to talk a little bit about where we've gotten so far on the review of operational experience and how we're doing on classification of digital systems.

We just finished the white paper. It went out a couple of days ago. It's ADAMS number is ML080590323 --

CHAIRMAN APOSTOLAKIS: Can you get us a copy to read?

MR. WATERMAN: Yes. Yes. You have a copy of the next to most recent draft.

MEMBER STETKAR: Yes, we have a copy of the draft.

CHAIRMAN APOSTOLAKIS: Yes, I know. I've seen that, but --

MR. WATERMAN: And to the credit of my management, they've pointed out a lot of things wrong with the draft. We updated and it really improved the quality of that draft. So I had a problem with my management on that.

CHAIRMAN APOSTOLAKIS: They can -- the process, I guess.

MR. WATERMAN: Before I get into this, I'd like to make a couple of comments. On the previous discussion, Myron brought out the point that computers are sequential state machines. Actually, not all computers are because some digital devices such as programmable logic devices, complex programmable logic devices and field programmable gate arrays are not sequential. They're actually simultaneous. Brings a whole new quirk on the inspection process. You have to be able to read VHDL.

The other thing is that plants typically depend upon having a different sensor for each channel. And so you can say, well, you might have some unique operating state in one channel because the sensor data matches up with exactly where that channel is. However, what we've seen is we've seen some designs come in where what the designs do is they share all four sensors and pick the one sensor that would guarantee the highest availability.

Well, Jack's been in plants before. He knows that every plant has its own personality. And if you go to one plant, they'll say, oh yes sensor C, that's always the one that goes first. Or sensor B, that's always the one.

Now if you take all those sensors and share them and you say well I'm going to take like the second highest sensor value, you may end up using the same sensor in all four channels all the time. And if that one particular sensor produces just the right signal that gives you a state that would cause your system to lock up or something like that, then we're talking common cause failure.

The other things is, is that in analog systems, for example this event 1 here, it was pointed out well yes this occurred in one channel because you'd need sensor failures or a failure in the sensor train, incidentally, not just the sensor. The sensor could be just fine and something in the train could fail. But there were other trips that would have tripped the plant.

Now along comes digital where we put all the trips functions on one microprocessor. Are we really sure that some other trip function will trip the plant? We're not really. Because what if some kind of a sensor or state on the machine causes all of the trips to fail? That's one of our big concerns.

But anyway, onwards and upwards, as they say.

The other point was is that out of 322 events, we didn't have very many 1E events. I guess the natural question to follow on is is well how many 1E systems are we talking about.  I mean, you know, 322 events.  Maybe we're only talking about 30 or 40 1E systems, and then 4 events.  Wow, really.

So, you know, just a couple of points on.

If we see a background, give you a little preliminary assessment 9/07.

We started developing our diversity strategies in September of 2006 and then on the basis of Commission meeting and some other recommendations we formed a steering committee in 2007. And the steering committee then formed a task working group to develop, among other things, diversity and defense-in-depth strategies and things like that.  So our research really kind of folded into that very nicely.

And we presented the approach that we were going to take I think somewhere in the summer of '07.

If we could see the next slide?

One of the things that came out of our discussions with you, George, and with the rest of the Subcommittee on this was in the summer of '07 I said well we want to develop some diversity strategies so we can answer the question how much diversity is enough.  I mean we've got seven issues, if you will, in the TWG number 2, six of those issues are issues with do we need diversity or don't we. And the other issue is, okay, you know you need diversity. Now what do we mean by diversity?  So my research was supposed to answer that question.

And George pointed out well if you're going to develop diversity strategies, don't you think you ought to know what the failures are so that your strategies address the most common failures, which is absolutely correct.

And additionally, when you have a diversity strategy, maybe you got to be sure that it's going to work with the type of system that you're going to apply it to. So you got to go out and classify your systems somehow so you can get it all put together; strategy A goes into a certain type of system, you know, they have certain types of failures and things like that.

And so we went out and we looked at a lot of different sources of data. And there's some sources of data that we have yet to acquire, but you know we intend to acquire them. And we looked at the NRC operating event report database. We looked at a common cause failure database and analysis system. I believe that's the one that was developed by Idaho National Lab. It used to be called the Nuclear --

CHAIRMAN APOSTOLAKIS: NPRDS.

MR. WATERMAN: Yes, NPRDS. Thank you.

And they gathered the INPO EPIX data. And so I'm not quite understanding why all of a sudden it's hard to get EPIX data when we've been gathering for some years now at Idaho National Lab.

The Organization for Economic Co-Operation and Development out of Halden has what's the COMPSIS Project, the Computer-Based Systems Important to Safety. And they're gathering all kinds of data from various countries because, you know, no one country has a lot of digital failure data so we're trying to gather it from all over the world and put that into a data base. And I'll talk a little bit about the quality of those databases.

And, of course, we have the INPO Equipment Performance Information Exchange database. It's part of developing diversity strategies and it's part of our emerging technologies program. Oak Ridge National Lab is also taking a look at various operating experience.

And then we've got the NEI/EPRI review that will be here sometime later this year. I made the comment I wish this was November so I could see it next month.

And the other sources of data we're looking at, that we're putting feelers out with Department of Defense. Of course, they're very reluctant to really talk about the kind of failures they have in their defense systems. So we're trying to figure out a way to get that.

And probably one of the best route cause investigating organizations, NASA. When they have a failure, they really dig in and figure out what the failure is. We're trying to acquire some more detailed NASA data.

Another source of data was the references that you sent me.

CHAIRMAN APOSTOLAKIS: Yes. Myron had the list of references and he sent to me, and I pulled out what I thought more relevant and created the list.

MR. WATERMAN: Yes. And I went and looked at some of those references. And three of them I can't get my hands on right now. A couple of them because I didn't want to buy them.

CHAIRMAN APOSTOLAKIS: And he can help you with that, I know.

MR. WATERMAN: Okay. And I didn't Dolores Wallace's treatise that she did for NIST in 1977. I went to the website. I just couldn't dig that thing up.

MR. HECHT: Not 1977. I think about 20 years later. It's not that old.

CHAIRMAN APOSTOLAKIS: Okay. You do have all these references?

MR. WATERMAN: Yes.

CHAIRMAN APOSTOLAKIS: Okay. So, please--

MR. WATERMAN: The orthogonal defect classification, I started to address it in the white paper and then I backed off because I didn't have enough time to really expand on it enough to give justice. And that was one of the references you gave me, and I'd already been to the website. I saw all the red marks, and hey, you've been here.

The Mar's plant orbiter, this is really interesting. I don't know if you've talked to Sergio

Guaro over here. He's got an excellent presentation on some of the NASA missions that have gone awry and why. And it's a lot of this stuff about, boy, where were your domain experts on that one. You know, which is one of the big problems is you get software engineers, they look at a spec and away they go. And if you don't have domain expertise there to kind of coach them along with, this is what we're really talking about, things can go awry on the system development there.

The Arian V I looked at quite a bit prior to that. That's a good discussion of redundant computers, same reason, of course. And that's the software reuse issue and the design issue.

I went to Sciencedirect -- oh, *Reliability, Engineering and Systems Safety*. That's quite a rag. But that was John Bickley's report. It was a very good report, incidentally.

CHAIRMAN APOSTOLAKIS: It's accurate.

MR. WATERMAN: And quite enlightening. And I looked through that --

CHAIRMAN APOSTOLAKIS: There's some numbers which I'm not sure about.

MR. WATERMAN: I'm not so sure about the numbers.

CHAIRMAN APOSTOLAKIS: But he collected a lot of information.

MR. WATERMAN: I'm more keyed in what the actual data was anyway.

CHAIRMAN APOSTOLAKIS: Right.

MR. WATERMAN: The Aviation Safety Reporting System, I thought oh by, this is good stuff here. Thirty years, wow.

I printed out the altitude deviation sections, 144 pages. I didn't realize it was that big when I hit print. And most of it is pilot narratives about well the plan went up real fast and we took it off autopilot and got it back down under the right altitude and put autopilot on, and nothing else happened. Not a lot of root cause data in there about this is why it happened. So it probably needs more digging.

And I looked at a safety critical mailing list. It's pretty interesting. It's out of CS York UK. Yes. It's a message board and you have somebody pose a question and a lot of experts come in and give their opinions on it, stuff like that.

I kind of pawed down through it. This is just one thread with 852 messages in it. If you ever go to a message board? Eight hundred and fifty-two messages is a pretty good it.

MEMBER BLEY: Did you ask the question?

MR. WATERMAN: No, I didn't. That's the stuff I just got into just recently here, and it looks like it may have some promise also.

The stuff that ORNL is looking at for I&C failure, they've actually looked at 27 different sources. Everything from aviation safety information, analysis and sharing that's the ASIAS system. The pyrotechnic -- the pyrotechnic? The petrochemical -- the pyrotechnics might be an interesting area to look at. Pyrotechnics is what goes on in here.

The petrochemical industry, their offshore reliability database, that looks very promising. They do have some root cause analysis it looks like in there.

The telecommunications industry, who hasn't heard of switching system seven. I mean, that as an O instead of a zero and bang, down goes the northeast telecommunications grid.

The U.S. rail industry data. They're a little bit more loath to provide data. They kind of keep it close to the chest. And primarily most of their safety systems, you know, they're sort of modeled after the New York subway system. I don't know if you've ever seen any technical articles on the New York subway system, but they're using relays that were built in the '30s and they're still running them. And they had some pictures in this one article, and those babies were -- they look like trash. I mean, the paper was coming off of them and everything else; still long.

MEMBER BLEY: As long as you got a burnishing tool, you can keep them running .

MR. WATERMAN: Yes. And, of course, we're looking at nuclear industry both national and international, COMPSIS and stuff like that.

Let me see here. If I could see the next slide, please. I'm supposed to be buzzing along here and digressing. Ah, OE review conclusions.

The white paper discusses a few things. Number one, the reason that I'm really interested in the failure data is because I want to develop diversity strategies that address the most common types of failures. What we find when we actually go out and look at failure data is you look at something that's suitable, perhaps, for a PRA but at that level it's software failed, right? And you don't know if the software failed, a lot of times, because it was a specification or design error. If it was a translation error where you're translating specification and designs into something that looks like software, or whether it was just an operator error. We've seen all three of those, right? We've seen all three kinds of failures.

When you go out and you look at all this failure data, you don't even that kind of granularity. So I'm kind of struggling here thinking where's my failure data. And every so often we come up with real failure data like the core protection calculator system failure data where it is, they changed the software to use the last good value when a bad value came in, right? Ahh. You know, that's a design error.

Or the Turkey Point load sequencer issue where, ah, now that's a design error, too, and it might be a translation error; the translation being the verification and validation of getting it all into the system. But for a lot of these error reports it's like computer reset. Really? You know what caused it? And there's no digging down in there.

And part of the reason for that is when you think about it, it sort of makes intuitive sense.

Is that if you really want to do good root cause analysis, you have to understand the system you're doing the root cause analysis on. You need somebody with experience who says, ah yes, I've been working with this system ten years. And when it does that, this is what causes it.

We've got technical changing so fast, who has got ten years experience on a Pentium 2 chip for crying out loud? It hasn't been around for ten years. That kind of experience. And so that really complicates root cause analysis when you need somebody who is smart enough to dig in and understand exactly what happened.

So the root cause analysis issue is probably going to plague us in on out, right?

So that's where the complications come from on gathering the operating even data is just being able to tunnel down far enough into it to understand is this a software timing error? Is this a function error? The function was incorrect? Is an error like the Arian error where it isn't a software error and it's not a hardware error. Arian wasn't either one, a software or a hardware error when you think about it. Arian was an integration error.

You took software that needed to take a

64 bit number and because of the hardware, strip it down to 16 bits and all the accuracy is gone, right? Had they had better hardware, they wouldn't have had to do that operand, right?

So, you know, sometimes it's not just software, not just hardware. It's what happens when you integrate one on top of the other. And if there's incapabilities there where the software may overstress the capabilities of the hardware, you're going to run into issues there, too.

So that's just my own experiences seeing things going on in the industry.

Now the rest of that classification, Steve's developed a classification methodology. The orthogonal defect classification looks promising, but we really haven't dug into it yet. But Steve's got a pretty good handle on classification. And I've been trying to follow in his footsteps.

MR. HECHT: Mike, if I could make some comments.

MR. WATERMAN: Sure.

MR. HECHT: First of all, NASA has a publicly available lesson learned information system website. And it comes off of -- and I know this because I use it a lot. NASA.pbma. PBMA is something, I don't even know what it.

MR. WATERMAN: PBMA?

MR. HECHT: Yes. But if you just put NASA lesson learned information system. It has a lot of NASA incidents, but if you just search for software, you'll get a lot.

The other thing about the ODC in particular about classification, a multi-dimensional classification system I think is important. Because, for example, if you look at errors from -- failures from the telecommunications system arena, what are their software development practices? What's their platform? How does that differ from what you're doing?

So causes have many meanings. Some causes, ultimately the causes are the seven deadly sins, right? Because software development is a human activity.

MR. WATERMAN: Yes.

MR. HECHT: But when we try to break it down a little bit more, the ODC in particular by giving you several dimensions is giving you the -- allows you to separate how the error manifests itself from what the development problems might have been from what the actual type of the error was. Was it interface, was it arithmetic, was it something else. Having a multi-dimensional classification is important.

And finally with respect to saying oh, the computer reset. Well, gee, that's wonderful news to know. Because if I know how often the computer resets and I have the operating time, and that allows me to determine a failure rate. And the only thing it does bad is reset or the only thing the platform does bad, for example, is reset then we know a lot. And that's something we can't know from anything in the source code probably, if we look at the source code.

And so I just wanted to make that point that if you do have operating time and you have thousands of hours of actual observation, real observation, you know where people are looking at it and you have confidence that they're actually writing the things down that occur. And it turns out to be "uninformative," that often might be very definitive particularly if we're talking about that offshore equipment database, which were the equipment a lot of it seems to be common to what would be in nuclear power plants.

MR. WATERMAN: Yes. My concern was that a computer reset doesn't tell me which of the NUREG-

6303 diversity attributes I should emphasize, you know the design equipment --

MR. HECHT: All right. But perhaps it's telling you that you have to have two separate computer platforms if every one is resetting on the average every six months and it's down for three minutes until it comes back up. Then you can --

MR. WATERMAN: Yes. One of the other questions that arose is if I have two different computer platforms, you know how diverse are they? Is an AMD diverse enough from an Intel that I can claim diversity.

MR. HECHT: Yes. And it may not be the AMD versus the Intel. It might be vendor A versus vendor B because the reset might be a result of some thermal problems.

MR. WATERMAN: Sure. Yes.

CHAIRMAN APOSTOLAKIS: Let's move on. Steve.

MR. ARNDT: Okay. Next slide, please.

We briefed this last time and I'm just going to give a quick update.

As you're aware, there are a number of different ways you can classify digital system. And the Committee asked us to look at a particular way, which was something we were also looking at in terms of reliability at one time, and we wanted to expand it a little bit to look at some of the issues.

The issues that the Committee talked about was understanding how systems could be classified in terms of their functional importance to the plant system and how you could analyze them in a particular way, i.e., are there certain characteristics of digital systems that make them more important or less important, or simpler, or less simple and you could apply a different strategy in terms of the review, be it actual guidance, or the amount of effort or where you place the effort on the various efforts, et cetera.

So in that line we looked at a number of different classification strategies that are out there both in regulatory space and in analysis space. And this is explained in the white paper, to some extent.

CHAIRMAN APOSTOLAKIS: Now, when NRR receives some application from someone else, which part -- how is a system classification scheme going to help the reviewer?

MR. ARNDT: Well, if you recall --

CHAIRMAN APOSTOLAKIS: Does the reviewer

care much about complexity, especially when you say from simple to highly complex, or maybe the reviewer simply wants to know this is an actuation system, this is a feedback and control system.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: In other words--

MR. ARNDT: I understand your question.

CHAIRMAN APOSTOLAKIS: -- have you taken the point of view of the user?

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: Now we're not done yet, and I'll explain to you why that's an issue. If you go back to this morning's presentation on licensing process, we basically use a two step classification scheme right now by default without calling it that.

If the safety system we look at it, if it's a nonsafety system we don't look at it, or at least we have a lower threshold.

When it is a safety system we look at it in terms of relative complexity and how new it is in terms of what we looked at before or not looked at before. In essence, that is a simplified version of our complexity matrix.

Is it a lot of different multi-processing systems, is it a very simple system, does it have a lot of inputs, does it have a long development process, et cetera. And based on that we look at different things in different ways.

The current guidance, as was discussed this morning, in BTP 14 is for everything and then we pick and choose based on the complexity of the system.

The concept here is to take that one step further and say based on what it's being used for, i.e., is it being used for a safety function, is it being used for a safety function that is highly important versus something that's less important, is it being used in such a way that you have to look very closely at its connectivity, is the terminology I use, but basically how closely it's coupled to the rest of the system. It's going to be more difficult, it's going to contain more staff resources to look at something that is a highly coupled system then one that's a stand alone, say for example, a turbine load sequencer as opposed to an integrated control system or a RPS, or an SS system.

So the concept here is to qualitatively in the beginning come up with a mechanism by which you can apply some of this new guidance that we're developing in a graded way so that you can look at things that are likely to be more important, more complex and more difficult to analyze from an inter-connectivity way and apply resources appropriately in something that is a consistent and reasonable fashion.

We didn't talk about it this time. We talked a little bit about it the last Subcommittee meeting. We actually have a criteria in the communications ISG that basically says if a system is so simple that you can test it completely, then you don't have to do as much of the software system. So it's basically the same general concept. If you are very, very far on the complexity side or the simplicity side, if you prefer, then you don't have to do the amount of review in terms of the software.

CHAIRMAN APOSTOLAKIS: But are you going to use metrics? I don't remember. Maybe you talked about it last time. For a complexity? Because you mentioned, I believe, a number of matrices.

MR. ARNDT: There's a couple of different areas where we are looking at for the metrics associated with this. And there's a lot of different potential things. And we're looking at two or three different ones.

CHAIRMAN APOSTOLAKIS: Or you can just use a qualitative thing, the way you just described it.

MR. ARNDT: Or you can use it entirely in a qualitative sense.

CHAIRMAN APOSTOLAKIS: Because, you know--

MR. ARNDT: Yes. Right now what we're looking at is seeing how we could do some of these things and seeing if it's going to be used. We don't want to get ahead of ourselves. If this isn't going to really help a whole lot --

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: -- then we're not going to make it a complicated process. If it does look like it's going to help, then we'll do more development.

CHAIRMAN APOSTOLAKIS: So the driver really should be the NRR reviewer?

MR. ARNDT: Exactly.

CHAIRMAN APOSTOLAKIS: And you are now one of them?

MR. ARNDT: I am an advisor to the NRR reviewers.

CHAIRMAN APOSTOLAKIS: You've moved to the other side?

MR. ARNDT: I've moved to the other side, that is correct.

But, hopefully, it will also give us some insights in terms of analysis and things like that.

CHAIRMAN APOSTOLAKIS: Okay. Good. Let's go on.

MR. ARNDT: Okay.

The next slide, please.

CHAIRMAN APOSTOLAKIS: Are you done?

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Go ahead. Okay.

MR. WATERMAN: For future activities, obviously we want to obtain more operating event information from various sources, not just the nuclear industry but other industries.

March 31st: Develop an inventory of existing and new digital systems and structure that to align with the system classification methods. We're moving in that direction now. I don't know why that date is there.

CHAIRMAN APOSTOLAKIS: So March 31st is what? In ten days or so?

MR. WATERMAN: Yes, ten days.

CHAIRMAN APOSTOLAKIS: Very good. See, you have to look at that from different perspectives.

MR. WATERMAN: Actually, the March 31st was not so much just the inventory, but the March 31st date was having our diversity strategies in a draft form delivered to us so we could start lining those up with some kind of a classification method. And about 5:00 this morning I opened the draft NUREG. So I'm starting to work on that now.

CHAIRMAN APOSTOLAKIS: Good.

MR. WATERMAN: So it looks pretty good.

Finally --

CHAIRMAN APOSTOLAKIS: But shouldn't this be also effected about what the NEI/EPRI are doing?

MR. WATERMAN: I certainly hope it is. And I'm anxiously awaiting their call. So I haven't got their data yet. It'll be interesting to see how they scrubbed it and things like that.

MR. ARNDT: What we're trying to do is look at all the different inputs, both our own work--

CHAIRMAN APOSTOLAKIS: Yes.

MR. WATERMAN: -- what NEI and EPRI has done, what we've seen from other efforts and integrate that both in terms of trying to assess whether or not this is telling us something new that would us lead us to modify our guidance or make improvements in the process.

CHAIRMAN APOSTOLAKIS: Okay. Yes.

MR. WATERMAN: And that's about it. But I would like to make one comment to Dr. Bonaca. And he was right on the mark.

CHAIRMAN APOSTOLAKIS: Bonaca? Stetkar.

MR. WATERMAN: Oh, I'm sorry. Stetkar.

CHAIRMAN APOSTOLAKIS: Bonaca has no use--

MR. WATERMAN: He would be interested. And the comment was was that the feed water systems versus safety systems. If you look at software integrity level classification systems, such as what you'll find in IEEE Standard 1012, when we wrote 1012 we wrote it with a software integrity level structure so that you could understand the level of effort you applied to different importances of software. And software integrity level 4 was not just loss of life. Software integrity level 4 was major financial impact on a business. And I would propose the loss of a feed water system, while it may not be major financial impact, would quality as a software integrity level 3 system. You don't want to lose feed water in a plant that's generating a million dollars a day revenue, right?

So I think it may be a little -- I don't know. I wouldn't classify safety and nonsafety systems as so much radically different when your nonsafety system has such a huge impact on the company's bottom line. And therefore, I thought Dr. Stetkar's comment was very well put.

CHAIRMAN APOSTOLAKIS: Yes. Okay.

MR. WATERMAN: Was very well put that, yes, we can say the only thing we need to worry about is class 1E and all these non class 1E failures are because the system's not as good. Yes, come on; even ATWAS systems have redundancy built in.

CHAIRMAN APOSTOLAKIS: So your second thing is just comment.

MR. WATERMAN: So I agree with that completely, is there is value in plant system data.

CHAIRMAN APOSTOLAKIS: Very good. Thank you, gentlemen.

We will review in more detail the traditional methods for digital reliability model work at the Subcommittee meeting whose timing will be decided in a few minutes. So my colleagues are apologizing to BNL for not being allowed to make a presentation.

Now, Mr. Arndt?

MR. ARNDT: Yes, sir.

CHAIRMAN APOSTOLAKIS: The first order of business is what you guys will present at the April meeting?

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: Which I understand we have an hour and a half in the morning on Friday. Because my colleagues like me and they want me to write a letter in the afternoon on Friday.

MR. ARNDT: I believe that is correct.

CHAIRMAN APOSTOLAKIS: That they like me? Yes.

MR. ARNDT: That they want you to write a letter in the afternoon.

CHAIRMAN APOSTOLAKIS: Okay. So what is it that you want to --

MR. ARNDT: We would obviously be interested in the Subcommittee's opinion. But right now what we would plan on presenting is a short review of the cyber ISG. Probably two or three slides.

CHAIRMAN APOSTOLAKIS: How about all three areas?

MR. ARNDT: Well, let me finish.

A short review of the licensing process

ISG. A short review of the PRA for Part 52 licensing guidelines ISG. We would also probably present at that time since we got significant feedback from the Subcommittee, our plans associated with that feedback. We probably won't have the time that gets you a new draft of that, but we will provide as part of the presentation on --

CHAIRMAN APOSTOLAKIS: So our letter then would be a little bit more specific on this feedback?

MR. ARNDT: IF that's --

CHAIRMAN APOSTOLAKIS: Because you will not have implemented it?

MR. ARNDT: We probably won't have the new draft.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: But we will provide to you and the Committee, if you would like prior to that time, maybe a page or two on how we're planning on revising it so you have a understanding.

CHAIRMAN APOSTOLAKIS: That's good. No, I think it's a good idea.

MR. ARNDT: You understand what we agree with and what we don't agree with.

CHAIRMAN APOSTOLAKIS: Yes.

CHAIRMAN APOSTOLAKIS: And how we're

planning on doing that.

We could then briefly go over the OE experience, ours and the industry's that we just heard or not, as you prefer.

CHAIRMAN APOSTOLAKIS: Well, the criteria here is you present it, the letter will say something about it. So you think it's ready for an ACRS letter?

MR. ARNDT: Probably not.

CHAIRMAN APOSTOLAKIS: So don't present it.

MR. ARNDT: Okay.

MEMBER SIEBER: You're off the hook.

CHAIRMAN APOSTOLAKIS: Huh?

MEMBER SIEBER: You're off the hook.

MR. ARNDT: Well, it depends on what you guys want to put in --

CHAIRMAN APOSTOLAKIS: Or we can say this is for information.

MR. ARNDT: We can put it for information or we could discuss it briefly and you could include in your letter that you believe it's important and it's going in the right direction or not going in the right direction, or whatever your comments are.

CHAIRMAN APOSTOLAKIS: But if you present, shouldn't EPRI present?

MR. ARNDT: We would be more than happy to have the industry provide a short brief, either on --

CHAIRMAN APOSTOLAKIS: Yes, he's here.

MR. ARNDT: -- NEI or EPRI.

CHAIRMAN APOSTOLAKIS: His body is here. The question is whether the staff should make a presentation to the ACRS full Committee on their work on operating experience. And if so, whether you would like also to do that. And I'll tell you when it is. It's Friday morning, April --

MR. ARNDT: 11th.

CHAIRMAN APOSTOLAKIS: April 11th.

MR. ARNDT: It would have to be very short.

CHAIRMAN APOSTOLAKIS: But you will be wiling to do it?

MR. ARNDT: Yes, sir.

CHAIRMAN APOSTOLAKIS: That doesn't mean we're going to schedule it, but at least we know that you're willing to do. Because I don't want to overwhelm the whole thing.

MR. ARNDT: I agree.

CHAIRMAN APOSTOLAKIS: In saying, yes, we have to cut you off before --

MR. ARNDT: No. I understand.

CHAIRMAN APOSTOLAKIS: Are the three ISGs you think enough to fill an hour and a half?

MR. ARNDT: Well, I would presume --

CHAIRMAN APOSTOLAKIS: I said two hours earlier, you corrected me to an hour and a half.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: So we have you and NEI then?

MR. ARNDT: Yes. I think what would be reasonable is what we did last time, which was basically NEI provided a short brief, like what they did today basically on their general thoughts on the process. And then we reviewed briefly for the Committee the three ISGs that we had briefed the Subcommittee on. I think that's appropriate.

If we'd like to also talk a little bit about OE, that's up to the Committee.

CHAIRMAN APOSTOLAKIS: I think that's a good idea. Huh, what do you think?

I mean, eventually all of this stuff will be presented to the full Committee.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: the question is how much do we schedule for the April meeting --

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: And how much is ready for comment from the full Committee?

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: So so far what I've got in these are the three ISGs, your plans for possibly revising the PRA ISG.

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: And then your presentation on operational experience and classification. Sort of a status report?

MR. WATERMAN: I thought we were going to hold off on that.

CHAIRMAN APOSTOLAKIS: Well, I don't know.

MR. ARNDT: Well, it's entirely up to you.

CHAIRMAN APOSTOLAKIS: We've got two hours now, Mike.

MR. ARNDT: I don't think we need to do that.

MEMBER STETKAR: George, for general interest to the Committee I think there might be at least some -- not so much on what you looked at and where the problems are and where you plan to look at more experience, but a little bit more background on the classification scheme. Because regardless of what you look at, that's eventually where things will be binned. And it kind of gives the full Committee some information about the direction you're headed. It had infinite data. It will eventually be organized --

MEMBER BLEY: And if it's not on the agenda, it will sneak itself on anyway.

MEMBER STETKAR: Yes, that's right.

MEMBER SIEBER: So if you define whatever it is you're talking about --

MEMBER STETKAR: That's right.

MEMBER SIEBER: -- and what you're--

CHAIRMAN APOSTOLAKIS: And this will be an information briefing.

MR. ARNDT: Yes. Yes.

MEMBER SIEBER: Right.

CHAIRMAN APOSTOLAKIS: And we still have NEI and EPRI there?

MR. ARNDT: Yes. I think one of our bosses wants to make a comment.

CHAIRMAN APOSTOLAKIS: Go ahead.

MS. UHLE: This is Jennifer Uhle from Research.

And I was just going to point out, I mean whatever the full Committee, we'll present. So at this point the operating experience and the classification is a work in progress. And so how you've recently phrased it, Dr. Stetkar, is appropriate that we could provide what we've done so far and what the path forward is, and how we intend to use it. And I think that would probably, how we intend to use it may be something we can elaborate on a little bit further.

CHAIRMAN APOSTOLAKIS: This, as I say, this will be an information briefing?

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: This part? Although the Committee may want to comment. I mean, who knows.

MR. ARNDT: Who knows? But, yes.

CHAIRMAN APOSTOLAKIS: But it will be understood that it's a work in progress.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: Okay. So we'll have these things.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: I think two hours, don't change it anymore.

MR. ARNDT: No. And we'll have a short presentation by the industry.

CHAIRMAN APOSTOLAKIS: Why do you say short? We will have a presentation by the industry.

MR. ARNDT: All right. We'll have a presentation by the industry.

CHAIRMAN APOSTOLAKIS: How much time did you guys have today?

PARTICIPANT: We started out with two hours --

CHAIRMAN APOSTOLAKIS: No. I thought you had what? I'm confused now.

MEMBER STETKAR: No, there was a lot of discussion.

MR. ARNDT: The original schedule for both the NEI and EPRI was about an hour. They ended up taking about an hour and a half.

CHAIRMAN APOSTOLAKIS: We took an hour and a half?

MR. ARNDT: About that.

CHAIRMAN APOSTOLAKIS: Today?

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Boy.

MR. ARNDT: Time flies when you're having fun.

CHAIRMAN APOSTOLAKIS: You're not going to have an hour and a half there.

MR. ARNDT: No.

CHAIRMAN APOSTOLAKIS: So you will have a brief -- actually the litany of the six -- did you present those?

PARTICIPANT: Yes, sir.

CHAIRMAN APOSTOLAKIS: I don't think we need that for the full Committee. They know you guys are active.

What we need is what Ray presented.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: With the support of his guys, especially real incidents. I think that's really important for the Committee.

MEMBER STETKAR: Well, the only problem is in time. Once you start talking about real incidents --

CHAIRMAN APOSTOLAKIS: Yes. But if we buy you lunch and you send you ought of the room, then we'll be quick.

MR. ARNDT: I don't eat lunch. But if it'll send you ought of the room, that would be great. I would appreciate that.

CHAIRMAN APOSTOLAKIS: Okay. We're done

with that?

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Then we want to have a Subcommittee meeting --

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: -- to pay due respects to BNL, OSU and everybody else.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: What I really want to do there is to go into more detail of the various modeling approaches that these groups are taking and remember earlier today I said that we need somebody to integrate all these things.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Because what happens is person A or group A writes a report, pays lip service to what other people have done. In passing he tells you how bad the other guy's approach is, and then he gives you 300 pages of the great stuff that they developed. And I want somebody neutral who is not developing anything to see how much of these things can use, especially in the failure mode and identification. Now that cannot be done at that Subcommittee meeting. I mean, you don't even know if you're going to have a project like that.

But would two days -- yes, Jennifer?

MS. UHLE: Thank you.

Yes, we would expect that the person who actually did some of the work for OSU, UVA would potentially be in the audience. But our preference would be a staff member doing the presentation who would have that neutral position.

CHAIRMAN APOSTOLAKIS: Only for that part?

CHAIRMAN APOSTOLAKIS: Yes.

CHAIRMAN APOSTOLAKIS: Not for two days?

MS. UHLE: No, not for two days. In fact, we propose that we have a one day meeting rather than a two day meeting.

CHAIRMAN APOSTOLAKIS: Yes. Let me counterproposal. What I really want to do is avoid what we did a couple of years ago with OSU where they came in here with one or two NUREGs and we had, what? Half a day, two hours?

MR. ARNDT: I don't recall.

CHAIRMAN APOSTOLAKIS: I mean --

MR. ARNDT: It was a relatively short amount of time.

CHAIRMAN APOSTOLAKIS: And then the next

thing I see is this NUREG is out, has been reviewed by the ACRS, you know, everything is fine.

So after the initial shock of seeing how many attachments that BNL sent us, the report with five appendices, I thought it would be a good idea to spend maybe a whole day on just that. Okay.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: So when these guys say that they define narrow course in context and they can get a failure rate, the rate of occurrence --

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: -- I'd like Bley to hear that.

MR. ARNDT: But let's try to define parameters.

CHAIRMAN APOSTOLAKIS: Huh?

MR. ARNDT: Let's try to define parameters. You would like to have a Subcommittee meeting of a significant length --

CHAIRMAN APOSTOLAKIS: Two days.

MS. UHLE: Well, we -- excuse me. This is Jennifer Uhle from Research.

We, speaking with Christiana Liu, who is obviously the Division Director in charge of the risk work from a traditional standpoint, and we do fee that based on the amount of information that we have so far that we could do a very detailed briefing for you, but one day would be the appropriate amount of time to cover it. And then if you did have particular areas that you wanted further information in, we could then potentially schedule another meeting that delved into those more specific details. But we think an overview with appropriate detail would be adequately covered in a day.

CHAIRMAN APOSTOLAKIS:  That prolongs it too much.

I also would like to see OSU present what they have done. Is that possible?

MS. UHLE:  We can look into that.

CHAIRMAN APOSTOLAKIS:  That's why it's a two day meeting, or a day and a half.

One day means that by 4:00 some people are getting out. So it's really not a full day. So the meeting will be at least a day and a half.

Now we can argue about it, negotiate about the hours, Jennifer.  But I started with two, now I'm down to one and a half.

MS. UHLE:  I'm trying for at least a day.

CHAIRMAN APOSTOLAKIS:  So you say you

want me back to two.

MEMBER SIEBER: If you say it goes two, that means three.

MEMBER STETKAR: That's right.

MS. UHLE: Would it help if we get the documentation to you earlier with --

CHAIRMAN APOSTOLAKIS: We do have that documentation.

MS. UHLE: Well, right. But with a little bit more, perhaps as the slides as well as perhaps a written description.

CHAIRMAN APOSTOLAKIS: Why is it so difficult to have a day and a half?

MS. UHLE: It's a matter of there's a lot of work going on right now in the digital I&C area and staff time away, and then as well as the contractor time.

CHAIRMAN APOSTOLAKIS: Well, not everybody needs to be at the meeting for the full day and a half.

MS. UHLE: We also don't want to bore you.

CHAIRMAN APOSTOLAKIS: You will not bore us. We will do the best we can to be entertained.

MS. UHLE: And if we finish early, then

we finish early.

CHAIRMAN APOSTOLAKIS: I started reading the BNL report and the appendices. There's no way we can do this in half a day. I mean Appendix C by itself is full of meat and somebody has to go over it, and that somebody's us, among ours being modest.

MR. ARNDT: Okay.

MR. WATERMAN: We also have another NUREG in the pipeline.

CHAIRMAN APOSTOLAKIS: I think the meeting will be a day and a half because that's convenient for our California folks. They can leave and maybe also have the afternoon.

MR. ARNDT: Okay. Now in terms of the broader context, I understand you want a meeting, no time, on the research aspects that you've discussed.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: We also have a number of regulatory actions we had discussed this morning about scheduling a meeting to update you on the progress of the Oconee licensing pilot plan. We will have some time early summer the manual operation action ISG, which is something that the Subcommittee had previously expressed some significant interest in.. This is the effort by the human factors group to define a process by which a particular time frame --

CHAIRMAN APOSTOLAKIS: The 30 minute thing?

MR. ARNDT: Yes, the alternate to the 30 minutes.

CHAIRMAN APOSTOLAKIS: Yes. You guys listen, huh?

MR. ARNDT: Occasionally.

CHAIRMAN APOSTOLAKIS: Very interesting.

MR. ARNDT: And then, obviously, the ongoing work in operational experience and the classification --

CHAIRMAN APOSTOLAKIS: So are you threatening us with more Subcommittee meetings?

MR. ARNDT: No. I'm saying in addition to the Research Subcommittee, at some point up to the Committee --

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: -- we need to have another interaction on these issues.

CHAIRMAN APOSTOLAKIS: Yes, I agree.

MR. ARNDT: Would you like those to be separate meetings?

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: Separate from the one that's coming up?

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: I want once to spend time looking at what those model developers are doing.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: Okay. And why they put the comma where they did. It's going to be a line-by-line review for those who are listening. Okay?

MR. ARNDT: Yes, sir.

CHAIRMAN APOSTOLAKIS: Now, I propose because there is a Subcommittee meeting on the 13th of May, which you probably would attend. That's a Thursday.

John is pessimistic that you will be allowed to attend that.

MEMBER BLEY: I'm on that one, too, but I don't think --

CHAIRMAN APOSTOLAKIS: Yes. So if we schedule then the Subcommittee meeting on Tuesday and Wednesday and adjourn by lunchtime, you can catch a plane back to California.

MEMBER STETKAR: Right. Sure.

CHAIRMAN APOSTOLAKIS: Yes. The full day Thursday, and half day Wednesday.

MEMBER STETKAR: It's just a matter of whether I go home.

CHAIRMAN APOSTOLAKIS: The 13th of May and half a day the 14th.

MEMBER STETKAR: Okay.

CHAIRMAN APOSTOLAKIS: Lunch, 1:00, 2:00, 3:00 you can go home.

MR. ARNDT: We'll have to look at our staff availability and contractor availability and get back to you.

CHAIRMAN APOSTOLAKIS: If you say no to this, we're going to go to August. And then maybe December. It's really terrible, I'll tell you.

MR. ARNDT: I understand the issue. We would prefer to --

CHAIRMAN APOSTOLAKIS: We are meeting with the Commission, by the way --

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: -- in June, June 5th. And they are very much interested in I&C, as you know.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Especially Commissioner Lyons.

MR. ARNDT: Yes, we are quite aware.

CHAIRMAN APOSTOLAKIS: And one of the -- I mean we can't put I&C on the table unless the ACRS has written a letter recently.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: They don't trust to just talk.

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: So that's why we really need the letter in April.

MR. ARNDT: And, as you know, just prior to that we will be meeting with the Commission.

CHAIRMAN APOSTOLAKIS: Good.

So I think we reached an agreement.

MR. ARNDT: Okay. In terms of a Subcommittee on the licensing issue, we will work with your staff on an appropriate date.

CHAIRMAN APOSTOLAKIS: Yes. June is out of the question, and July most likely is out of the question, too.

MR. ARNDT: We'll do what we can.

At this point before we get any further back, would you like to make any closing comments?

MR. WATERMAN: I did have one.

CHAIRMAN APOSTOLAKIS: Okay. Yes. Yes.

MR. WATERMAN: We have NUREGs coming in from the University of Maryland just on our proposed--

MR. ARNDT: Would you turn the microphone on?

MR. WATERMAN: We have a NUREG that's just gone over to NRR and NRO review now on the work that University of Maryland was doing.

CHAIRMAN APOSTOLAKIS: Which group over at University of Maryland?

MR. WATERMAN: Carol Schdmit's group on the reliability prediction system where they use metrics as a mean of detecting reliability.

CHAIRMAN APOSTOLAKIS: Didn't you do that three years ago?

MR. ARNDT: You reviewed a preliminary report on that.

MR. WATERMAN: You reviewed a preliminary -- the validation report is in now where they applied those metrics to validate NUREG-019. And that is in review. I've asked for comments back by May 1st. My period of performance on that project runs out the 1st of June or 30th of June.

CHAIRMAN APOSTOLAKIS: Would you like them to come also in May?

MR. WATERMAN: That's a big report. Well, we need to get it reviewed. It's about 400 pages of equations and tables, so --

MS. UHLE: Can I make just a suggestion here? I mean, there's a lot of NUREGs that we have going. We have quite a bit of activity going on in digital I&C. But I mean with regard to the purpose of the Committee in the sense of reviewing of everything, would you feel it'd be more appropriate if we take a bunch of the work that we're doing and integrate it together and talk about how it will be used in the regulatory context rather than going through a report that's 400 pages and looking for more of the theoretical issues?

CHAIRMAN APOSTOLAKIS: At this point nobody knows what the right way is. I'd rather review NUREGs. After you guys start putting together regulatory positions, it's late. I don't know. I mean, 400 pages but how many tapes are usual to retape.

MR. WATERMAN: It's about a long -- how many what?

CHAIRMAN APOSTOLAKIS: No. I mean if this upcoming meeting is to be on research, independently aware that it's done by the Office of Research or whatever, should it be presented as well?

MR. ARNDT: I think the --

CHAIRMAN APOSTOLAKIS: Or is too early?

MR. ARNDT: I think the Research Office needs to decide that and provide you a recommendation.

CHAIRMAN APOSTOLAKIS: Are you the Research Office?

MS. UHLE: I'm the Research Office. Sorry. Well, I'm a representative for the Research. So maybe what we can do is just take away and I can interact Christina and we can figure out the best way to go forward.

CHAIRMAN APOSTOLAKIS: Okay.

MR. SHUKLA: So I guess we need two white papers, one from NEI, one from the staff?

MR. ARNDT: Let me look at my list of to dos. I have to provide to you the NEI white paper on operational experience. I'm trying to find the --

MR. SHUKLA: And there is one that Mike was talking about.

MR. WATERMAN: The operating experience--

MR. ARNDT: Oh, operating experience draft NUREG.

MR. WATERMAN: Yes.

CHAIRMAN APOSTOLAKIS: So what have we agreed here or tentatively agreed?

MR. ARNDT: We've tentatively agreed that the --

CHAIRMAN APOSTOLAKIS: Brookhaven, OSU?

MR. ARNDT: Yes.

MEMBER BLEY: Virginia keeps getting mentioned.

CHAIRMAN APOSTOLAKIS: Yes. I mean the fault injection thing.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Yes? And how about this integration? You want to have a preliminary thing over integration for failure modes only?

MR. ARNDT: I don't know --

CHAIRMAN APOSTOLAKIS: Or plants? Maybe plants.

MS. UHLE: Well all these works are in various stages of completeness. And so they're all at this point in time, you know, a work in progress. And what I was proposing is if we could delay things a little bit so that we have more of the work done, and then also a bit of an integration to talk about how it would be used. And that's what I was proposing. I may not have said that very clearly.

CHAIRMAN APOSTOLAKIS: Well, let's look at the integration. Okay. That's enough.

And ask, I think it's always you ask isn't it, the report is joint?

MR. ARNDT: Yes, it's a joint effort.

For the 11th we're going to talk about a short review of the --

CHAIRMAN APOSTOLAKIS: The 11th of what? Oh, of April.

MR. ARNDT: Of April.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: The short review of the three ISGs, short review of how we're planning on dealing with the Subcommittee comments on the risk ISG, a short review of how we're planning on using the OE and a presentation from industry.

CHAIRMAN APOSTOLAKIS: The latter being just information?

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: Okay.

MR. SHUKLA: So you could draft an agenda for the full Committee meeting and send to us?

MR. ARNDT: Some member of the staff will do that.

CHAIRMAN APOSTOLAKIS: Thank you, gentlemen. Thank you very much.

Now the last thing we need to do, there's one last thing. We usually go around the table and the Members say some conclusions or whatever, comments. So, John, you want to start because Myron is new to this business?

MEMBER STETKAR: Okay.

CHAIRMAN APOSTOLAKIS: Okay.

MEMBER STETKAR: I think in summary, I don't have too much more to say.

I'm encouraged by a lot of the things that I see. The staff, the industry I think you're doing an awful lot of work on a really, really difficult topic.

I'm yet a little bit cautious because I'm not quite sure how I see things coming together from a practitioner's point of view in a way that will help me to evaluate the contribution from digital I&C, whatever that is, to risk. Things that we were talking about before; the importance of defining the failure modes, defining the scope and the interfaces, defining component boundaries.  And I shouldn't use the word "component. But defining boundaries of the piece parts that we're analyzing.  Both piece parts in the way of hardware, piece parts in the way of software and things like that.

So I'm still a little bit -- I'd like to see a little bit more in that area in terms of the vision forward, in terms of how all of this information will be combined in a way that we see in terms of practitioner's view of the applications.

And that's it.

CHAIRMAN APOSTOLAKIS:  Dennis?

MEMBER BLEY:  Yes. I guess first I'd like to thank everyone from the staff and industry who made presentations today.  And the quality of those presentations and the depth of the answers are really appreciated. Sometimes people can't dig as deeply into issues as we did.

I'm, in some ways, rather encouraged. And this work on failure modes, I guess I would reiterate to me is really crucial to getting a handle on what to do.  The link to the PRA begins there and when that's really well understood, I'm a little more optimistic than some others.

I think once we know how to categorize

these failure modes and come up with categories of their effects, it might be possible to move to quantification with higher hope.

The efforts to get into other data from other industries on similar processors and pull the similar parts together and get data I think is a really -- well, is the one way we'll be able to move ahead if we ever can with quantification.

CHAIRMAN APOSTOLAKIS: Jack?

MEMBER SIEBER: Well, I think like my colleagues, I'm encouraged by what I heard today. And I think that we're moving out of the theoretical speculations down to practical matters where we're going to ultimate reach a conclusion.

My impression of event analysis, even though I think it's been parsed a lot of different ways, to my recollection there's only about somewhere between 33 and 38 systems, subsystems that have been approved by NRR for application in power plants. And they are all little pieces of things like proposition indicating systems, three element feed water control; that kind of stuff. And I don't see how on these little systems and so few of them you're going to get operating experiences reason to help you. You've got to spread out into other industries.

And obviously my experience that goes back longer than I'd wish, the driver in the I&C business was always chemical industry, chemical and petroleum. You know, if it were just a power plant, they'd all be out of business.s And so I think that's the place to -- that's one place to get event data. And I encourage looking further at databases outside the nuclear industry in the United States. Perhaps you can overseas, because I know there's more activity there than here.

And so if I come out of all of this, I think you've done a good job but there isn't -- there just isn't enough data for me to draw any conclusions.

And I did figure out on the FAA event reports why there is so many more events that say that the airplane climbs suddenly, the pilot leveled out as opposed to ones that said the airplane dove.

MEMBER BLEY:  Good reasoning.

MEMBER SIEBER:  In any event, in summary I think everybody has done a good job, they're on the right track. And I think we have to expand our horizons.

And I guess the other thing is that there is so manu possibilities for system architecture that effects the 3D process immensely that you have to give a lot of thought to whether it's advisable to run a pipeline on one CPU. I've never had a computer last more than five or six years. And so I would think about architectural concepts like that as to how it fits into diversity and defense-in-depth.

So I guess that's my comment.

CHAIRMAN APOSTOLAKIS: Myron.

MR. HECHT: Okay. Well, I guess first of all I should clarify for the record that I am a consult, and therefore --

CHAIRMAN APOSTOLAKIS: Everyone knows that.

MR. HECHT: Okay. And I have a paper one rather than a plastic one.

I guess if there's anything that I would want to, I guess, make an overarching comment about it's that the conceptual framework for gathering the data is the key issue. And if the conceptual framework is proper, then we can incorporate data from multiple disciplines. We have to distinguish between events. I mean, not the reports, but the incidents, actual incidents and we have to distinguish between those and the causes. Within the causes we have to distinguish between process causes and other types of causes.

And we have to be able to isolate what's common from other systems to the nuclear world so that we can actually incorporate that experience. And once again, that relates to that digital system boundary, not necessarily the sensors and actuators, but whatever it is that lives between there and the actual CPU that is relevant.

And the other thing that I think it's important is that as we look at operating experience, we also have to look at successes, not failures. There's no hypothesis here that's unstated, I think, which is that digital systems have common cause failures which will surely eventually cause something terrible to happen.

And I think it's incumbent on the people gathering the data to either approve or disprove that hypothesis to whatever level of confidence we can, which I guess we don't have an alpha here. I guess we have a thing called engineering judgment. But that should be the purpose of it all.

And in the process of looking at that, trying to get specific lessons learned so that we can speak about what the D3 guidelines are.

CHAIRMAN APOSTOLAKIS: Thank you.

I agree with the comments of my colleagues. The most important thing in my mind that came out of today's meeting is this idea of having someone pull together all these efforts on failure mode identification and try to come up with a comprehensive approach, maybe supported by computerized guides that the staff can use to identify failure modes. Because I think the state-of-the-art right now can support something like this. IT will evolve over the years, but it can support it. And it was not a subject of today's meeting, but I'm really, really pessimistic about any probabilities, meaning probabilities coming out anytime soon. I speak as an individual, of course. But the failure mode work that is being done in various research efforts of the agency I believe are very good and very useful.

So with that, unless somebody has a comment. Staff? No. Public? Sure.

MR. BOWERS: Wes Bowers from Exelon.

One observation I had overall, especially that came out of the morning session where I think Paul Loeser said something about the effect of in a regulatory process reviewing the Oconee was kind of a trial and error process. So that's a challenge, I think. Challenge to the industry, challenge to the staff and a challenge to the Committee to make sure that as we go through all of these reviews and get probability numbers, get failure data that it gets translated into, I'll call it an actionable criteria that's very, very clear so that the industry knows what the criteria is and how to satisfy that criteria. So the staff knows very, very specifically what the criteria is, how they're going to satisfy it, what they're going to look at in the amount of documents, what they're going to do in the review.

We have to drive, all of us together drive towards having an actionable criteria that we can provide closure in the licensing process. It's a challenge for us all.

CHAIRMAN APOSTOLAKIS: Very good. Thank you.

Any other comments?

Okay. Thank you very much, gentlemen. It has been very informative, as usual. And we'll see you in two weeks or so.

The meeting is adjourned.

(Whereupon, at 4:29 p.m. the meeting was adjourned._