Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, February 5, 2009

Work Order No.: NRC-2649 Pages 1-226

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

+ + + + +

559th MEETING

+ + + + +

THURSDAY

FEBRUARY 5, 2009

+ + + + +

ROCKVILLE, MD

+ + + + +

The Advisory Committee convened in Room T2B3 in the Headquarters of the Nuclear Regulatory Commission, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Mario Bonaca, Chair, presiding.

ADVISORY COMMITTEE MEMBERS PRESENT:

MARIO BONACA, Chair

SAID ABDEL-KHALIK, Vice Chair

J. SAM ARMIJO, Member-at-Large

JOHN D. SIEBER

SANJOY BANERJEE

DENNIS C. BLEY

JOHN W. STETKAR

ADVISORY COMMITTEE MEMBERS PRESENT: (cont.)

DANA A. POWERS

WILLIAM J. SHACK

MICHAEL T. RYAN

OTTO L. MAYNARD

CHARLES H. BROWN, JR.

HAROLD B. RAY

MICHAEL CORRADINI

GEORGE E. APOSTOLAKIS

NRC STAFF PRESENT:

MARY DROUIN

GARETH PARRY

JOHN MONNINGER

MAITRI BANERJEE

DOUG HUYCK

BONNIE SCHNETZLER

TIMOTHY REED

PAT HILAND

BILL KEMPER

RICH STATTEL

PAUL LOESER

ALSO PRESENT:

KEN CANAVAN

DON VANOVER

CHRIS EARLS

RICH FREUDENBERGER

MIKE BAILEY

SEAN KELLY

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

P R O C E E D I N G S

(8:29 a.m.)

OPENING REMARKS BY ACRS CHAIRMAN

CHAIR BONACA: The meeting will now come to order. This is the first of the 59th meeting of the Advisory Committee on Reactor Safeguards.

During today's meeting the committee will consider the following: draft final NUREG-1855, Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking; two, draft final Regulatory Guide DG-5021, Safety/Security Interface; three, digital upgrade of the Oconee Reactor Protection System and engineered safety features; and fourth, preparation of the ACRS reports.

The portion of the session dealing with the digital upgrade or the Oconee Reactor Protection System and the engineered safety features may be closed to protect proprietary information to Duke Energy and its contractors, pursuant to 5 USC 552(b)©)4.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Sam Duraiswamy is the designated federal official for the initial portion of the meeting.

We have received notice of comments of requests for time to make oral statements from members of the public regarding today's sessions. We will have representatives of Duke Energy and Mr. Norbert Carte on the phone bridgeline to listen to the discussion on the digital upgrade on the Oconee RPS and the ESP.

To preclude interruption of the meeting the phone line will be placed on listen in mode.

A transcript of a portion of the meeting is being kept, and it is requested that speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume so that they can be readily heard.

I will begin with some items of current interest. First of all a happy event, Bill Shack has been appointed to the ACRS for a fifth term.

(Applause.)

We want to congratulate him, and I will like also to thank Ed Hackett for making it happen.

We have two new staff members. First of all Brandi Hamilton joined the ACRS staff as a management analyst in December, 2008. She currently works with the ACRS office information technology team, and serves as the ADAMS records custodian, and

the Share Point project manager.

She also performs WebACTS maintenance.

Prior to joining the ACRS staff Brandi worked at NMSS for about four years. She graduated from the NRC nuclear safety professional development program in October of 2008.

Brandi possesses a master's certificate in government contracting from the George Washington University School of Business, and a level two contracting certification from the Federal Acquisition Institute. She also holds bachelor's degrees in biology from Bennett College, and is currently pursuing a master's degree in environmental management from the University of Maryland University College.

Welcome aboard.

(Applause.)

And the second person that came on board is Vanice Perin. She joined the ACRS staff recently for a three-month rotational assignment. Vanice holds bachelor's and master's degrees in nuclear physics. She joined NRC in 1997. Vanice has worked in MSS, RES, and NRR, performing various tasks including nuclear criticality reviews for the licensing and regulatory oversight of fuel enrichment, fuel fabrication and waste facilities; and evaluation of

validation data needed for fuel depletion and criticality codes.

For the past three years she has been a project manager at NRI, leading several licensing related activities, including the boiling water reactor vessel and internals project.

Vanice also worked for the Los Alamos and Idaho National Laboratories. As a senior scientist at INL she worked on fuel and target development for the modular high temperature gas-cooled nuclear production reactor. For that work she performed Monte Carlo neutronics and transmutation ORIGEN-type analysis of heat generation in tritium production in the Loose Particle Irradiation Test at the Advanced Test Reactor.

Vanice, welcome aboard.

(Applause.)

With that, I think we are over with the introductions, and we are moving on to the first item on the agenda, and Professor Apostolakis will take us through that presentation.

DRAFT FINAL NUREG-1855, GUIDANCE ON THE TREATMENT OF UNCERTAINTIES ASSOCIATED WITH PRAs IN RISK-INFORMED DECISIONMAKING

MEMBER APOSTOLAKIS: Thank you, Mr.

Chairman.

The subject this morning is report NUREG-1855, guidance on the treatment of uncertainties associated with PRAs and risk-informed decision making.

As several of you recall this committee has been asking the staff to produce a document like this for some time now. I believe we started back in - we wrote a letter actually, we started before that, we wrote a letter in 2003 urging the staff to look into the issues of uncertainties, and especially model uncertainty.

We had two subcommittee meetings on the matter in December of 2007, and September of 2008. This is a draft final report, and we are expected to write a letter at this meeting on the report whether it should be published or not.

There are also at least two or maybe more EPRI documents that deal with the same subject. They have been published over the last few years. One thing that we saw for the first time this time around was the appendix that the staff is proposing to add to the report, and this appendix borrows heavily from an EPRI document, the approach that they describe there, how to identify important model uncertainties and so

some sensitivity analysis.

So we are ready to hear from the staff. And who is first, Mary or John?

MS. DROUIN: Good morning. We are delighted to be here. It's been a long way to get to this document, a lot of work.

I want to introduce the entire team, because it has been a lot of work by a lot of people. So at the table with me to my left is Ken Canavan - I don't know, you introduce your people, I think that is better.

MR. CANAVAN: Okay. Ken Canavan, I'm the project program manager for the risk and safety program at EPRI. We have been before you a couple of times on previous revisions to this document, and very happy to be here today.

With us today also is Don Vanover of Erin Engineering, a contractor to EPRI on this task; as well as in the audience is Doug True, also with Erin Engineering, and both key contributors to the development of this report.

MS. DROUIN: And we are both at the table because it is an effort that we have collaborated under our MOU with EPRI, and these two documents work together hand in hand.

We gave an integrated presentation last time, and it seemed to go a lot better than giving separate presentations.

From the NRC side Gareth Parry and then our contractors that have helped us are John Lehner from Brookhaven, Jeffrey LaChance from Sandia, and Timothy Wheeler from Sandia.

Now before we get started, John, do you want to make some remarks?

MR. MONNINGER: Maybe if I could, first, I'm general manager, I'm the deputy director for the division of risk analysis in NRC's Office of Nuclear Regulatory Research. I wanted to thank the ACRS very much for this opportunity for the staff to allow the staff and EPRI to present you with the status of where we are, and hopefully receive a letter from the ACRS endorsing the issuance of this report.

As Professor Apostolakis mentioned, it's been a project underway for about four or five years now, and it's a very important project to us. It is referenced within the Commission's phased approach to PRA quality. What I mean there, in addition to the PRA standards that are under development by the staff and that will be referenced within Reg Guide 1.200. Other supporting approaches and methodologies are

within that plan, including this, and including work that the staff has ongoing in the HRA field.

So with that in mind I just wanted to thank you very much for this opportunity. If I could just maybe throw in 30 seconds more, yesterday the industry and the staff briefed the Commission on the progress or the status of risk-informed performance space regulation within the NRC and the nuclear industry, and the consideration and treatment of uncertainty came up during the Commission meeting as being a very important topic, and we believe that the issuance and use of this document will contribute to resolution of some of those outstanding issues.

Also wanted to mention that several things that were discussed or emphasized by the Commission, that the staff has also been working with the ACRS on in the pure air include digital I&C, fire PRA, HRA and the various PRA standards.

So we very much do appreciate the opportunity to interact with you in the past on these topics and look forward to it in the future.

So with that I'll turn it back over to Mary.

MS. DROUIN: Thank you.

The objective from our perspective of

today's meeting is to discuss the work that NRC and EPRI have done, and the documents. Theirs have been published. We are getting ready to send ours to publications.

We also want to talk about the future work, where we are going from here. At the last meeting with the subcommittee, a lot of issues were raised, and we acknowledged those issues. They were important issues, but they were for a future revision. Because we felt that it was important that we get something out on the street right now for both NRC and industry to start using.

In fact we've already started looking into putting into place what is it we want to do next year and the year after. There may be two revisions or three revisions to this document. But we have already started identifying things that we want to start doing in `09 for revision hopefully in `10.

MEMBER APOSTOLAKIS: So you are talking about revisions rather than additional documents?

MS. DROUIN: To be decided. If it makes more sense to have additional documents, if it makes more sense to revise the document, that is a decision to be made.

MEMBER APOSTOLAKIS: Okay.

MS. DROUIN: And to request a letter, unless it's a bad letter.

(Laughter.)

MEMBER APOSTOLAKIS: Speaking of the document, there is no opportunity now to revise this document. This document, is it a go or not go?

MS. DROUIN: That is correct. We've got the final - I mean after this meeting our intent is to start the publication process.

MEMBER APOSTOLAKIS: Okay.

MS. DROUIN: But I don't want to jump ahead. But as I've said we've already intended to revise this document. And I'll talk about it more when we get to the end of the presentation.

We have a major workshop that we have already planned, a two-day workshop in May on this document. And so I anticipate we will have a lot of lessons learned coming out of that workshop. So not just to revise and perhaps additional clarification, but as we go through and look at the scope of limitations to expand on that in a future revision, not just from lessons learned, which brings me to my next point.

We do want to spend the bulk of the presentation going through the example. We are going

to quickly reiterate what the purpose was, and how NRC and EPRI, how we have collaborated, and what is the scope and actual limitations. That seemed to be an issue at the last meeting, and we didn't spend a lot of time on it. So we wanted to spend a little bit of time talking about the scope and limitations, because again that is going to dictate some of the things we are looking for to do in the future with this document.

We also wanted to go through what are the explicit changes that we have made to this document since we had the subcommittee. We did go through and identify what we thought were some of the issues that were raised by the subcommittee last time, and we tried to systematically address all of those. And I know, George, we got some feedback from you on that point. So we are going to try and walk through and show you where we have made changes.

But then again, we want to really spend some time walking through the example. We put a lot of effort into that. EPRI has been invaluable in helping us in that endeavor.

And then last, talk about the future work and what we do plan to do.

So when we look at this effort, a primary

purpose of it is to give support to the standard. When you look at the ASME/ANS standard, all the requirements in there just tell you to identify your sources of uncertainty. And to characterize them. And that is all the standard requires you to do. And it doesn't provide requirements, when it tells you to characterize it, what do you mean by that? Because again the standard is written from a "what" perspective, what do you need do in your PRA, and it doesn't provide you guidance with how you go about doing it.

So one major purpose of both of our documents was to provide that guidance. How do you go about characterizing and identifying those uncertainties?

Then the next part of our document -

MEMBER BLEY: Can I ask you a question about that?

MS. DROUIN: Sure.

MEMBER BLEY: Some years ago I know there was a strong feeling that there ought to be a lot of that kind of guidance for various parts of the standard. This is one. Are there others underway, and is NRC participating if there are?

MR. CANAVAN: Yes, there are several

areas that are under development in the area of PRA scope and quality that essentially serve as guidance for the standard or elements of the standard, supporting elements of the standard, supporting requirements or elements. And they span the range of activities. And we are working with NRC research on them through Pete Appignani's group. We have a memorandum of understanding and work pretty closely on many of those activities.

MEMBER BLEY: Okay, thanks.

MS. DROUIN: You know, there are the HRA good practices. And we have identified, whether or not it gets approved, but we have identified for some future work some supporting guidance documents still to be developed, particularly in the area of success criteria.

And also we have a cooperative agreement with ASME, which also has a cooperative agreement with the PWR Owners Group to develop training on the standard. And that's going through -- it's not doing the how-to, but it's going through each requirement that is in the standard and explaining what was the intent of that requirement. And that is the training material that is being developed, but then they are ultimately going to put on some training courses on

the standard, which should help in that arena.

MEMBER BLEY: That's great. I hadn't understood where that was headed. Thanks.

MS. DROUIN: Yes. And in fact they are already looking into expanding the training to start taking on the internal fire product.

So in terms of -- it's supporting the standard, but then once you know what these sources of uncertainty are, what do you do with this information? So the guidance document is addressing that part of the issue.

MEMBER APOSTOLAKIS: But it's a central part.

MS. DROUIN: Oh, it's a very essential part. I'm not trying to dismiss it, because probably three-fourths of the document is --

MEMBER APOSTOLAKIS: As it should be.

MS. DROUIN: Yes, absolutely, of our documents. I got to keep remember saying documents, documents, because it's both NRC and EPRI.

MEMBER CORRADINI: Can I ask a question about that, since you have emphasized the interplay. So for accessibility purposes, neither one stands alone? That is if I went to the NRC document I would have to eventually get the EPRI document?

MS. DROUIN: Basically yes.

MEMBER APOSTOLAKIS: Which from an accessibility standpoint is that obviously easy? I guess I want to understand that.

MR. CANAVAN: The EPRI document is publicly available at epri.com. All you do is type in the --

MEMBER CORRADINI: Oh, it is? Okay, I was under the impression it required some sort of payment and an agreement. That is incorrect?

MS. DROUIN: No, we would not have been able to collaborate if the EPRI work was not publicly available.

MEMBER CORRADINI: I didn't understand that. There were some comments before in the last subcommittee, I didn't understand.

MR. CANAVAN: Yes, we had a little bit of -- we publish -- it's a two step process, so it comes out published. And if you look when it first gets published, before we get the publicly -- the public designator on it, it will come back and say, yes, for $10,000 we will sell you this report.

MEMBER CORRADINI: That was what I guess I was getting to.

MR. CANAVAN: It took us about three days

to fix that, so if you hit in those three days you got that notice. Right after that it's just a download.

MEMBER APOSTOLAKIS: You should collaborate more frequently.

(Laughter.)

MS. DROUIN: And I think that one of the changes that we tried to do to both our documents was to show clearer how the two documents work together.

Anyway, when we first started this program we did sit down with EPRI, and we kind of scoped out what we wanted to do, and what we were going to do in our document and what EPRI was going to do in their document. So that collaboration started from the very beginning of the program.

And the big thing is of course our focus was going to be from a regulatory perspective, and the EPRI from an industry perspective. And we felt it was important that both those perspectives come out with these documents.

Both of our documents --

MEMBER POWERS: Mary, I am struggling a little bit to understand this collaboration that you've hit upon here. You felt it was important to have the industry perspective. Felt it was important to have the regulatory perspective. There seems to be

a part missing here. Why wasn't a second collaboration set up with a party that would represent say the academic perspective?

MS. DROUIN: I am not really sure how to answer that, because I guess I don't appreciate -- I probably will upset you with this answer -- but I don't appreciate why an academic perspective, what you mean by that?

MEMBER APOSTOLAKIS: Be careful, Mary, be careful.

(Laughter.)

MR. MONNINGER: This is John Monninger, from the staff and research. We do have some grants and cooperative research programs with several schools out there. Some of them are in the I guess this is more of an approach to the treatment of uncertainty, but we have one project ongoing with the university in terms of the quantification or some advanced approaches too.

We have some other work ongoing -

MEMBER POWERS: Maybe you're just misinterpreting what I was using in academic for legitimate reasons. I mean you are looking at the academic area as more advanced thinking in this thing, and that is a perspective that is probably useful.

But I don't know - I mean that may be more for the future to document. I was really looking at - I was following the esteemed Dr. Wallis' view that the academic represented the public interest.

Suppose I was more explicit and asked, why didn't you set up a collaboration with the Union of Concerned Scientists? Would they not have a different view on treatment of uncertainty that would be of some value here?

MS. DROUIN: I'm sure they would.

MEMBER POWERS: And so why not set up a collaboration with them?

MS. DROUIN: The only way I guess I know how to answer it is that - to come back with, why don't I set up a collaboration with a lot of people.

MEMBER POWERS: Okay, fair enough; that is a good question.

MS. DROUIN: Where do you draw the line on that collaboration?

MEMBER POWERS: You're the one that is drawing the line. You are the one that is going to have to answer where the line is drawn.

MR. CANAVAN: If I might?

MEMBER POWERS: Sure.

MR. CANAVAN: I think one of the reasons why this effort is a collaboration is because when it began EPRI and NRC had separate products under development. So we had research ongoing in the pipe with significant resources committed from the technical communities of both the regulator and the industry. So it made sense to collaborate in some form because the documents had slightly different perspectives in them, and to make sure that those perspectives didn't result in the inability for us at the end to incorporate these into the PRAs and make useful products.

MEMBER POWERS: I think I understand exactly why you would do this. What I'm asking the regulator here, and I appreciate your - is that you have the same problem that you were trying to avoid here. When you come to interventions, where there is the two perspectives on the treatment of uncertainty that perhaps there is a failure to communicate - the communication goes on this way. And so I get these documents from the Union of Concerned Scientists that look upon uncertainties in one way, and others from the staff looking at the other way, that maybe that with a collaboration these people could be brought into enough of an alignment that we can resolve

things.

Exactly the same problem that you are trying to avoid between the industry and the regulator, it seems to me we have the same problem in the intervention and the regulator. And so I'm just asking, why not asked - invite them to the table for their perspective?

MS. DROUIN: Well, they are invited to the table when we go out for public review and comment.

MEMBER POWERS: That is a little different.

MS. DROUIN: Well, I understand that.

MEMBER POWERS: You're presenting, here is a fait accompli, and I know exactly how these things go. Somebody offers an orthogonal view, and you will throw up 6,000 reasons why that should not have been taken into account. This is quite different than in the preparation of the document.

MS. DROUIN: I'd like to differ, and all I can offer is my personal perspective and personally how I have always worked. And I have never summarily dismissed any public comments. Now that is not to say that I have always agreed with them, but I haven't come in with ideas that the public, whether it's the

Union of Concerned Scientists, are not going to offer something that is not worth listening, or that they don't have a good idea.

We did make some major changes to this document, because we went through two public review and comment periods, and we made some major changes, because we got some very shrewd thoughts from the public. And that's one of the reasons why this document that we started in 2003, and here we are 2009, because we rescoped a lot of work based on comments we received.

Now I do know that the Union of Concerned Scientists are aware of this document. They brought it up several times in the meeting yesterday.

Yes, whether or not we should do a collaboration -

MEMBER POWERS: What did they say yesterday?

MS. DROUIN: They just said how important it was, and it needed to get out, is my recollection. John, you might -

MR. MONNINGER: This is John Monninger for the staff. They actually - I don't want to put words in their mouth, but from their slides and my recollection they fully supported the issuance of this

document. As a matter of fact, they don't believe - I don't want to put words in their mouth - I interpreted them to believe we should not be using PRA and risk-informed decision making until all these standards are done, until the uncertainty documents are out there, et cetera.

So they have reservations with the staff using and industry using the current PRA methods and practices without fully endorsed Level 3 standards, without the document - without guidance out there for uncertainty, et cetera.

One thing I will affirm, the staff has in the past for certain efforts or projects, included parties other than the staff, and potentially industry. If you recall from the original development of the reactor oversight process, the staff established a FACA panel, similar to the ACRS, and on that FACA panel there were representatives of state governments. They had a representative of the Union of Concerned Scientists. There was a representative from the New England Coalition of Nuclear Pollution, et cetera.

So there are areas and times when the staff does use I guess maybe it's academia on certain projects. I think a question, a fair question, would

be, what are the skills and abilities, or what technically is being brought to this project? I think the people we involved on the project, I think we do believe that they bring a solid level of technical skills. And if there are other areas, I think we would potentially be receptive to that.

MEMBER POWERS: So your view, then, is that there were no technical skills on the part of the intervenors that could be applicable?

MR. MONNINGER: I guess my thought would be is, I'm not aware of a lot of work that they are doing in this area. I know EPRI is doing a lot of work. There are universities that are doing a lot of work in there. We are also working with international parties. We are working with NASA, who does a lot of work in this area.

So they are the parties that we are aware of that are -

MEMBER APOSTOLAKIS: I think we need to move on on this.

MEMBER POWERS: They have answered my question.

MEMBER APOSTOLAKIS: You have by the end of the day copies of the slides that were presented yesterday to the Commission. Maitri, are you the one

to do that?

MS. BANERJEE: This is Matri Banerjee. I attended presentations, the briefing yesterday. I will provide copies for you all.

MEMBER APOSTOLAKIS: I'm sure everybody around the table will appreciate that. We'd like to see them.

Okay, let's move on.

MS. DROUIN: Okay, both of our documents address the parameter and model uncertainties. It's what we do in those different areas where the key differences in the reports.

Regarding the parameters' uncertainties, our document is providing guidance on the characterizations and propagation. The EPRI report -

MEMBER APOSTOLAKIS: Could you explain to me what the word, characterization, means?

MS. DROUIN: When we talk about characterization, we talk about what could be the impact, not how much the impact is. What it would - what it could impact. Could it change an initiating event? Could it change what one of your contributors are? Could it change what one of your accident sequences?

MEMBER APOSTOLAKIS: Does it include the

sources of these uncertainties?

MS. DROUIN: Yes.

MEMBER APOSTOLAKIS: Because characterization is the whole pattern?

MS. DROUIN: Yes.

MEMBER APOSTOLAKIS: Okay, thank you.

MS. DROUIN: Okay. Regarding the model uncertainties, the EPRI report is providing guidance on the identification and characterization of the source. If you remember the EPRI document has that detailed table that goes through and gives this wonderful generic list of what potential sources of model uncertainty are, and characterizes them as I just explained.

Our document is providing guidance on how you go from that, and identify which are your key ones, for your decision making. Because not every source of uncertainty needs to be evaluated when you come to a particular decision. So our document is going through and providing the guidelines and the criteria to use to determine which of those are the key to your decision making.

Our document in terms of the uncertainties, ours also looks at what we usually refer to as completeness uncertainty. How do you deal

with the things you didn't think about? You still need to take that into account in your decision making.

So when you look at the risk and the insights that are coming out of the report, what we are trying to do is also give guidance into how do you integrate all of it into your decision making.

MEMBER APOSTOLAKIS: So let me ask a question here. I remember reading that in the document. I was wondering is there any reason to go back and revise Regulatory Guide 1.174, based on what you guys learned here?

MS. DROUIN: We are in the midst of updating Reg Guide 1.174, and NUREG-1855. How that should be factored into it is being considered.

Okay, scope and limitations. When you talk about uncertainties, there are uncertainties all over the place. But this document right now is limited to just those uncertainties associated with the PRA.

So other types of uncertainties at this point in time, whether or not it will ever be changed for that, those are the things we are going to have to be thinking about. But right now the scope and limitation of this document is just associated with

the uncertainties from your PRA.

MEMBER APOSTOLAKIS: Would it be more accurate to say PRA Level 1?

MS. DROUIN: At this point in time it's Level 1.

MEMBER APOSTOLAKIS: It's really focused on that.

MR. PARRY: And LERF.

MEMBER APOSTOLAKIS: Sorry?

MR. PARRY: And LERF.

MEMBER APOSTOLAKIS: Yes. But it's really focused on the Boolean type kind of events.

MS. DROUIN: Yes.

MEMBER APOSTOLAKIS: Although in passing you mention other things. But I think some other document in the future should address uncertainties say in Level 2 severe accident kind of analysis, thermohydraulic analysis. So that was not made very clear in the report.

It's a minor point, but it really is focusing on Level 1, on one blast, let's say, one blast.

MS. DROUIN: Yes, and that's why I'm going through the scope of limitations, but we tried to make this clear in the document. And every single

one of these bullets are discussed in the report matter.

So right now as you just said it's just Level 1, internal events, LERF, at power. So we are not providing right now looking at the sources of internal fire, your external hazards, and low power shutdown.

Now it is our plan to expand this to cover the whole PRA. But we feel like this should be done in synch with the standards, so the standard is just now out that covers a general fire, and hazard, so now we can start looking at that. When the standard comes out for low power shutdown, we will do that.

There are standards underway for Level 2 and Level 3, but you know again, whether all of this is going to be in a single document, or whether it makes sense to have multiple volumes, you know, those are all decisions. But it is our intent to cover the uncertainties associated with the entire PRA.

Guidance is provided on the process for identification and characterization and how to factor the results into the decision making. It's independent right now of the source of uncertainty. And what I mean by that is when you look at the process that we have laid out in that document, it

doesn't matter if you just want to take the process and apply it whether or not you are dealing with say a full Level 2 or internal fire, the process is still applicable.

What it doesn't have is what are the sources of uncertainty associated with these other parts of your PRA.

MEMBER APOSTOLAKIS: Let me ask a question or comment on something more specific here.

When you said, guidance is provided on how to factor results into the decision making process, I think that what you - what essentially the document does with EPRI documents, is that it gives you ways of identifying what could be important from other uncertainties in the decision.

Now that is not the same as saying that it gives you guidance how to - let's say something is important. It passes the screening process, and it's important. I'm not sure the document tells you how to handle that. In other words it doesn't go the extra step of quantifying this uncertainty or doing something to see what it's impact is on the decision.

If it is screened out, fine. But if it passes the screening process and it's important, I think you stop short there, and maybe that is

something you ought to consider in the future work.

You know I don't expect this document to solve everybody's problem. But I think it's important to acknowledge that certain things are done and certain things are not done.

MS. DROUIN: Yes.

MEMBER APOSTOLAKIS: So if you look at the appendix, because that's where really you give an example of how these things apply, you have all these methods of saying, you know, now you do this - you don't necessarily have to agree with that but you do this to see whether it's important or not. Fine, there is a method to do that.

But after you decide it's important, there is silence.

MR. PARRY: We mentioned a little bit about the use of compensatory measures for example, or limiting the scope of applications. But in terms of saying that how do you deal with it by saying that you are 5 percent - the confidence level is 5 percent in this hypothesis, we don't go down that road.

MEMBER APOSTOLAKIS: That's true, and that is something that you may want to think about in the future. There is no way that all the problems can be solved in one document.

MS. DROUIN: I agree, and I think that's why this workshop is very important as we walk people through it, to find out where do we need to at least in the short term add more guidance to make the document useful - we think it's useful now, but to make it more useful.

MEMBER APOSTOLAKIS: Usefuler.

MS. DROUIN: Usefuler, and what do we need to be doing in the longer term, and then in the real long term.

MR. VANOVER: If I may, this is Don Vanover from Erin. I think when we get to the example of - in my mind the whole purpose of running through this process is to identify those important model uncertainties that could impact the decision, and then the key pieces, being able to identify them, and being able to consider if compensatory measures could be put in place, or what kind of actions could be put in place to offset the uncertainty associated with those model uncertainties.

So I think that - we didn't exactly say what comp measures may be acceptable. But the process that we try to define is what would identify those issues that need to be considered.

MEMBER APOSTOLAKIS: And you do that.

All I'm saying is that in the future it would be nice to go beyond that and expound on it. And another thing, for example, since you mentioned compensatory measures, I don't think that ultimately say five years from now we should have a report that says, you know, and you figure out the compensatory measures. It seems to me that if you propose a compensatory measure, you should go back and do some quantitative analysis to see if that measure in fact does what you want it to do. You don't just find it and say, aha. Because it may not. In other words there is a change now in the plant because you have decided to have an operator do this. You go back now and ask yourself, well, is he going to do it? That is the probability that you want, and how does that affect what I have calculated.

But I do repeat that this is something for the future. All I want to make sure right now is that you guys agree that there is a need to do something here.

MS. DROUIN: Oh, absolutely.

MR. VANOVER: Another point to follow up on that is, I think that is a good idea for those things that can be quantified, but not all comp measures that would be identified would be easily

quantified, and be able to show a reduction.

MEMBER APOSTOLAKIS: Yes, we're trying to speculate now how much good can be done. I don't want to get into that. All I am saying is, we want to have an agreement that somebody is going to look at that.

MR. VANOVER: We'll look at it.

MEMBER APOSTOLAKIS: Yes, and dismiss it if you can?

MR. VANOVER: We will follow it up.

MEMBER APOSTOLAKIS: Thank you very much.

MEMBER RAY: In addition to agreement among the experts, it seems to me like there needs to be a clear caution to the less expert audience who may become overly confident in something that all the experts understand there is more work to do. But the others out there who I'm acquainted with don't recognize those cautions if they are not explicit.

MS. DROUIN: Now we did - and we can add some - we did put a caution, it may be too vague for you, but we did try and put a caution in the foreword, to say that this document is anticipated to be revised, and it is a FAR, and just the fact that it's a FAR you can't write a whole lot there. But usually people do read a foreword and right up front we wanted to let people know, don't look at this as the end all.

MEMBER RAY: But there is a strong tendency to want to do that.

MEMBER APOSTOLAKIS: I think on this point, Ken told me before we started that EPRI is going to have some, was it process or activities, for executives? Maybe that is relevant.

MR. CANAVAN: I think it is in many respects. There is - at the Commission brief we presented doing some - a program just to begin our Socialization of Risk Technology, which is -

MEMBER APOSTOLAKIS: Your what?

MR. CANAVAN: WE call it Socialization of Risk Technology.

MEMBER APOSTOLAKIS: Did you get paid a lot of money to do that?

(Laughter.)

MR. CANAVAN: But the idea is to at least start getting people who make decisions familiar with the technology, and what we are trying to do, and what are the considerations that they should have in mind when they are doing - when they are applying this.

MEMBER RAY: And you don't want an over-reliance by the uninformed. We know of other experiences where that has led, catastrophe.

MS. DROUIN: And one of the other things

we are thinking about, I mean we are having this workshop, but the other thing that we are thinking about for the future is do we develop some kind of training that goes along with this document just as a - and if so, if we decide that is a good idea, and it's worth putting the resources into it, to me a major part of the training is, you know, what the document deals with.

George, I think for the sake of time, because I really don't -

MEMBER APOSTOLAKIS: You are so slow, Mary, I don't understand.

CHAIR BONACA: We need to move on.

MS. DROUIN: Because we really want to make sure we get to the example. I'm going to - and so we are going to jump right to 11 -

MEMBER APOSTOLAKIS: Slide 10.

MS. DROUIN: Oh, I was going to go all the way to 11.

MEMBER APOSTOLAKIS: Well, the first bullet of 10 caught my attention, maybe wrongly. Can you just tell us quickly what that means, slide 10? Can we make sure that we have 10 on the screen.

MS. DROUIN: Oh, sorry.

MEMBER APOSTOLAKIS: This is eight.

MS. DROUIN: When you look at a model uncertainty it is real important that you understand and separate it from what is an assumption or an approximation. And all we are trying to say here is that guidance, we don't have guidance for that in this document explicitly.

MEMBER APOSTOLAKIS: But isn't the model -

MS. DROUIN: So that is a limitation of this document.

MEMBER APOSTOLAKIS: Isn't the model a set of assumptions essentially? I mean these are different assumptions.

MR. PARRY: Yes, these are limiting assumptions in the sense of, am I going to - yes, scope and level of detail of the model, as opposed to an issue that we don't know how to model. Which is really all we're focusing on.

MR. CANAVAN: A true uncertainty versus a scope and level of detail choice.

MEMBER APOSTOLAKIS: So somebody dictates, in this case I am not going to do floods.

MR. PARRY: Or I am not going to put in failures of manual balance, for example.

MEMBER APOSTOLAKIS: Yes. But we do

agree that the model is based on -

MR. PARRY: Yes. Yes.

MEMBER APOSTOLAKIS: All right.

MR. PARRY: So these limitations would in fact have a - they bias the results. It's an uncertainty that could be reduced.

MEMBER APOSTOLAKIS: But this is part of the incompleteness?

MR. PARRY: I think it's more the level of detail.

MEMBER BLEY: It's an intentional bias.

MR. PARRY: It's an intentional bias.

MS. DROUIN: It's not an incompletion. When you think of completeness issues, are the things you don't know about. This is an incompleteness of the document, and that we haven't gone through and addressed that explicitly in our guidance.

MR. PARRY: I think Dennis is right in saying that its impact is really if it applies.

MR. CANAVAN: It's a simplification. I guess the reason for separating them is, if you have a - let us say you decided to do with this really coarse screening fronting analysis, but you get to an application and fronting analysis is required or impacted, it becomes a key assumption. Well, you

would naturally remove that simplification. It's not a - it's no longer something that we need an uncertainty. Because when we get to the application we will build that level of detail back in, and when we do that, we shouldn't be trying to do uncertainty or sensitivity cases, on things that were purposefully simplified in the analysis. We should only do it in those areas that are true uncertainties in different competing models and approaches.

MEMBER APOSTOLAKIS: Okay.

MS. DROUIN: Okay. Now we are going to - Gareth is going to walk you through the changes that we've made, and then Don is going to walk through the example.

MR. PARRY: What I am going to talk is mainly the changes that we made in response to the comments that we heard from the ACRS at the last subcommittee meeting.

So what we've done as to, we tried to clarify the scope and limitations regarding what this document addresses, because I think that was a concern that you had last time, which initiate events, and we discuss which operating states, which hazards for example.

MEMBER APOSTOLAKIS: This is really where

our earlier discussion is applicable. It's not emphasized enough that you are limiting yourselves to Level 1.

MR. PARRY: To Level 1.

MEMBER APOSTOLAKIS: To Level 1 class. I don't know if you still have time to add a few words there. I thought it was important to make sure that the reader - if you have a chance, do it please. What you said earlier, it's a power - although in passing you do mention. But it's essentially a power Level 1, or 1-plus. Is that standard now, terminology, 1-plus?

MR. PARRY: Level 1 plus limited Level 2, I think.

MEMBER APOSTOLAKIS: Well, that's one class.

MR. PARRY: But I think in a sense that that limitation really only applies to the sources of uncertainty, which applies more to the EPRI document, and to the appendices in the EPRI document, than it does to the process in our document. We try to make that different.

MS. DROUIN: George, we can add it.

MEMBER APOSTOLAKIS: What I'm saying is, several groups now are working on advanced reactors, so this document is supposed to apply to everything.

And there the uncertainties are not of a type where there is a Boolean event. I have this code. It was developed for light water. Now I'm using it for sodium. I have uncertainties. I don't know what the transfer provision is. This document doesn't help that guy. And you know why should it?

MR. PARRY: Not in detail.

MEMBER BLEY: Yes, I think what Gareth said, it's the process described which seems to me pretty complete. The examples and the language are what put the Level 1 cast on it.

MR. CANAVAN: And that was done actually on purpose.

MEMBER BLEY: I understand, and that's all George is saying.

MS. DROUIN: We can add that.

MR. PARRY: Okay, the second bullet on that page, I know Dr. Bonds had left but he thought that the guidance was - that the way we had written it was more an excuse for not doing something rather than what you needed to do. So we changed it.

MEMBER APOSTOLAKIS: Well, there was a strong message in earlier versions anyway.

MR. PARRY: And I think it was specifically aimed at the EPRI document, but I think

there was a little bit in ours too. So we - I think both documents will try to change that tone.

And yes, there was another concern - again, this is more a description of scope - we have made it clear that what we are talking about in this document is the guidance on how to deal with uncertainty in the context of a risk-informed decision rather than an absolute assessment of uncertainty on CDF and LERF.

So we are always - because really we feel that the importance of the uncertainty lies when you make the decisions. So that's what we were trying to do with that.

MEMBER APOSTOLAKIS: That's a very good approach.

MR. PARRY: The - we've also added a little bit of guidance on really it's how you present the results to a decision maker. So we have added some guidance on how you present an assessment of the credibility of the results from alternate assumptions, and how you represent that for a decision maker.

I think it was John Stetkar that pointed out there was a lot of useful information in Table A-4 which we really didn't make use of. So I think we have added the comments in both - that we actually

boiled down in the NUREG report to point out the Table A-4 is particularly important I think when you - it might be - if the types of applications where some of the common assumptions that we make like Atlas isn't important for example might not be true. And that table provides additional sources of uncertainty that you might want to refer to.

Another comment that we received was that, what do you do about a consensus model, or what do you do about a single model which is not necessarily a consensus, but it's the only model you've got? And what do you do about uncertainty in that regard?

And I think what we've done is pointed out that we don't necessarily say that there is no uncertainty; that the way you deal with that uncertainty typically is to somehow characterize your uncertainty on the output of that model, of that single model, whether it be a consensus model or just a - the only model in town. But you have to have some assessment of the uncertainty in the results of that model.

So we've added discussion on that.

There was a concern with the term, uncertainty intervals. And really it wasn't our term; it was the term that is in the ASME standard. So that

we have done is to provide our interpretation of what that really means in the context of this document. So we've clarified in a sense at least what we are interpreting as uncertainty intervals, which really means it's a characterization of the uncertainty and typically we are going to be using probability distributions as we do.

MEMBER APOSTOLAKIS: I noticed these uncertainty intervals. I mean, it's 2009, it's so hard, never die. It's amazing to me that we still talk about this, and you have a little table why one should use the benefits of Bayesian versus frequencies.

There is a single answer to that. How many PRAs are there around the world? How many have you done? In America we have 104 I suppose.

MR. CANAVAN: Sixty five dual-unit sites.

MEMBER APOSTOLAKIS: How many of those are based on frequency distributions?

(Simultaneous speakers.)

MR. PARRY: People use frequencies to test when they are doing simple tests to see whether -

MEMBER APOSTOLAKIS: That's not the PRA. That's not the PRA.

MR. PARRY: Well, but it can provide

input into the PRA.

MEMBER APOSTOLAKIS: Anyway. I thought all these people were dead or retired.

MS. DROUIN: Well, I was going to suggest that you send in an inquiry to ASME on that term.

MEMBER APOSTOLAKIS: You want me to retire?

MS. DROUIN: Okay.

MEMBER APOSTOLAKIS: Anyway, I was surprised to see, but anyway. At least it has some definitive statements.

Okay.

MR. PARRY: Okay. I think John again was worried about the - well, actually let me move to the second bullet.

We've changed to call it epistemic correlation, George, so you will be pleased to know, instead of state of knowledge correlation.

MEMBER APOSTOLAKIS: Yes, in most places.

MR. PARRY: In most places, yes. Obviously we still use state of knowledge -

(Simultaneous speakers.)

MEMBER APOSTOLAKIS: - should use both because there's a transition.

MR. PARRY: Right, exactly. So we have

added a warning about not taking into account the epistemic correlation on truncations.

The third bullet relates to I think the screening criteria, which probably is in Chapter 6, and it is more related to the way you do basic CDF levels reading low within some of the screening criteria that we use for operating reactors, for example, and that you find in the ASME standard, really don't make a lot of sense. So we have added that.

The last bullet refers to the fact that I think we were using the word, estimate, and primarily in the EPRI report.

MR. VANOVER: There was a specific paragraph in the EPRI report that was confusing without the addition of showing as an alternate in lieu of propagating, so we added that clarification.

MR. PARRY: Right.

We had some discussion on how you treat the human reliability analysis. Because it is an issue that you can't really expect somebody to go and do their human reliability analysis with a totally new method; that would be unreasonable.

So what we have added is a statement in there that really what we should be doing is that

based on the assumption that if you do the human reliability analysis correctly in terms of identifying the human failure events, and judging their relative difficulty if you like, then if you had the ranking right, you've gone a long way, and we proposed to treat the human reliability by doing sensitivity studies on the set of HEPs if you like.

We've also realized that the sensitivity studies ought to be broader than just taking the 95th percentile of that one method. It really ought to reflect the range of possible methods that you can glean from industry.

So that - we added that. And then -

MEMBER BLEY: Are you going to come back to this in examples?

MR. PARRY: Not particularly in the example, no. We did the sensitivity study, but not the -

MEMBER STETKAR: The sensitivity study in the example does exactly what you said you provided warnings not to do. It places the 95th percentile of uncertainty from a specific method. So if I'm a user of this document now, I have an NRC-approved methodology that says I can do that by example.

MR. PARRY: Well, I think that we have

put sort of a government health warning in the front of that example, though, to explain -

(Simultaneous speakers.)

MR. PARRY: But I think that is a good point, John. Maybe we can add a footnote into the example or do something else that would clarify or that would relate back to that example. It's a good point.

MR. PARRY: Let me talk about that when we get to the example.

MEMBER BLEY: I was just going to say, not only is it not reasonable to expect people to use a range of HRA models; I'm not sure what that does for you. There is no good evidence yet that these three models will give you the range of uncertainty in the performance characteristics.

But the same kind of ideas you talk about, the things to think about that could drive the answer, ought to apply here. Now you can't point to one thing that tells you exactly how to do that.

MR. PARRY: And the other thing, too, is I think that we point out, and it is pointed out in the example, that by understanding the results you can identify which specific HEPs are significant, and you can pinpoint to those as being areas where you might

want to bolster up your training or do prejob briefs or things like that to at least as a compensatory measure if you like on the failures.

I think - it's a tricky area, but I think what we have - I think we can add a couple of things in the examples maybe.

MEMBER APOSTOLAKIS: Can the NUREG stand alone without the appendix?

MS. DROUIN: It could.

MEMBER APOSTOLAKIS: For a short time?

MS. DROUIN: I think it devalues the document.

MEMBER APOSTOLAKIS: But it avoids problems like the ones we just discussed.

MS. DROUIN: I think it's easier to add the cautionary notes which would not take a lot of time to do than to not have the example.

MEMBER APOSTOLAKIS: I think putting together the cautionary notes would take a long time.

MEMBER BLEY: To get them to the point. I guess one of the things that bothered me with the examples is rather than thinking about all the good things that are in the document, about how to think about uncertainty and what drives it, they tweak the numbers. They pick the 95th on their distribution that

they might not have any real basis for, they double something without telling you about doubling, is an especially useful thing except it was judged. So they don't seem to get at the heart of what the document is trying to tell you to do when you do this uncertainty analysis. That's why I'm not comfortable with it as it is. I don't think it's showing you how to do what the document tells you you ought to do.

MR. PARRY: Well, let me - we will get into that more when we talk about the example, but I think the example does more than do - you are really focusing on the sensitivity studies at the end. I think looking at the example as a whole in terms of how you analyze the results to identify the sources of uncertainty, and how you are using the techniques to come up with the key sources, is illustrating what's in the document.

MEMBER BLEY: You are probably right. The sensitivity studies -

CHAIR BONACA: We should move to the example, because that seems to be the center of the problems.

MS. DROUIN: And we're there.

MR. PARRY: Yes, we're there. The last point on this slide was just - I think it was - raised

the issue that it is not so much the parameter, the standby failure model, it's the model itself. And we have added words on that, too.

Okay, so we are going to talk about the appendix A. I'll give it a brief introduction and then I'll hand it over to Don.

What we wanted to do with this document was to provide an example that exercised as much of the document as we could. So the things we focused on for example are, well, how are you using the PRA to generate the results you need? What - it's broader than perhaps the scope of the document, although not broader than the scope of what is in Chapter 7, how you determine what the scope of the PRA should be, so we have addressed issues like how do you determine which of the hazard groups you should incorporate, and which can you not incorporate, legitimately, and to that extent there is a very nice little example of the seismic theory as a sort of bounding analysis - okay, John doesn't think it's very nice but I think it's very nice. Then there are some examples of screening of the other hazard groups.

But we included contributions from more than one hazard group deliberately, so that you can see how it is necessary when you reason the PRA, to

decompose the results to understand the contributors. So we think that is one of the key messages that we want in this document is that you don't do things blindly; you really need to understand where the results are coming from as a precursor to identifying what the sources of uncertainty might be that can impact the result.

So what we did was, we chose a particular application which is not an unusual application, which is looking at an AOT extension of an RHR system for an unnamed BWR.

MEMBER BROWN: What is an AOT extension? What is an AOT?

MR. PARRY: Allowed outage time.

MEMBER BROWN: Say that again?

MR. PARRY: Allowed outage time. It's the time that you can use -

MEMBER BROWN: I understand. Once you gave me the name, I can go from there.

MR. PARRY: Okay, all right.

So on that note I will hand it over to Don and Doug and Ken that primarily provided the example.

MR. VANOVER: Okay, my name is Don Vanover from Erin Engineering. And I started working with this program after Doug True and Dr. Ed Burns and

Ken had developed the initial EPRI report in 2004, where the main focus of that report was identifying all the potential sources of uncertainty. That list has been maintained in Table A-4 of the current EPRI report, and that is a valuable starting point for what we are doing now.

There was also some guidance in that initial report that tied to identifying key sources of uncertainty as the standard was written at that time.

We published a second report trying to apply the process that was outlined earlier in the 2006 timeframe. At the same time Reg Guide 1.200, Rev. 1, was getting finalized, and that was issued, and changed the wording to just identify and characterize the source of uncertainty.

And then key was reserved for applications.

So given that background the EPRI report was being looked at by the NRC. EPRI started working with the memo of understanding. NUREG-1855 was in the works, so it was obvious that we needed to collaborate or you know lest we develop something that was contradictory that both the industry and NRC would be referring to.

So we started in 2007 with some lively

discussions looking at our methods that we had originally proposed in the original 2004 EPRI report, compared with the thoughts that were in the works for the NUREG-1855, and we've been working closely together in the last two years, and it's evolved to where we are now to what seems to be a pretty good consensus approach, independent of the different identification of sources of uncertainty, but the approach to try to identify those.

So that's sort of some of the background of how we got where we are.

The example as Gareth indicated is for an extension fo an allowed outage time for an RHR system. So that the acceptance guidelines are defined in Reg. Guide 1.177 for a tech spec change. That refers us to the regional figure for delta CDF and delta LERF in Reg. Guide 1.174.

And then part of 1.177 we have the five minus seven, conditional change in core damage probability, and five minus eight, conditional change in large early release probability, for every entry into the extended allowed outage time.

Given it is an analysis of trying to keep the plant at power, we only looked at events that were applicable at power, from the PRA model. So we did

not do a specific low power shutdown analysis. That was obviously not needed since the goal was to stay up power for the duration of the allowed outage time.

The only way that would have been an issue is if we were challenging the other limits, the other side of the curve in the Reg. Guide 1.174, but since we are dealt the calculations maintained in Region III, then we didn't have to do an absolute check of the CDF and LERF to make sure we didn't exceed those limits.

So that is part of the process. It's first defining what the scope is, what the acceptance guidelines are, and that is laid out in both the EPRI report and the NUREG, that is the first step in the process.

Next slide. So the key part and what we tried to demonstrate in the example is that you need to really understand the results of the model as it is shown. We had quantified information from internal events, internal floods and internal fires, and we looked heavily at those insights for the allowed outage time at this two-loop plant. We had to run both the cases with the A loop out of service, look at what insights came out of that. Then we had to look at the B loop out of service, and we had to run the

model for both the internal events, flood - which included floods and fires. And the insights were obtained by looking at not just the absolute value of those case runs with the different loops out of service, but the important thing is to look at the delta from the base model. And the insights we gleaned to try to identify the sources of uncertainty were based on looking at that delta.

So it's never a simple look at one case model run and see what insights you can glean from it. We had to do four separate case runs effectively and look at the deltas through the base for each of those four individual cases.

So we were able to do that for the fire and internal events and floods. A lot of the appendix goes into detail of, you know, laying that out and the process we went through to get those insights.

There is a brief quantitative screening of seismic analysis. So for that we referenced the hazard curves for the site from NUREG-1488; developed a midi-initiating event tree for different seismic hazard groups; and then looked at what the impact on the site would be for the different types of events.

The most dominant type of seismic event would only lead to a transient at the site with no

major equipment failures. So given that, and the frequencies associated with that type of seismic event, we looked at the internal events model, and what would be similar impact. And that would be a transient event with loss of PCS, loss of power conversion system.

So we compared what the CDF and release fractions, large early fraction. But it's from those events, compared that with the frequency of the seismic event that would lead to those similar type of transients, and showed that it was roughly 1 percent of what was already in the model, so we quantitatively screened it that way.

MEMBER STETKAR: They are not going to go past that, and I just have to get a quick thing in. It's unfortunate we didn't have time to kind of go through the appendix in detail in a subcommittee meeting, where we could talk more extensively about the specific examples. But to kind of highlight a couple of my concerns about the appendix, and this is just an example, is that - I read through that, and there were a couple of places where I didn't think that indeed the analyses that you did justified the conclusions that you had done a bounding screening type analysis.

For example you seem to treat seismic induced loss of offsite power - an internal event - as independent from your analysis of seismic induced LOCAs, because you have a separate treatment of seismic internal events and seismic-induced LOCAs, and you go through analysis. While indeed they are not independent; if you have a seismic event that is strong enough to cause a LOCA, you don't have offsite power. So they are combined events, and yet the analyses treat them separately.

That doesn't detract from the general guidance about how to think about the problem, which is excellent. It's the old devil in the details in the examples. Once you transition from how to conceptualize the scope of this problem, which is I think really good in the first part of the appendix, then you start to implement that concepetualization in specific numerical examples is where I started to have a lot of detailed comments, which are obviously - we obviously don't have time to go through them in this format. So I'll just leave that as one example, since you mentioned seismic, and just leave it there.

MR. VANOVER: The way the graded approach worked with the initiating event tree, maybe it wasn't as obvious as it needed to be. But if we had a LOCA,

then we also assumed a loop. I mean it had - it was - you know, one was the worst - if the LOCA curve of the loop occurred, then the loop occurred. So maybe we need some clarifications. Then the boundary condition would be applied in that simple bounding example for LOCAs, we used loop boundary conditions. Maybe that wasn't obvious.

MEMBER STETKAR: That certainly didn't come through. But again - and if it didn't come through to somebody who's played with this, it's not going to come through to the general practitioner, let's say.

And again, that certainly doesn't detract from the general guidance about what to think about. It's the details of the actual calculations, and how much information is presented, and what caveats are presented, or what caveats are not presented.

I'll just leave it there, because we are getting -

MR. VANOVER: Okay, and I'll go through that we did similar type analysis with different seismic categories. We referred to insights from the internal events to come up with what we thought were bounding calculations for the contribution from seismic. So I won't say anything more about that.

The other piece of the up front work was to qualitatively screen the remainder of the hazard groups, and that's up front on page five and six of the document. And for various reasons either RHR would not come into play for different types of postulated hazard groups, or the impact of the hazard group is independent of whether RHR is available or not. So we spelled that out in a simplified manner in the up front section for each of the hazard groups. And I think that is probably going to be what is going to happen with a lot of applications in the near term for many of these other hazard groups.

Okay, next slide, Mary.

When we went through the detailed analysis, we had to do all the different case runs, aggregate the results from the different contributors. What we were quantifying, what's shown in this table, is the aggregate impacts from both the fire and the flood in the internal events model.

So these were the second set of base case results if you will that did implement easy to measure comp measures. So some of the identified comp measures in the example would be no maintenance on other key trains while the given RHR loop is out of service, or other key components.

So given that is an acceptable comp measure that is easily measurable and can be easily controlled while you are in this allowed outage time, we did take credit for that. And that enabled us to get below the acceptable guidelines for all of the figures of merit.

MEMBER APOSTOLAKIS: So this table includes compensatory measures?

MR. VANOVER: Only the compensatory measure for no maintenance on other obvious systems, something that is easily measurable. We just zeroed out those maintenance terms.

MEMBER APOSTOLAKIS: And these figures of merit are mean values?

MR. VANOVER: These are the mean values, yes.

MEMBER BROWN: Were there other bounding values?

MR. VANOVER: The bounding values are not -

MEMBER BROWN: That's obviously something on either end if you are using a mean value.

MR. PARRY: Actually that is what the acceptance guidelines require is comparison with the mean values. That's the way they are stated.

MEMBER APOSTOLAKIS: So these are the mean values of the baseline PRA that does not include a lot of the stuff that the NUREG is dealing with, model uncertainties and completeness.

MR. VANOVER: Right, this is the best estimate of -

MEMBER APOSTOLAKIS: Well, it's not the best estimate.

MR. PARRY: Yes.

MEMBER APOSTOLAKIS: Okay.

MEMBER BROWN: The title of this is, this is the result supplied to the decision makers, whoever did this evaluation, and somebody has got to say yes or no.

MR. PARRY: Not yet.

MEMBER BROWN: Not yet?

(Simultaneous speakers.)

MR. VANOVER: This sets the framework for what we are going to do now. So these are - if we didn't meet the acceptance guideline to begin with, then we couldn't meet the application. So the first step is to show that you meet the general acceptance guidelines for the license amendment request, and then now we are going to say, okay, we met them, but now we are going to deal with uncertainty and figure out what

is important to having confidence that we do meet the acceptance guidelines.

MEMBER BROWN: Who is the decision maker?

MR. VANOVER: In this example we would be submitting to the NRC and going through RAI process to determine different things.

Okay, next slide.

Okay, in the - starting with the middle part of the appendix, the - what we did then is decomposed all the results, the aggregated results into the different hazard group contributors, and looked for what were the dominant group contributors to each of the delta assessments, highlighted things that showed up as potentially key sources of uncertainty, and that was based on a detailed review of the accident class contribution from the internal events model, the initiators, where we outlined the different initiator and percent impact on the delta assessment for both the A loop and B loop cases.

We provided a limited set of cut-sets and importance measures just for the purposes of report, but we had a lot more than that that we looked at. And this list of issues is what we identified first from the internal events assessment of what could be potential key sources of uncertainty. And this is

just from the dominator contributor perspective, not from looking at table A-4 or other sources of uncertainty.

MEMBER STETKAR: That's what I was going to ask you, Don, is that the whole appendix and the examples are focused on a - let me call it a top down in the sense of important visible contributors to the results using standard ways of cutting the PRA results, important measures or contributing sequences or cut-sets or whatever. It's looking at the results and looking at the top of those results.

There doesn't seem to be any attention paid to the fact that uncertainties might significantly affect the things that you can't see. In other words, the things that you quantified, this is not a completeness of the PRA issue; it's things that you quantified but are numerically smaller than wherever you have drawn the line to look at the important contributors. And how could the uncertainties possibly affect those contributors? Could they force them to rise to the surface?

There is some discussion of that in the main body of the NUREG, but again the examples here don't kind of follow through on that kind of comprehensive thinking about uncertainty and how they

might affect your overall competence, let's say, in the results. I'll just make that as a comment.

MR. VANOVER: I think that is a good comment. The process -

MEMBER STETKAR: It consistently looks from the top down and searches for potential sources of conservatism, if you will, that might be making those contributors at the top of the list and might make them worse.

MR. VANOVER: Right.

MEMBER STETKAR: Or better in some cases, but might affect those top contributors without applying you know any focus - I was going to say equal focus, but any focus - on equal and opposite effects.

MEMBER APOSTOLAKIS: Don, is there another way of putting it, these insights are really based on what has been done without asking what else could be done or done differently.

MEMBER STETKAR: But my point is that what has been done is down there in the set of results that you haven't focused on. That has been done. It's not that - we are not talking about issues of completeness of the models or these known biases because I didn't quantify some contributors that I know about. We are talking about things that you

actually quantified. An example, and I don't mean to focus on things, but suppose a human error probability was a factor of a thousand times too low, and it artificially suppressed a whole series of cut-sets, because it's common to all of those cut-sets.

And because those cut-sets are suppressed, you don't identify that human error as a potential contributor to your results here. It's something you have already quantified. It's not something -

MEMBER APOSTOLAKIS: But that's what I mean. What has been done within you know I don't know the confines of what they did. Not that they didn't do other things, but these are the dominant contributors based on the numbers they used.

(Simultaneous speakers.)

MEMBER BLEY: They are.

MEMBER STETKAR: Again, in the sense of how a practitioner will interpret this appendix.

MEMBER APOSTOLAKIS: No, I understand your point.

MEMBER STETKAR: The guidance says, if all I need to do is look at the top. I don't need to worry about this other phenomena.

MEMBER BLEY: Where your process might have identified a source of uncertainty that could

have elevated it.

MEMBER STETKAR: The process in the main body of the NUREG indeed does speak about the fact that you need to look at not only the top of the pile, but also the bottom of the pile. We didn't talk about the bottom of the pile as much but it is in there.

MS. DROUIN: But however, in many cases - I mean if I go back, when we used to do sensitivity, then you were only dealing with what you had ultimately retained. But now in many cases when you are doing this, you are redoing the whole model.

MEMBER STETKAR: But this doesn't do - the appendix does do that. It still works within the constraints of the retained -

MEMBER APOSTOLAKIS: Would it be proper, instead of saying here are the human errors, say, no, now you have to look at those human errors.

MEMBER STETKAR: You know, it's too much detail to -

MEMBER APOSTOLAKIS: No, but would that be a way out of this. Because then you wouldn't have to worry about the example you gave where something was dismissed. But now you say, let me look at it again. Whereas here you are not looking at it again.

MR. PARRY: I think, too, part of it is

is that the walks included in table A-1 of the EPRI report, typically those sources of uncertainty that they think can affect typical PRA, okay, what's in A-4, for example, are the things that might affect specific portions of the PRA, like ATWS, bring that one up. In this example that wouldn't be exercised, because it would still remain really low. So we wouldn't be thinking about looking at those sources of uncertainty. Maybe we didn't explain that, but I think there is a structure to the sources of uncertainty in the EPRI document that is based on what is most relevant to Level 1 PRAs and LERF.

MR. VANOVER: And we did try to - I agree, we did do a top down approach in laying out the important contributors, and that is consistent with the process as outlined in figure 4-1 at EPRI coordinated 5-2 or something in the NUREG, and we tried to address that by looking at the source of uncertainty from the base model, and we considered a couple in the appendix. But then we didn't carry this forward; we dismissed them for various reasons.

So we did try to do what you are asking for.

MEMBER STETKAR: I guess it's time, since you brought it up, and - I think that from my

perspective trying to think about this as a collaborative effort, we have NUREG, we have EPRI reports. The NUREG is a document being issued by the agency. The EPRI report is a document being issued by EPRI.

I recognize how the EPRI report, how kind of the things are laid out. A bit of my concern is, should the agency be in whole force adopting all of that directly? Because once - when you say, well, in the EPRI report we have things organized this way, and I have no problem. I mean that's EPRI, the industry decided that this is the approach they want to take.

The question is, does the agency want to completely adopt that by example that will be cited by users as NRC-approved methodology? Or does the agency want to step back from that a bit and say, here are some really good ways to think about the problem without getting bogged down in the details of these examples?

MR. PARRY: I think we - one of the things we were trying to do consciously is to try and come up with a pragmatic approach to this, which is really to focus on the things that are important. I mean I'm not sure if we can ever satisfy you without looking at all the sources of uncertainty. We have to

have some sort of screening approach.

MEMBER STETKAR: But Mary mentioned something that might. Mary said, remember in the old days when we used to do sensitivity analysis by requantifying the whole model.

MR. PARRY: That's what these are.

MR. CANAVAN: Actually, interestingly enough, I think we are missing a key point. This is for any uncertainty that would affect this application as written, so a model has performed an uncertainty evaluation is done on that, a base model. And then that base model will suggest that you reflect a change. Then that model is requantified with the change. Then what you are looking at is uncertainties that affect the delta, the cause and effect relationship.

So we don't want to just look at random uncertainties. It has to be one of the ones that's in the cause and effect relationship. In other words, we had an application; it has this effect on the model; and whether the uncertainties that can change that cause and effect. And so that is where our focus is, and maybe we lost some of that or didn't emphasize that.

MEMBER STETKAR: But there again, we

don't want to get bogged down in the details of the specific example or specific numbers. Because human error probability for some error with - a maintenance error that could be elevated to much more importance under an extended outage time of the second train, for example.

MR. CANAVAN: There's a cause and effect.

MEMBER STETKAR: And in fact human error probability is a factor of a thousand too low, and it doesn't meet your list of cut-sets that you are looking at, you are not going to identify that as something to think about, as something that could be sensitive for this particular application, for this extended outage time.

Yes, that's detail, which I actually want to stay away from the detail here, because it is wasting the rest of the committee's time.

MR. VANOVER: The fact that we are meeting the standard requirements for developing the human error probabilities in the model; hopefully we don't have a HEP that's off by a factor of a thousand.

MR. PARRY: And the other time to make those, I think - and Don correct me if I'm wrong here - but I think when the HEP sensitivities were done, they were done for the whole set, in the model. And

the model requantified. So the cut-sets are going to be different for sure. They are not going to be the same cut-sets. We are not just taking the cut-sets, and changing numbers in the cut-sets.

MEMBER BLEY: I am wondering, Don, and I was unfair earlier, Gareth, we had been talking about the sensitivities, I had focused on them. I am wondering, Don, and I don't remember the specific examples, but the cases you mentioned where you did surface a couple of things that got dismissed. But with that kind of a thought, just a little text saying, some times these things that come up can be important just to identify them so that we don't slide past them so easily.

MR. VANOVER: On page 40 we tried to relook at things based on the base model assessment that was done in identifying the potential source of uncertainty. Part of the input to identifying potential sensitivity cases is relook at that base model assessment to see if there is something else that should be considered.

Frankly we did look at it, but given this application was somewhat straightforward, and what was dominating seemed to make sense, we didn't identify a lot of other things to consider.

CHAIR BONACA: We need to move on.

MEMBER APOSTOLAKIS: I think we have exhausted this issue.

MR. VANOVER: Okay, I won't go through all the details here. But based on the detailed review from the internal events we had identified these six potential key sources of uncertainty, including some human actions, and the ability of CRD injection to remain viable post-containment failure scenario.

MEMBER APOSTOLAKIS: This conclusion here is not based on sensitivity analysis.

MR. VANOVER: That's correct.

MEMBER APOSTOLAKIS: This is just - this is what we know, these are potential - okay, let's go.

MR. VANOVER: These are the potential sources of uncertainty. So go ahead to the next slide, Mary.

We also did a detailed look at the fire results, internal fire results. And a lot of the same human actions that were important in the internal events, and the same assumptions, model uncertainty issues, also were very important in the fire analysis.

So that was - those were identified as cross-cutting issues impacting both models.

Then we also identified a couple of other issues that were unique to fire. Just in general the scenario initiating event frequencies based on some more recent EPRI work that has been going on the last year, we have some reason to believe that the methods that were used for this plant may have been conservative in the development of those frequencies that included data all the way back to 1968 in the identification of generic frequencies; and that in general the methods of the fire scenario treatment we don't credit every potential PRA model system in the fire analysis, and for things, we don't have cable information.

And we also take limited credit for - we take no credit for X control room manual actions in short time frames, and we also have some other embedded conservatisms in the model that factor into the analysis.

But I think the key point to bring across here is another detailed review was done to see what additional insights could be obtained from the fire results.

MEMBER APOSTOLAKIS: Are the fire experts in the agency agreeing with your last bullet?

MR. VANOVER: Ken?

MEMBER APOSTOLAKIS: Are the fire scenarios given conservative?

MR. CANAVAN: For a function of the - well, I don't think this is a specific - the second bullet is a specific modeling issue. The first bullet, the scenario initiating event frequencies, are high, I think we had general agreement on that.

MEMBER APOSTOLAKIS: For the second?

MR. CANAVAN: For the second bullet.

MEMBER APOSTOLAKIS: We have all this work going on trying to understand cabinets and smoke.

MR. CANAVAN: I know, I'm up to my eyeballs in it.

MEMBER APOSTOLAKIS: Yes, sure. And then to make a blanket statement, the way we are doing it is conservative.

MR. CANAVAN: But it's for this model and this evaluation. So in their model they came to the conclusion that they didn't have cable information, they didn't credit the system at all, because they didn't know where the cables ran, but that is relatively conservative, because if the fire is in the reactor building corner, and they are looking at feedwater -

MEMBER APOSTOLAKIS: Did they include for

example the impact of smoke?

MR. CANAVAN: Model specific again.

MEMBER APOSTOLAKIS: So there was no need here to do that? There is no smoke here?

MR. CANAVAN: I don't think they have smokeless fires. But I'm not sure that - I'm not sure how the model treated -

MEMBER APOSTOLAKIS: I find it too strong a statement.

(Simultaneous speakers.)

MR. CANAVAN: Maybe it needs to say within this model.

MS. DROUIN: Right, this is not a general statement about fires. This is a statement strictly within the context of the model used in this example. And this is just - and this is just on the Vugraph.

MEMBER APOSTOLAKIS: No, it's also in the text.

MR. PARRY: But it is intended specifically for this application and this model. It's not a general statement.

MR. CANAVAN: Yes, we need to - that is a problem, I think. I was just taking a note, interestingly enough, that was saying substantial discussion of the fact that in this model, and in this

example, we may have been a little quick to dismiss certain things where that dismissal wouldn't apply to a different model.

So we need to be careful and say, this is what we are trying to do here. We are trying to look and see how this plays, in this model it's conservative, in your model it might not be, so think about the effect for your model.

Maybe it needs to point back to the text in the document where we have the deeper thought.

MR. PARRY: And also, we hadn't really focused on the fire contribution in the sense of illustrating the - at least the sensitivity part of the model. It wasn't our main focus. We needed it in there because we wanted to discuss how to decompose the results for the different contributions. It's really just through the aggregation issue which we discuss in the document.

MEMBER APOSTOLAKIS: No of course, readers like us, even if you put these extra sentences that Ken mentioned, we have no way of convincing ourselves that this is true, the analysis.

MR. CANAVAN: That's correct. It's supposed to be illustrative.

MEMBER APOSTOLAKIS: So what if you say,

then, if the treatment of fire scenarios is conservative.

MR. CANAVAN: Yes, I think it should say -

MEMBER APOSTOLAKIS: Something to that effect.

MR. CANAVAN: It should say, in this particular model it was conservative. If it's not, you need to do this; if it is, you need to do this. And that is the kind of discussion I think we need to have, plus pointing back to the text of the model that says, don't forget what you are really trying to do -

(Simultaneous speakers.)

MEMBER APOSTOLAKIS: This is the first time we saw it. Why didn't we see it at the subcommittee meeting?

(Simultaneous speakers.)

MS. DROUIN: This was one of the things that we were planning on doing we told you when we came back, which is now, we would have the example.

MEMBER APOSTOLAKIS: Because this is not the place to actually - but it's very hard. I was really struggling with it. Because I agree with what you guys said earlier, that there is a lot fo good stuff in there, but there is a lot of stuff I would

not be comfortable with.

MEMBER BLEY: It's hard, it's probably impossible to find an example that illustrates all the things one wants to illustrate. And caveats don't quite work, because people see this, and they replicate it handbook style despite everything you say in the main report saying don't do that. I guess that is just kind of what we are kind of hanging on.

MEMBER CORRADINI: And so can I go there with that, since you guys are all the detail people? I'm struggling with having an appendix with one example. And now we are getting to a point that strikes me - it seems to me if this is going to be useful, you ought to have some sort of web-based library of examples, and this is the starting point, and it is one of many. I mean it's almost like benchmark problems. You are essentially saying, I have a methodology. This is how you move through the methodology, and here is an example of how you exercise the methodology. But this is one of N.

It strikes me that at least Appendix A ought to at least have a preface that says, this is one of N, it's an example, it's a demonstration. It's not the way to do it, it is a way to do it, and we expect to see N more coming in the future in the

revisions to this.

MR. PARRY: We say that in the beginning of the example in italics, more or less.

MEMBER STETKAR: They do. The problem is -

MEMBER CORRADINI: But more than just this one?

MEMBER STETKAR: - people's experience shows that people gloss over that. I hate to say it, but they do, they gloss over the fact that this very quickly transcends from being a very very specific example of a very specific application. Because if you listen to the responses to a lot of the detailed comments, they are, well, you have to recognize that for this particular example it was done this way. People, the general reader, loses that very quickly, and it very quickly becomes guidance for an acceptable way to do it.

MEMBER APOSTOLAKIS: But I do like, though, Mike's suggestion for having more than one example.

MEMBER BLEY: Mary, can I ask you a question? George asked if you could publish those without the appendix, and you said, it would lose a lot, and I think I agree with you. There is a lot in

here that is helpful.

Is it possible to publish the main report and a separate draft for comment in the appendix?

MS. DROUIN: Well, I was going to get into this when we got to the end, when we talked about the future work and the publication of this. Do we want to talk about this now, or do we want to let Don get through the rest of the example? Why don't we let him finish with the example?

MR. VANOVER: Next slide.

Okay, the parametric uncertainty evaluation in this example was fairly straightforward. Given the cut-sets we did not include any dominant contributors with state of knowledge correlation included. So by a review of cut-sets we were fairly confident that the mean values would not be far off from the point estimate values, and this table basically confirmed that.

So we did do the full propagation to confirm our insight based on looking at the cut-sets, but to show the process we did go through the full propagation, and there in all cases they were very close.

MEMBER APOSTOLAKIS: But what is the message you are sending here? I mean if I am now to

apply to pick up the NUREG, look at the example, and have my own example, different license application request, what are you telling me here? That I should do it both ways? And why should I do the point estimates if I already have done the mean ones?

MR. CANAVAN: You get them first.

MEMBER APOSTOLAKIS: There is no reason - yes, what do I do first?

MR. CANAVAN: Yes, that always comes out first. It comes out with a point estimate. Then you usually run a separate code to produce uncertainty. So you have the point estimate. Doing the propagation is another step.

MEMBER APOSTOLAKIS: So propagation of mean values means what? It's still point estimates, but it's of the mean values?

MR. CANAVAN: Yes.

MEMBER APOSTOLAKIS: And there is a third calculation with the full uncertainty?

(Simultaneous speakers.)

MEMBER APOSTOLAKIS: My question is, why bother with the second then if I do the first?

MR. PARRY: This is really meant to illustrate the -

MEMBER APOSTOLAKIS: Yes, but if your

message is that in this case it didn't really matter. Why do you also say, my example worked? It's not going to matter here, so I'll do the point estimates.

MR. PARRY: We would have had to fake up an example where it did matter, I guess, in this case.

MEMBER APOSTOLAKIS: That's right. It's really puzzling me. I mean it seems to me it's not difficult to do the rigorous thing, is it? I mean you take SAPHIRE or CAFCA or whatever and put the uncertainties and it does it.

MR. VANOVER: It's not difficult. The first answer is the point estimate, and then we tend to get - and the importance measures are based on the point estimate, and we look at that. And this was confirmatory in our case that the propagated means -

MEMBER APOSTOLAKIS: So somebody in the future then will only do the point estimate?

MR. VANOVER: Possibly yes.

MR. PARRY: not necessarily. Unless they - if they follow the guidance, no.

MEMBER APOSTOLAKIS: We are beginning to run out of time, so let's keep going.

MS. DROUIN: Okay, let me jump in, and maybe we don't finish the example, because we do need to talk about what we need to do with this example.

Because I just think the next slides we are going to get into more.

As I've been listening to this, and I'm trying to come to a solution that will meet our needs and y'all's needs. It occurs to me that perhaps what we could do is publish the NUREG without the example, but, the famous but, come back to a subcommittee hopefully in March, early March, and then publish an addendum, a draft addendum, it would be published as a draft addendum. Because we really want the public to have this example before them, and have read through it, before the May workshop.

MEMBER CORRADINI: The key is the workshop.

MS. DROUIN: Is the workshop, so publish the document without the example -

MEMBER APOSTOLAKIS: Without the appendix?

MS. DROUIN: Yes, without the appendix. Come back to a subcommittee in March, where we get your detailed comments, we take those into account, and then we publish an addendum that is just the appendix, and it gets published as a draft.

MEMBER APOSTOLAKIS: You have a hell of a lot of experience with the ACRS, Mary. I like what

you just said. I do, I really do.

MS. DROUIN: Well, thank you.

MEMBER RAY: And then the suggestion of an example that illustrates the problem rather than confirming the point estimates is I think an excellent thing. In other words a cautionary example rather than a "everything is okay" because it's -

MEMBER APOSTOLAKIS: And I think that is why will happen in the - at the subcommittee meeting that Mary suggested. We are going to give and take.

MS. DROUIN: We won't make any changes - we won't have anything to give you for the 30 days in advance, but we can come to the March subcommittee saying, we have now heard what you said, and we have some ideas, and then y'all offer your ideas. And then that puts me in early March, and then I can issue this as a draft addendum in the April timeframe.

MEMBER APOSTOLAKIS: When is your work trip?

MS. DROUIN: Why don't we just go straight - oh sorry.

MEMBER APOSTOLAKIS: May 5th and 6th.

(Simultaneous speakers.)

MEMBER BROWN: Can I make - I just want to make an observation on a standard or regulation,

whatever it is, without a set of examples. IEEE has a number of standards that they put out for people to do calculations in various electrical areas, whether it be transformer calculations, blah blah blah, whatever. And if you look at the definition of terms, they are often in the minds of the preparers were very very clear, but in the minds of the users who are not going through all these mind manipulations, they become somewhat ambiguous.

I just finished - the reason I'm bringing this up - because there was not an example in this IEEE standard of the process, the methodology they used, and a manufacturer that we had that was doing a design did one set of equipment, did the calculation, came out, got the right answers, all that kind of stuff, he took his methodology, applied it to one that had a slightly different configuration of the same stuff, where he had to come up with numbers from a different source book on that design. He got the wrong answer. He didn't meet the requirements. He didn't meet the specifications. But he advertised that he did, because I'm spring-boarding off of this, you take the mindless - mindless is the wrong word - you get into, hey, this is the way they did it, and they used this number from this line in the electrical

diagram, they plugged it in and they got the answer, and in one case it was right, and the other case, it was the wrong source.

So all I want to say is, I think examples are valuable, but I also want to echo that you - they can't be ambiguous, or I don't know if that is the right word or not, but that's what I comment - as a non-PRA expert it looked kind of fuzzy when I got down toward the end.

MEMBER APOSTOLAKIS: Don't forget - I mean I fully agree with what you said, and I think the spirit of the comments that we have been making is along these lines. But another important, very important consideration here is that if this is - this will be a NUREG report, which means the staff is blessed. It creates precedence. Somebody else comes later and says, I put everything on the 95^{th} percentile, and we complain, he says, what are you complaining about? So that's a major consideration.

MEMBER STETKAR: I understand. That's why examples, and how you get data and where you use it, how you use it, is valid for those people who have to use it. That's all.

MS. DROUIN: I want to ask my management what they feel about, because I just threw this out

without talking about my proposed solution. I'm putting my job on the spot.

MR. MONNINGER: Which is good, because maybe I can respond and say I don't have a response. I think we can consider it. I think it's good to have good guidance out there, thorough guidance, et cetera. There are issues with schedule. I assume you guys are considering the letter later on that Mary would monitor those activities. Could we report back then?

MEMBER APOSTOLAKIS: I don't understand, what did you just say, John?

MR. MONNINGER: With regard to what Mary is proposing, to give you further our insights.

MEMBER APOSTOLAKIS: Yes, what? Are you asking whether the ACRS is supportive?

MR. MONNINGER: Yes, as opposed to responding -

MEMBER APOSTOLAKIS: One member is. I don't know about the others. We cannot speak of the ACRS, and the ACRS will not tell you now. But you are welcome to come later today or tomorrow when we discuss the draft letter.

MR. MONNINGER: Good.

MEMBER SHACK: I don't like this idea you should give reasons why you don't like it.

MEMBER APOSTOLAKIS: Sorry?

MEMBER SHACK: I was just suggesting to John that if he doesn't like this idea it's - you should speak up.

MEMBER APOSTOLAKIS: He's not ready. If you want to speak up, speak up.

MR. CANAVAN: Well, what we are discussing is the proposal that Mary had.

MEMBER APOSTOLAKIS: No, we can't really make a decision.

MR. CANAVAN: No, I wasn't asking for a decision. I was just trying to get what the discussion was.

MEMBER APOSTOLAKIS: You want to add to it?

MR. CANAVAN: No, it's just putting the NUREG out without the example, and then later -

MEMBER APOSTOLAKIS: And then, yes, and then have maybe a more detailed meeting with us or some of us on the addendum as you call it back and forth, and make sure that there is some sort of consensus as to what -

MEMBER BLEY: But getting that out before you public -

MR. CANAVAN: I would like to weigh in as

a stakeholder if I might, as a representative of the industry, they have been after EPRI to get this guidance to them for five years now, so there is significant pressure to get some resolution for some approach. And right now there is no guidance. So I would say some guidance that isn't in error; in other words, some - any level of guidance is extremely useful to those folks.

MEMBER APOSTOLAKIS: The NUREG, one possibility is to have the NUREG out as soon as possible. It's the exercise at the end, the example that seems to create problems. So that can be delayed a little bit, but we will do our best to support Mary to have it before us at least in some form.

MS. DROUIN: The solution I am trying to off, that we publish this NUREG without the example, and we publish the example -

MEMBER APOSTOLAKIS: In some form later.

MS. DROUIN: In April. Now in meeting an April date, I am not talking about that we are going to have the time, because there is not the time, to go and do a really huge format change to this example. But going through and adding you know where we think appropriate, the right caveats, the right cautionary notes, that we can do in this timeframe. And that is

what I'm hoping if we have these cautionary notes in there, then we can look to after the workshop, because I think we are going to get a lot more comments on this coming out of the workshop. And then after the workshop stepping back and saying, okay, what do we really need now to make this example really work. And maybe everybody is happy.

MEMBER APOSTOLAKIS: In my mind, based on what I have heard, I would really love to see a NUREG report with several examples in the future in the appendix. Applications, or whatever.

MS. DROUIN: But that's way down - that's in the future.

MR. PARRY: Unfortunately, George, I don't think the NRC staff is going to be able to do that. I think this would have to come from industry.

MEMBER APOSTOLAKIS: But you have an MOU.

MS. DROUIN: Well, I mean those are all things as I said, you know, we foresee that there is future work here.

MEMBER BLEY: Mary, let me ask you, what I heard you say is, you come back to us, you think about adding some caveats and the like, and you issue it as an addendum for comment, is that right, or a draft addendum?

MS. DROUIN: A draft addendum.

MEMBER BLEY: So it wouldn't be a final out there?

MS. DROUIN: It would not be final. We would issue it in a draft. And then after the workshop, you know, we hand out -

MEMBER BLEY: More information.

MS. DROUIN: Where we got more information, then we would bring it back into - either we would make a quick change right then and issue it as a final addendum. I don't want to make promises, because I don't know what is going to happen with the workshop. So coming out of the workshop it may be that we keep it as an addendum, because there is enough information coming out of the workshop that we need to do some significant work to the example.

Or it could come out that we come out of the workshop at the other end where we are happy with the example, then we could pull it into the next revision of the NUREG or we issue it as a final addendum.

MEMBER APOSTOLAKIS: There are some details to be worked out.

MEMBER MAYNARD: I think the thing we need to consider - and first of all I'm all for

examples, and the more examples the better - I think that what we have to take a look at for this, and I don't know the answer to it, is this more valuable with the one example or without any examples?

I mean the commitment could be made to provide more examples later, and - or this could be taken out - if we were to propose that this be issued without the example, does that strengthen the document or does it weaken the document?

MEMBER APOSTOLAKIS: Well, the question is not posed as to whether - the way you put the question you assume that the example is in good shape.

MEMBER MAYNARD: Just as is.

MEMBER APOSTOLAKIS: It does not add. I think Mary's proposal, and we can work out the details, is a way out of this.

MS. DROUIN: And you know, please don't forget when we look at the future work, and as I have said before, we have already started in the works, the things we know we want to do to this document. And again I said there are some short term things, and there are long term things. We know that there are going to be insights and lessons learned coming out of the workshop in May, so we already have it in our plan to revise this NUREG document.

So personally I think it devalues the document by taking away the example. We are going to revise the document, and at that point we can also revise the example. But we need to publish the NUREG.

MEMBER APOSTOLAKIS: Any other - would you like to add anything?

MR. CANAVAN: I have just a few short comments. One is we have appreciated working under the MOU. We think it's been very effective in ensuring that the research is complementary and that the results are clearer than they would have been separately. There is a - there is an urgent need for the information, just as an aside, in your deliberations.

MEMBER RAY: But on that point, this urgent need, I just want to point out that it is contrary to Mary's vision that - well, let's put it out there and just tell everybody we are going to further revise it later, it is going to get sucked up and used, because people are really anxious to get it. And if it's not - if it winds up misleading people now, it will be a tremendous job trying to turn it around later.

MR. CANAVAN: I don't think - I think right now in the absence of anything we already have

misleading. So something would be better than nothing, maybe another subject for your deliberation.

We do intend on expanding the scope to other items, so we will be pursuing putting in external events, fires is the most likely culprit to come into the fold next, and we will be pursuing that in the short term since it takes quite some time to get these things out.

As far as Mary's bullet here to expand support for new reactors, at least from the industry side, from my perspective, we are considering that right now but we are not fully signed up to expanding to new reactors yet.

MS. DROUIN: Okay, the only thing I would like to add is that - is the schedule for all of this. Because I don't want you to think when we are talking about the next revision that we are talking way into the future. Because when I talk about adding you know the other scope items, that's not the short term when you start bringing in - okay, to expand to include internal fire you're talking a year to two years in the future.

I'm talking about another revision in this document in the short term to address the lessons learned coming out of the workshop. So to prevent

exactly - that everybody gets sucked into this version, that we would have another version within a year out on the street that would replace this one.

The only other thing I would add is that I do want to say, the one action item that we did come away - the commitment that we did make, was to go and add in the scope and limitations section a little bit more in terms of making it real clear this version is Level 1 internal events, LERF. And so we did commit to do that, and we will make that change right now, we can get it into the document before we turn it over to publication.

That's all I have. I don't know, John, if you would like to say anything.

MR. MONNINGER: Just, we thank you very much, and we do enjoy the interactions and we find them very valuable. The other areas that I mentioned, HRA digital I&C, and we are looking forward to working with the ACRS.

MEMBER APOSTOLAKIS: Any comments from the members?

Okay, so back to you, Mr. Chairman. Thank you.

CHAIR BONACA: It is amazing.

MEMBER APOSTOLAKIS: It is not amazing.

CHAIR BONACA: With that, I think we'll take a 15-minute break. And I want to thank you, presenters. That was a good presentation.

We will meet again at quarter of 11:00.

(Whereupon, the above-entitled matter went off the record at 10:29 a.m. and resumed at 10:46 a.m.)

CHAIR BONACA: We are back. Nice to see you again.

MS. SCHNETZLER: Nice to see you.

CHAIR BONACA: Okay, 10 CFR Part 73.58, safety/security interface requirements for nuclear power reactors, was issued last year, and we as a committee reviewed the rule in July I believe of last year.

That rule requires that changes to configurations of security be evaluated for their potential of adverse effects, or the capabilities to maintain the safety and security.

Now the staff has prepared a Reg Guide which is essentially one way of meeting the requirements of the law, and they are here to present it to us. And so we are here to listen.

DRAFT FINAL REGULATORY GUIDE DG-5021, SAFETY/SECURITY INTERFACE

MR. HUYCK: Thank you.

First, a couple of brief introductions. My name is Doug Huyck. I'm the branch chief for reactor security, rulemaking, licensing branch, division of security policy in NSIR. Of course Part 73 rulemaking and the guidance development is definitely one of the responsibilities that fall within our branch.

Presenting today is Bonnie Schnetzler. Bonnie is our team lead within our branch responsible for rulemaking and the guidance development.

And also in support we have Tim Reed from the Office of NRR, and Tim has been providing support on the rulemaking and the guidance development.

Our purpose today is to provide you a status, and update, on the Draft Reg Guide 5021, which is managing the safety/security interface.

Our role today as we make this presentation is to receive your acceptance as far as a Reg Guide that would be a means of meeting the regulations 73.58.

So thank you for this opportunity. And at this time I'll turn it over to Bonnie.

MEMBER APOSTOLAKIS: So we are writing a letter on this, Mario?

CHAIR BONACA: Yes.

MS. SCHNETZLER: Okay, good morning. Next slide, please.

Since our last update with ACRS last summer several things have occurred with the power reactor security rulemaking. The rulemaking went to the Commission for approval, and the Commission did approve the rulemaking in December.

It is currently with OMB for review and approval, and we are anticipating and estimating that mid to late March it would be published in the Federal Register. So that is the status of the rule.

We presented to you in the past three portions of the security rulemaking that we think will need ACRS review. And today we are focusing on the guidance for 73.58, and requesting a letter on the acceptability to the Commission of this Reg Guide. The particular piece that we are focusing on is 73.58.

73.58 in part addresses a petition that we received from the Union of Concerned Scientists. They requested establishment of regulations, so that when changes were made at facilities which could adversely affect security, we would have specific guidance for licensees in that area.

The regulation basically has three major

parts. First is that licensees must assess and manage the interactions between security and safety. Second, they must consider planned and emergent activities including EP activities, emergency planning. And then lastly that they take compensatory or mitigative actions when potential adverse effects are identified.

MEMBER APOSTOLAKIS: So would this then imply that you would have to go back to Regulatory Guide 11.74 and add an extra box on security? And if it does not why not?

MS. SCHNETZLER: We did recommend that - in the guidance it recommends that you look at Regulatory Guide 11.87.

MR. REED: Exactly George what do you have in mind on the extra -

MEMBER APOSTOLAKIS: Well, you read the document and representations of course along the same lines, and the message was clear. And I think you also said that's why the UCS petition wanted, that if there is a change in the plan, any kind of change, part of the approval process would be to consider security and the interface with safety.

Well, one regulatory guide that is used extensively in the approval of these cases. So I mean we have a box on defense in depth, we have a box on

safety margins. Wouldn't it be reasonable to add a box, you know, with appropriate words about security? You don't have to do it now, but it seems to me that that's where we're going.

MR. REED: I'm not aware that we have considered doing that. I'm not saying it's a bad idea. But that's the first time I've heard of it.

CHAIR BONACA: You know again, this is one way of meeting the requirement to the law that they have presented. And clearly it is based on two things, one is configuration management with the focus being changes that may impact security, and the other is 50.59, the changes that may affect safety. So it's one way.

MEMBER APOSTOLAKIS: I can interpret this guide that is in front of us today as playing the same role that the other guides regarding service inspection and so on play, that interpreting the basic guide, which is 11.74. So there is no conflict.

All I am saying is that maybe - in fact I think the previous group, Mary's or Gareth, said that they are in the process of revising 11.74. So it seems to me that would be a good opportunity to say something about security.

MR. REED: I understand. I would just

add one thing, is that I think this Committee is aware of this, when it comes to security events, they are initiated by acts of commission, and they entirely proceed by acts of commission, and from a probabilistic risk assessment standpoint it becomes very very difficult to get a handle on that. So from a risk perspective, we would have to be sensitive to whatever we did in 11.74.

MEMBER APOSTOLAKIS: - is risk conformed.

MR. REED: I understand, I just want to throw that out there.

MEMBER APOSTOLAKIS: It's an integrated decision making process.

MR. REED: I agree.

MEMBER APOSTOLAKIS: I notice you are objecting.

CHAIR BONACA: No, I'm not objecting. I'm only saying that when I looked at 50.59 on the sites, it's a very well implemented program in general because it has been around for a long time and has been the focus of a lot of reviews, et cetera. And the sites really are familiar with the implementation of the process.

So I get quite a lot of comfort that they are using 50.59 as a means of identifying possible

impacts on safety resulting from configuration changes for example security changes.

The reverse is essentially a new configuration management program they have to track the effects on security of plant changes. So as you know I'm supportive of this approach.

MEMBER APOSTOLAKIS: Okay, we can discuss it again.

CHAIR BONACA: Right now, this one here that they are presenting is one way of meeting the regulation, and I think it can be effective.

MEMBER APOSTOLAKIS: Absolutely.

MEMBER BLEY: I'd like to follow up George's point. Because I see how this document tells how to bring plant changes under review with respect to security. However it's titled, managing the safety-security interface, and it gives some words up front about safety and security. And yet when you get into the scope every event is having people knowledgeable in physical protection program reviewing all these things against the security requirements, and no links to safety.

CHAIR BONACA: There is a paragraph on safety.

MEMBER BLEY: It doesn't seem to me it

manages the safety-security interface. It seems to me it's all about making sure plant changes come under security review.

CHAIR BONACA: But that's because again the 50.59 process is highly implemented within the sites, and therefore if you refer to that, that means something very specific. I mean sites have thousands of screens on 50.59 every year to perform changes without direct NRC approval. And I think that that is an observation I made at the beginning myself.

MS. SCHNETZLER: And that is accurate.

MR. REED: That is absolutely accurate. We explicitly tried to let the safety side stay where it's been. It's been worked on for a long time going back to the 1980s. So we wanted to leave that intact to the maximum extent possible.

MEMBER BLEY: Just that it seems to me it ought to say that. Because it introduces itself as doing both, and then it never, except for one paragraph saying 50.59, it doesn't talk about how they are tied together.

MEMBER STETKAR: Do you have confidence that the 50.59 process is working adequately to manage - let me say the office of direction, the changes to the security systems that might have an effect on

safety? I mean you apparently have some experience looking at that process?

MS. SCHNETZLER: Can you repeat that again?

MEMBER STETKAR: Yes. Do you have confidence that - Mario said that the plants already have a lot of experience implementing the 50.59 process to look at the effects of changes on plant safety. In your experience do you feel confident that that 50.59 process is adequately addressing changes with specific focus on changes to the security, either security hardware, security programs, implementation, in terms of their effect on safety.

MR. REED: Okay, I have a lot of confidence when it comes from the security side into the safety side.

MEMBER STETKAR: You do?

MR. REED: Okay, tons of confidence -

MEMBER BLEY: Any changes in the security do get -

MR. REED: Once the safety side becomes aware of those changes, okay, once they have knowledge of them, they can look at the full implication of all the changes. So we've bounced the rubble on that side.

What I didn't have confidence in, and I think there were some issues in what's going on on the security side, in the dark so to speak, that these guys didn't know about. And this is what we really have focused, you see a lot more focus on the security side and understanding what changes mean for that, okay.

MS. SCHNETZLER: It's not that when we reviewed the two parts of it, the operation safety part of it is very well developed, but the security portion of it is not to the same maturity that it needs to be, and so that is why you see some of the balance of this guide.

MEMBER STETKAR: And I didn't appreciate that experience when I read the Reg Guide, because it is obviously focused on the direction from plant operations, maintenance, et cetera, impact on safety. And it certainly didn't come through that indeed the existing 50.59 process adequately manages the other direction of that interface.

MR. REED: I would add, it's more than just 50.59 too. It's tech specs, it's (a)(4), it's all your configuration control in the facility. When you go to the security side, it's actually I think a little bit more difficult. It expands out even into

the inner control area, you know, you'll get much broader - some things that may not be obvious to you may be significant in security. So it's a different challenge. And I think most of the interaction issues that were identified from all the post-9/11 stuff that was put in place, and there were a lot of physical changes and these things started popping up, they tended to be on the security side.

CHAIR BONACA: You know one thing I would like to say is that the site already has to meet the requirements of safety and security today, before this Reg Guide. And my sense is that is exactly what they have done. What is in the Reg Guide is the traditional way of doing that, to use 50.59 from a security standpoint, you use what they are proposing here. So that is one of the reasons why I think it documents what really is already happening there. It establishes some requirements in so far as references to several regulations.

MS. SCHNETZLER: You are right, it has always been implicit, but it's never been explicit. And that's one of the purposes of the rulemaking was to make sure that it was.

MEMBER BLEY: One last question for Tim, because you said something very clear. Once they

become aware of it, operations incorporates any changes in the security system into 50.59 and other processes I would think the safety-security interface would try to make sure that they become aware of it right away.

MR. REED: Yes, you're absolutely correct.

MEMBER BLEY: And I don't see that. Am I missing it? Or it already there somewhere else?

MR. REED: It's in 73.58. That's like at the rule level, and this is just trying to implement that. I think we, as ex-licensee, and I have some other ex-licensees here, you put something in the rules, you get people's attention. So we've definitely got the attention of people by making this an explicit requirement.

MS. SCHNETZLER: And even though this isn't a small - I mean this looks like a small rule if you look at the actual rule language. The undertaking of it is actually quite significant, because it does require the licensees to go back through their procedures and processes and make sure those ties are there. So that is a pretty large undertaking procedurally. The scope of it and the complexity of it is pretty large.

CHAIR BONACA: You need to have cognizant individuals with security background and information to be involved in almost every site process. So that's an important element of the rule too, that it requires expertise and knowledge in the processes.

MS. SCHNETZLER: This was published in the Federal Register in 2007. We had public meetings and we received comments. From that point forward we had several public meetings between September of - it says 2009, I'm sorry, it should say 2008 - September, 2008 and January the first week of January of this year, to resolve and disposition those comments. Those meetings were very interactive. We went through paragraph by paragraph with stakeholders, NEI and specific stakeholders including security and operations personnel, so that we had a good understanding. And that is where some of the push toward security came from. WE started with kind of a really big process, and looking at both sides pretty heavily. And then through the course of the interactions began to realize that the safety side of it has very many of those things in place, so that's where some of this sway toward security comes from is that, is through the course of these meetings.

So I just wanted to let you know that it

was vetted very carefully with stakeholders and had significant amounts of interaction.

And we've discussed some of this. The focus of the guide is new types of controls and processes that are intended for review. Review of current licensee processes and procedures, which is quite a large undertaking, actually. And a listing of program areas that may fall subject to this regulation, such as operations, maintenance, planning, and other groups.

It also talks about the types of activities that should be considered such as loss of power - loss of power, removal of security barriers, addition of security barriers which could impact operations. It talks about the screening process, 50.54(a) changes, quality assurance plans, 50.54(b)P, screening changes to the security plans, 50.59, and then it points to Reg Guide 11.87 for evaluating changes touching experiments.

We added additional security related questions for licensees to consider, and like I said this was kind of an amalgamation of security and ops type personnel that thought these questions would help both security and safety. And then there is a discussion in the guide of requirements for training

of site personnel on the program. And I think that is another key piece, that once you have gone through these procedures and modify them to identify the potential cross-cutting issues that both parties need to be aware of, that you provide the training on those changes to make sure that plant personnel are aware of it and how to handle that.

CHAIR BONACA: I think of this as actually much larger than simply the safety-security interface, because any change on the site which may affect the balance of plant components, which is now going to be part of the safety, has to be evaluated for impact on security. So I was looking at the title of it, through the narrow scope. In reality the scope is larger. It's anything that you do on site.

MEMBER APOSTOLAKIS: I thought the questions that you had there in bullet form were very good, and I agree with you that you will need a good group of people who understand both security and safety to answer those.

What's not clear to me is, and maybe you did not deliberately - I don't think you provided advice as to what to do if in say, three of those questions, the answer is yes, there is an impact. You are leaving it up to the expert group to decide?

MS. SCHNETZLER: We actually in the working group that we had on the - working on the Reg Guide, we started down that path, and we realized - and we actually had a really nice flow chart that we were going to put into the Reg Guide. Then we realized that basically the plant has these things covered. If you have a security issue, and you are looking at mitigating other actions, you are stepping into security processes that are already in place that you are either going to provide compensatory measures or some other type of measure that is already pretty well defined.

And then when we looked on the other side of it for you know the other departments, operations and those groups, they already also have things defined. So we were a little uncomfortable about stepping in with a guide, potentially stepping into areas that are already defined and regulated through other methodologies.

MEMBER APOSTOLAKIS: But I don't understand what that means. So I have a problem somewhere. A security measure impedes access to a fire by the firefighters, something like that. Now of course there are many many regulations regarding fires, and there are I'm sure you are getting there

now regarding security. What do I do? I mean you said that there are already things in place so I cannot touch those. So what would I do in this hypothetical case?

MS. SCHNETZLER: The biggest issue I think of the regulation is to make sure that you are aware of it, because once you realize that potentially you may be putting a piece of security equipment in front of a fire hydrant, or fire necessary equipment, then both sides have avenues of changes that they can do or compensatory measures, or other things that they can resolve the issue. It's really the focus of the regulation is to make sure the parties are aware of it.

MEMBER APOSTOLAKIS: And I do appreciate that. I think being aware of something is a giant first step. But I can also see cases where people might say, ah fire, these things never happen, they'll just work around it, these are smart guys, and they dismiss the issue. I guess one way of looking at it is to see how people implement this for awhile, and if they do a lot of this stuff, we come back with - because I do appreciate that it would be really a lot of work trying to anticipate what would happen under each of these questions and what the actions should

be.

The awareness issue I full agree is extremely important.

CHAIR BONACA: There are requirements also for audits, for inspections, and I think that the expectation is that the site polices itself on this issue, and then they are inspected by the NRC.

MEMBER APOSTOLAKIS: I think there is a broader issue here, it's probably in my mind, but it seems to me that throughout the agency, because we saw that earlier this morning too, people will say, okay, there will be some compensatory measures, and everybody is happy. They don't ask the next question, are these effective? Are they affecting anything that - you know are they achieving what you want them to achieve?

We seem to be happy with identifying the compensatory measures and saying that's it. But that is a broader issue. I don't want to get into it here.

MR. REED: You gave the example, it's a classic example. Any type of adverse action, you know, you got the fire guys there blocking security, or the security guards blocking the fire guys, whichever way, including egress or whatever, access into an area, my answer to that is, you fix it as fast

as you can, and in the interim you take compensatory actions to address the situation, recognizing what you can do. Because you could be in violation of Appendix R or what have you immediately. I mean there could be things right - and so we talk about taking compensatory actions right in the rule, and you have to comply with regulations. So what happens there is like what happens at the plant whenever you get something like this. It doesn't have to be security. It could be any adverse condition which is discovered. You basically go into that situation where you are in kind of a compensatory measure and get it fixed in an expedited manner. So I think that is what we're trying to do.

MEMBER APOSTOLAKIS: Well, one hopes that people would react that way. But you know -

MEMBER MAYNARD: I think it's an important aspect of why the change is needed. It could dictate some actions. First of all if it's a voluntary change, you just can't make the change until you can comply with both sets of requirements. However if you find yourself in a degraded situation, or a new requirement, something has happened that you have to change this, that's when you typically go to compensatory measures to provide additional levels of

safety or security until such time as you can make it a permanent change. So the reason for the change usually makes a big difference in what actions you take too.

MS. BANERJEE: And Maitri Banerjee here, I think I would expect the existing corrective action program that is employed at the plant will take care of these things if it happens.

MEMBER APOSTOLAKIS: I really would like this to be part of Regulatory Guide 11.74. But that's outside the scope.

CHAIR BONACA: That would be a revolution within the site. I mean sites typically have -

MEMBER APOSTOLAKIS: Look, you can put it in the same vague way. The security philosophy should be preserved.

MS. SCHNETZLER: Maitri has a good point, though, that I may not have fully thought through, that going forward, if a licensee fails in this area, they are probably going to have to document that in their corrective action program and take corrective actions and look for trends and other possibilities. So long term we do have a capability of reviewing those collective actions and looking for program deficiencies maybe.

MEMBER APOSTOLAKIS: But there is so much judgment involved in these things; it can go either way.

MR. REED: Absolutely.

MEMBER MAYNARD: Something else that is different today from what it was 15 years ago, you've always had requirements you can't make security changes that have a negative impact without certain reviews. You have it for 50.59. There's a number of these different requirements out there. And in the past plants have typically reviewed those individually.

Most of them now have gone to an integrated change process that they go through a check list whenever any change is made and identified for impact on any of those things, and a process for resolving it if it does.

MS. SCHNETZLER: Right. Nowadays a lot of times you will see a change package out of engineering, when they are going to do a design change that there are several checkoffs that have to come from several different departments. And that's one of the things that this will do is force licensees to review those types of documents that they already have and ensure that they have the right review on them.

MEMBER MAYNARD: The requirements have always been there.

MS. SCHNETZLER: Somewhat of a silo maybe.

MEMBER MAYNARD: This really nails it down, I think.

CHAIR BONACA: What kind of feedback did you get from the industry?

MS. SCHNETZLER: Actually we have one of the NEI representatives here if you'd like to hear from him. But it was very interactive, and very questioning. We went through the guide paragraph by paragraph, and there was a lot of interaction about, well, what does this mean? Initially we had a lot of information in here about what compensatory measures or things you might look at. And as we started working through it, and running potential different scenarios through it, we started backing out a little bit because of the complexity of how it could be touched by various areas, and we really didn't want to step on any other regulations or requirements. So that's why you see some of the higher level of this.

Any other questions?

MEMBER BLEY: We appreciate your presentation.

MS. SCHNETZLER: Thank you, sir.

MR. REED: Thank you.

CHAIR BONACA: I wonder if the gentleman from NEI would like to say something?

MR. EARLS: Thank you. I'm Chris Earls with Nuclear Energy Institute. Yes, I want to echo what Bonnie has said. The industry has worked closely with the staff on this. We are happy with where this Reg Guide has ended up. One of our big concerns was that we didn't end up having to generate some special process out there that is just for security. What we've been stressing in the meetings is, let's take advantage of these other processes that already exist at the sites, that work well, we have a long history. So let's focus more on integrating security into those processes. And we think that this document has gone in that direction. So we are very satisfied with it.

We are still concerned, once we get into the implementation phase, that that's actually how it rolls out, but that burden is really on us and the licensees really to do that. So we are fundamentally very happy with where this Reg Guide has ended up.

And frankly what I've been trying to relate this to, over the years we have integrated

other organizations. I was a chemistry manager at a site for a long time; chemistry and radiation protection for many years were outside the integrative work process, and we had to roll those organizations in. I see this as just the next step in that evolution. We are rolling in another organization, being security.

There are some unique aspects to it with regard to safeguards and that sort of thing, but fundamentally it's the same integration that we have done before so we know how to do it.

CHAIR BONACA: Thank you.

MR. EARLS: You're welcome.

MS. BANERJEE: Maitri Banerjee again. Can I ask a question to the staff, please?

CHAIR BONACA: Sure, go ahead.

MS. BANERJEE: I was wondering, you have specific questions here, screening questions. But how do you know that you covered everything?

CHAIR BONACA: Well, it says it was not all inclusive.

MS. SCHNETZLER: We were pretty careful to say these are examples.

CHAIR BONACA: If there are no further questions we thank you very much for the presentation.

MS. SCHNETZLER: Thank you, sir.

MR. REED: Thank you.

CHAIR BONACA: We are going to take time for lunch. We are going to come back at 1:45.

(Whereupon, the above-entitled matter went off the record at 11:18 a.m. and resumed at 12:44 p.m.)

CHAIR BONACA: Let's get back into session. The next item on the agenda is digital upgrade of the Oconee Reactor Protection System and engineered safety features. And the meeting is open and closed, I believe, to provide that information.

DIGITAL UPGRADE OF THE OCONEE REACTOR PROTECTION SYSTEM AND ENGINEERED SAFETY FEATURES

MEMBER BROWN: Okay. I guess we'll go ahead and start, is that acceptable?

CHAIR BONACA: Yes.

MEMBER BROWN: The purpose of this briefing today is to really provide an advanced heads up discussion and brief of what the first operating plant upgrade to digital INC system, what it will look like, what it encompasses and what it contains.

NRR is here to present that to us. I appreciate them being here, by the way. I understand normally they don't do most of this stuff until after

they've got all their information in. So I would like to emphasize, they don't necessarily have answers. They've got all the paper in. They have not completed their review. The SER is not done. It will be done later, and so if they say they don't know, we ought to move on, and get on to something else. I just wanted to get that in up front after my seven months experience now of watching how this process goes.

Part of this meeting will be closed. We will, when we get to some proprietary information, Pat Hiland will let us know, and we will then clear the room, whatever the process is. I presume Mario will help me on that so we can get that taken care of, right?

Anyway hopefully they will address at least the four - and I think they are, based on my advance look - the four major pillars that I look for in digital INC in terms of evaluating its goodness or badness, and that is redundancy, independence, deterministic nature, and defense in depth. And other stuff, there's other stuff that is important, but if you don't meet those metrics you really don't have anything. And that's kind of to give everybody what it looks like, and you can ask questions and develop your own thought processes obviously, and we'll go

from there.

Pat, I'll turn it over to you.

MR. HILAND: Okay, well, thank you, Mr. Brown.

We appreciate the opportunity to address the full ACRS committee. As Mr. Brown mentioned, most of the information that you hear today is what we've termed pre-decisional, is that our review of the Oconee application, we are about halfway to two-thirds of the way complete with that, and so the issues that are open we may or may not have answers today, and sometimes our answers may change as we go on.

Let me first introduce the staff that I brought. I'm the division of engineering director in the Office of NRR. With me today the principal spokesperson and the leader of this review is the branch chief of information control, to my left, Mr. Bill Kemper.

Also one of our INC engineers who will have a speaking role today is to Bill's left, Mr. Rich Stattel.

But I did bring some familiar faces in the bullpen just in case we get some hard questions.

(Off the record comments.)

MR. HILAND: In the back there of course

Mr. Steven Arndt, who is trying to regain his youth. If you noticed he removed his beard recently. And to Steven's left and our right is Mr. Paul Loeser. Paul has not been directly involved in this particular review over the past year. He has been working on a digital INC application for another facility. However he does act as our own personal consultant in house for some of the technical areas, and so we made sure to bring him.

And then to Paul's left and our right, the last person in our bullpen is the deputy director in my division, Mr. David Skeen.

Very quickly I will go over -

MEMBER BROWN: Did you introduce the Duke? I neglected to do that.

MR. HILAND: I was going to do that when I get through with the first page.

MEMBER BROWN: That's fine. I couldn't even follow my own rules.

MR. HILAND: Let me go through and what we are planning to do of course is to provide an introduction. You will hear the term, if you have not heard it in the past, is Teleperm. Teleperm is the microprocessor that the applicant has chosen to use in their digital INC amendment.

Mr. Bill Kemper will discuss the overview of the license amendment request, where we have been. This amendment request has been in house just over a year. The amendment request that we are working on came in January 31st of last year.

He will also discuss the diversity and defense in depth, that was a specific topic that the full committee asked us to address, and we are prepared to address where we are on that topic today.

Mr. Stattel then will discuss communications, communications of the microprocessors and the machinery, back and forth. And then we will discuss some of the changes that have taken to the Teleperm platform, since it was approved by the NRC back in 2000. It's kind of interesting in that we've had a platform approved almost 10 years ago, and this is the first fullscale application of it.

Now I'd like to introduce Mr. Rich Freudenberger. He is the safety assurance manager from Duke, and he has a few words to say.

MR. FREUDENBERGER: Thank you, Pat.

I'm here representing a small contingent from Duke and AREVA. We are here to support your discussions and I guess be the bullpen to the bullpen.

I am Rich Freudenberger, like he said. I

am the safety assurance manager at Oconee. I'm the licensing sponsor for this project.

We also have here Boyd Shingleton who is the lead licensing engineer. Then we have - Boyd, would you raise your hand back there and stand up for a second?

Then we have Mike Bailey. He's the engineering supervisor in our plant engineering group at the station, and he'll be the ultimate owner of the system, so he is heavily involved in design considerations, and making sure we get the product that we want into the plant.

Jacob Bryan is engineering supervisor in our Oconee major projects group, which is the projects implementing large modifications. He is responsible for the design, testing and installation of the system.

We also have from AREVA Sean Kelly. Sean is the chief engineer at the TXS detail design center in Alpharetta, Georgia, and heavily involved in this project.

This digital upgrade of our reactor protection system and engineering safeguard system - I'll call it RPS/ES from now on - is one of many digital upgrades that we have undertaken at Oconee to

address obsolescence and improve the reliability of our systems.

Other systems that have already been upgraded include condensate system polisher controls, our integrated control system, our turbine EHC system, our control rod drive systems, and the Keowee hydrostation has the governors for that, that's our emergency power generators for emergency power system, there are two units there. Their governors have been upgraded to a - using the same platform, the Teleperm XS system. All those modifications have been done under 50.59, and did not require prior NRC review.

The RPS/ES system of course will include use of the Teleperm XS digital protection system. The amendment request was submitted in January, 2008. Since then there has been frequent interactions with the NRC including weekly conference calls that address both SE issues and the logistics as the project progresses, as testing procedures become complete, and test schedules get planned. There have been a lot of logistics to ensure that appropriate activities get reviewed by the NRC as they are ongoing.

There have been three audits that have been performed, the one in May, 2008 at Oconee, one in September, 2008 at the AREVA Alpharetta offices; and

in November/December of 2008 there were audits and observations of the factory acceptance testing in Erlangen, Germany, at the test facility there.

Through all those interactions we have been able to develop a strong collaborative effort and a good relationship to be able to work through the many issues that are involved with this first-of-a-kind application.

We expect the second set of RAIs, requests for additional information, within the next month. And we expect approval and a documented in a final safety evaluation in the fall of 2009.

Following that we have recently made a decision to push installation on our first unit to unit #1 in the spring of 2011; then unit #3 will follow a year later in the spring of 2012; and unit #2 will be in the fall of 2013.

The reason for that push was application of some operating experience from our other systems that we've installed, and right now we have a high focus on making sure we have a good design, got that design complete, when the design is stabilized we need to have an additional high focus on translating that design into implementation documents, and have a strong plan to be able to install the system without

any errors, to get it into the plant and don't have any latent errors that we put into the plant as we install that system. So that is the primary reason for that additional delay.

That's what I have as prepared remarks. Are there any questions?

MR. SIEBER: A quick one only to kind of orient myself. I know that Teleperm systems have been backfit into European plants. I'm really familiar with the Beznau nuclear plant, so that's a Westinghouse design. It's had a fault in protection and safeguards. How similar is the Oconee platform to for example what was installed at Beznau? Is it basically the same, or are we talking about something that is evolutionary? Because Beznau was installed I think in `99.

MR. FREUDENBERGER: I am not familiar with Beznau, but perhaps Mike or -

MR. BAILEY: Again, my name is Mike Bailey from Oconee Nuclear Station. At Beznau, we actually did - there was a users group meeting a couple of years ago, and we actually went out there and benchmarked against what Beznau had. And our design functionally may not be set up exactly the same with all the exact same functions, but hardwarewise,

equipmentwise, we are on the same general generation and platform of equipment that they actually utilized.

MR. SIEBER: Thanks.

MEMBER APOSTOLAKIS: Let me understand this. This is now operational at Beznau?

MR. SIEBER: Yes, and it's been operating for about six years, I think. Don't hold me to the exact dates, but it was `99, 2000.

MEMBER APOSTOLAKIS: The Swiss authorities then approved it?

MR. SIEBER: Yes.

MEMBER APOSTOLAKIS: There is a six-year experience?

MR. SIEBER: Yes.

MEMBER APOSTOLAKIS: Have we taken advantage of any of this?

MR. FREUDENBERGER: Yes, that was part of the basis for our selection of - when you look at why we chose Teleperm over other systems that may have been out there when we entered into this project, we did the benchmarking as part of the input to make the selection, and it also fit in as well because of the long-standing relationship we had with AREVA.

MEMBER APOSTOLAKIS: Are you gentlemen aware of what the Swiss did and what they found, their

experience?

MR. KEMPER: No, we have not communicated directly with that organization. The Teleperm as you know is a previously approved platform. We have already reviewed that, so we are very familiar with its technology. So whether this review is really approving the implementation of that technology in a specific license application.

MEMBER APOSTOLAKIS: But it seems to me that learning from the Swiss what the experience has been would be useful. Is there a mechanism for doing that? Do we have an agreement with them, some way that would be easy to do this?

MR. HILAND: I think if you know - I'm sure you are familiar, sir, with the work of the Digital I&C Steering Committee, and the operating experience efforts that we have underway in our research, the Office of Research. I can't answer specifically the Sweden and this facility in its application. But we do have efforts underway to try and reach out and identify operating experience for digital I&C systems. I just can't answer the question regarding specific -

MEMBER APOSTOLAKIS: So you have become aware through the Office of Research?

MR. HILAND: Yes.

MR. KEMPER: That is correct. And there's a project ongoing right now to do that.

MR. ARNDT: Historically, both in previous research work - Steven Arndt - as well as in our interactions internationally both with the database, failure database work sponsored by the international organizations, as well as some of our collaborative work, we are aware of a number of the different installations such as the one in Temelin and some of the German applications as well. I'm not sure that we have actually specifically talked to the Beznau folks.

But the real issue is as Bill mentioned earlier is that we are quite familiar with the hardware. This is a different application of the hardware, so the real issues are understanding the particular application.

MEMBER APOSTOLAKIS: That was not the spirit of my question, but I understand.

MEMBER STETKAR: From the time the staff approved the original platform and installation and philosophy behind this until this goes into service is going to be about 13 years. I understand the concepts have carried through through that period of time, but have there been changes in hardware like CPUs and so

forth that have occurred?

MR. KEMPER: Absolutely, and we intend to cover that, as a matter of fact. That is part of our agenda.

MEMBER STETKAR: To me that is sort of important. I can't picture 13-year-old equipment sitting on the shelf and waiting for a buyer, and having it suitable for a modern installation.

MR. KEMPER: You are absolutely right. Good question.

MEMBER STETKAR: And a comment, I think the Swiss gave a very brief presentation at the meeting.

MR. FREUDENBERGER: Thank you.

MR. HILAND: Thank you.

The license amendment request from Duke when it came in a little over a year ago, we hadn't quite had in place what we term today our acceptance review procedure. However - and I think we sent the packages of information out, what we did and what Bill will cover as far as how we got into the review, is we sent our acceptance letter, but there were six topics that we felt were critical to even start the effort, and so those six topics were the subject of our first audit.

What we also did, and what you have sent over in your packages are trip reports for the audits that we did, which are public information. And what is important about that is that we had our I&C staff go out and make some decisions and some conclusions, and document them, so that the licensee or the applicant in this case had that information up front so that they could make plans as far as when to implement the changes.

That doesn't mean, as I said, this is still pre-decisional. I might change my mind. If I change my mind, they have this piece of paper they can come and discuss with us what were the details that caused it.

With that I'd like to turn it over to Mr. Kemper and let him talk a little bit about the background.

MR. KEMPER: Thank you, Pat.

Well, again, my name is Bill Kemper, and good afternoon. It's a pleasure to be here. We've already covered some of this, but I'll just go through it so that we all understand the dates that are important.

In January 2008 Oconee submitted a license amendment request to replace the existing analog

reactor protection systems and engineering safety feature systems with a digital system which is based on the approved Teleperm XS system.

And as we said a moment ago, we will commonly refer to this as a TXS platform. So if you will that is probably the way we will describe it during this presentation.

The Teleperm was approved in May of 2000 as part of the NRR acceptance route process the staff accepted the LAR in April of last year for review, and documented six issues that could present significant - or not significant, but could present challenges to approving the LAR.

And I have them listed here, diversity and defense in depth; bi-directional communications; the AREVA software program manual, the use of that in the LAR; TXS platform changes that have occurred since it was approved, both hardware and software and programmatic; verification and validation program and practices that the Oconee application claimed; and also the use of software tools for V&V.

Now we intend to talk about items one and two and four in detail in these presentation; there is not enough time to talk about all these things, and we weren't asked to either. But we can certainly answer

questions in these areas if you have them.

Duke has since provided 11 licensing amendment supplements to their LAR, and responded to all the RAI questions. At this point there are 113 of them. And as Rich said there is another round that is likely to occur here in the next month or so.

The NRC as Pat said is roughly about halfway or two-thirds of the way through our review. And we have conducted three audits, as Rich Freudenberger said, and the results of those audits are publicly available with the exception of the factory acceptance one. We are about to publish that during the next couple of weeks. Next slide, please.

Now with regard to the review process, the staff is conducting the review in accordance with the Standard Review Plan, Chapter 7 of NUREG-0800, LIC-101, and also several interim staff guidance documents that are applicable to digital safety systems.

The Interim Staff Guidance documents that we are using have been reviewed by the ACRS previously. So it's my understanding that you are familiar with these criteria.

These documents clarify the licensing criteria for digital safety systems, and compliance with the ISGs is what we term the fast track or the

HOV lane for licensees to receive regulatory approval for their submittals.

Specifically the staff used ISF #1 for review of the cyber security aspects of the application; #2 is being used for the diversity and defense-in-depth review; and #4 is a primary tool for reviewing the communication aspects of this application. Next slide, please.

Now I'd like to provide an overview here. They say a picture is worth a thousand words. I'll try to get this done in less than a thousand words if I can. And Rich will use his little pointer there, his mouse, to try to point out some of the things that I'm going to describe here.

This figure shows you a 20 reactor protection system, and engineered safety feature systems architecture. The digital system consists of a four channel reactor protection system with a two out of four coincidence trip logic, integrated with a dual three channel RPS system that provides a two out of three coincidence trip logic.

The system is redundant, and the three division one channels in the blue boxes, coexist with channels A, B and C of the reactor protection system.

The integration of RPS and ESPS as Duke

calls their ESFAS system, combine two of the four echelons of the fence and layers described in NUREG-6303 for protection against software common cause failures. And we will discuss that later in more detail in the presentation.

Both of the ESPS divisions share the same sensor inputs. This is illustrated by the blue and the orange and the green lines there. And the two out of three voting logic for each ESPS division is performed by the TXS voter modules themselves down at the bottom of the slide.

These are redundant computers that receive inputs from the channel signal processes as shown here.

The two out of four voting logic for the RPS system is implemented via hardwired relay logic similar to how the analog system is currently designed. And that is just for simplicity illustrated by this yellow block.

MEMBER BROWN: Does that mean the ESPS is software voting logic and the RPS is hardware voting logic?

MR. STATTEL: That is correct. That is correct. That is a major difference between the two systems.

MEMBER BROWN: But both sets do it the same way, of the ESPS, both sets?

MR. STATTEL: That is correct, and that's what's shown here.

MEMBER BROWN: I just wanted to make sure if I understood the boxes right.

Hold it. What they've done is for the ES - for the emergency safeguard system - well, I'll let you explain it. I know what they've done. What do you want to know, the difference in hardware logic and software?

MEMBER APOSTOLAKIS: The difference in the logic.

MR. KEMPER: Well, the voting logic, it's an electronic - they're computers, and they are electronic. They take inputs, and in fact I was going to go through that. Let me if you will, let me finish my spiel here, and hopefully I can answer your question.

The thick green lines represent communications pathways for communications between the individual channels as well as communications between the channels and the voter modules themselves. Each of the ESPS voters must receive channel trip status information from the signal processors in order to

perform the two out of three actuation functions. The channel to voter communication pathways facilitate the transfer of that information. That is the thick green lines there.

The interchannel communications enable fault tolerance features to be included with the signal processing logic. For analog signals, a second min second max function is used to accomplish this, and we'll talk more about that later in the presentation, exactly what that means.

So for example an ES channel receives a sensor value status from its own channel and also from the other two channels. It compares those, and the voting logic and the voter, and if it meets the two out of three trip signal, it sends a signal down through those diodes and actuates the equipment.

MR. STATTEL: So basically the bistable feature occurs in the sensor channel so the trip status gets fed to the voter. The voter receives that trip status from all three channels.

MEMBER BROWN: But that voter is software?

MR. STATTEL: It is software based.

MR. KEMPER: It is a configured that is driven by software, that is correct.

MEMBER BLEY: And that means a program is directing these into registers that do some kind of calculations, is that what it means?

MR. STATTEL: Yes, that is correct.

Now one thing I'll point out here, there are two sets of voters. There's odd and even voters shown here. And there's - well, it's basically just a redundancy.

MR. KEMPER: Yes, it's important to note that actuation of either voter, odd or even, will execute the safety function.

MEMBER APOSTOLAKIS: But odd and even is just a name?

MR. KEMPER: It's just a name. It could be A or B, it could be green or yellow, whatever you choose.

MR. STATTEL: Also the blue voters on the right side of the diagram here, those are the ESFAS voters, not the reactor protection voters, right? Remember the ESFAS division one coexists with the reactor protection.

MEMBER BROWN: Let me - if you look at the diagram you will see a little green arrow in the middle of those three - look at the channel one RPS/ES, see that little bitty green arrow coming down,

that goes to the reactor trip vote breakers. The long green line goes through that; it doesn't connect to it; and goes to the blue voters.

MR. KEMPER: So all four of the voter boxes that you see at this level of the diagram are for the ESFAS functions.

MEMBER APOSTOLAKIS: ESFAS is safety -

MR. KEMPER: Engineered safety features safety actuation system. Duke calls theirs engineered safeguard protection system, ESPS.

MEMBER APOSTOLAKIS: They are four votes?

MR. KEMPER: That's correct, two redundant sets of voters, that's right. And it's important to realize that either set, either the orange set or the blue set, they are completely redundant channels. The only thing they have in common is the input sensors.

MEMBER BROWN: Let me make one other observation, if you didn't pick this up. The reactor protection channels, three of them actually perform - they are mixed. In other words the safeguards functions, all that software is mixed between the two, so it's all performed in one channel. It's not an independent - let me put it this way, ES channel, the little blue boxes are not independent of the RPS

system. It's all in the same platform.

MR. KEMPER: They are integrated; they are not segregated protection systems. Which is what the analog plants typically are now.

MEMBER BROWN: Now the other difference now is there is a second set of ESFAS stuff which is independent, at least based on the diagram, from the reactor protection system, and the other safeguard system.

MR. SIEBER: But that uses the same software?

MEMBER BROWN: Yes, it uses the same software. But a different set of platforms to process it, is that correct? Did I say that correctly?

MR. KEMPER: Right. You said the same.

MEMBER BROWN: Yes, it's the same program, same lines of code.

MEMBER APOSTOLAKIS: And what happens after you have the - you have the four voters, now. You say - what logic do you have there? When do these things start working?

MR. KEMPER: Okay, so once - so let's take the orange channels, the three on the left there. Once you receive a trip signal from two out of three of those, and they're fed to both voters, odd and

even, at the same time, then the voters will make a decision. It's completed the requirements for executing the safety function.

Then it will send a signal through these diode representations that we have down here to these two arrows going down really are what they call odd and even actuation, like division A, division B, okay, actuations, systems. So either one of those divisions being actuated will execute the design basis safety function of the plant.

MEMBER BROWN: You've got open a valve, shut a valve.

MR. KEMPER: Open a valve, start a pump.

MEMBER BLEY: You say odd and even. Did you say - both one voter from the orange, one voter from the blue, feed the even, and same for the odds.

MEMBER APOSTOLAKIS: Evens go together, odds go together.

MEMBER BLEY: Now do both - do either one of them execute all safeguards functions?

MR. SIEBER: Be careful - what he wants to ask I think is if I have two pumps in the plant does even start both pumps?

MEMBER BROWN: Yes, if you've got two trains, does any one of them start all trains.

MR. SIEBER: Think of the even and the odd as division A and division B. So if I had two pumps in the plant -

MR. KEMPER: So division A would be the A high pressure injection pump; division B would be the bravo high pressure injection pump. The design of the plant is such that alls I need is one train to operate, to safely combat all the design-

MR. SIEBER: Got you.

MR. KEMPER: So the way this is lined up is you have two redundant channels feeding into an even voter - excuse me, an even set of actuation devices, and two redundant channels feeding into an odd actuation.

MEMBER APOSTOLAKIS: What is the logic down there?

MR. STATTEL: At the diodes it's basically an OR function. The diodes basically perform an OR function. I guess either/or.

MEMBER BROWN: Either one.

MR. KEMPER: And just to quickly show you the difference, to answer your question, your package, if you look at page 25, I won't try to go through this in detail, but this shows the hardware logic implementation of the reactor protection system. This

is how the actual coincidence actuation is approved.

MR. STATTEL: But that's the more traditional approach.

MR. KEMPER: That's more traditional. That is very similar to the analog, except instead of using analog solid state devices for bistable switches and so forth we are using a computer algorithm.

MEMBER BROWN: Then it's not analog. If it's a computer algorithm, it's not analog.

MR. STATTEL: There is no computer algorithm involved with the reactor protection system.

MEMBER BROWN: That's what he just said down in the voting section.

MR. KEMPER: If you look at the drawing, the box on page 25, the box at the top of each channel is the TXS processor. Okay that is where the inputs are compared to a set point, and trip signal is developed. Then that is fed into each of the four channels.

MEMBER BROWN: So BA, BB - take the yellow one, BA, BB, BC, BD.

MR. KEMPER: That is correct. And eventually you will meet two out of four. That is all it takes.

MEMBER BROWN: But those are the trip

signals there?

MR. KEMPER: Say again?

MEMBER BROWN: The BA, BB, BC and BD are just the trip signal coming in.

MR. KEMPER: Those are relays.

MEMBER BROWN: Are they relays?

MR. KEMPER: They are relays that actuate -

MEMBER BROWN: Solid state relays or electromechanical?

MR. KEMPER: They are electromechanical relays.

MEMBER BROWN: Conventional electromechanical relays.

MR. KEMPER: They are the original supply equipment of -

MEMBER BROWN: I'm not saying it's wrong. I wasn't trying to send a message there.

MR. KEMPER: This is how the system works now.

MEMBER BROWN: Okay, so it's not a computer algorithm?

MR. STATTEL: Not for the voter.

MEMBER BROWN: Not for the voter.

MR. KEMPER: Only for comparing the

signals and computing the trip logic itself.

Okay, so let me move on to the next slide if I may.

MEMBER APOSTOLAKIS: Can I - let's pick the blue box there, the first one. What inputs does it receive? The RPS -

MR. KEMPER: The voter or the channel? Okay, ES channel A. Now again -

MEMBER APOSTOLAKIS: It says RPS input channel A. I'm looking at the blue box #1. RPS input channel #8, right? And it also receives what?

MR. KEMPER: Okay, that channel receives RPS input signals.

MEMBER APOSTOLAKIS: One signal?

MR. KEMPER: That's right. And it also receives input signals for the engineered safeguards function of the algorithm. So those dual channels, those combined channels, can create a reactor protection trip signal as well as an engineered safety features actuation trip signal simultaneously.

MR. LOESER: I think you may have misspoken. Blue number 1 does not just get one sensor signal; it gets the channel A, all of the channel A sensor signals in and processes all of them, that particular box, both for EFS and for RPS.

MR. KEMPER: Yes, we are actually getting ahead of ourself. We intend to cover all this in Rich's presentation.

MEMBER APOSTOLAKIS: I'm trying to understand what kind of redundancy we have, and why. Why do you have four blue boxes?

MR. KEMPER: Well, four blue boxes are there to satisfy our IEEI 603 requirements for redundancy. That is typical in the industry. You typically always several redundant channels to accommodate simple failure as well as coincidence logic for various trip avoidance.

And so they've maintained the same basic design philosophy with their computer based system. So for RPS and B&W plants they have four channels. For ESFAS they have three channels, which is different than a Westinghouse plant or others, many other plants have got four ESFAS channels.

MEMBER APOSTOLAKIS: This redundancy protects me against what kind of failure? Who might fail?

MR. KEMPER: The redundancy primarily protects you against failure of any one channel, a single failure is what it boils down to. In other words the system has to be designed to be able to

execute its safety function with any one single active failure. And so that is what redundancy primarily does for you.

MEMBER APOSTOLAKIS: Where?

MR. KEMPER: Within one of those blue boxes, they could be any number -

(Simultaneous speakers.)

MR. KEMPER: It could be a communication process.

MEMBER BROWN: There is - I don't know having seen what the inputs are, but typically in the old plant, the older plants, if you had four pressure channels you'd have channel A go to channel A; a second pressure detector go to B; a third pressure detector to C; and a fourth pressure detector to D. If you had four power range neutron detectors, one would go to A, one would go to B.

MEMBER APOSTOLAKIS: But you don't have the green lines.

MR. KEMPER: Now, the green lines, they serve a much different function. I'm going to get to that in just a second. We don't want to do that yet, okay, because we will spend all our time talking about communications, and we're not there yet. Can you hold off for a few minutes, please?

MEMBER APOSTOLAKIS: Yes, sure.

MR. SIEBER: You're not going to get to this, and this could be a simple question. On the outputs of the voters you have, let me call it a lead voter and a comparator voter, and each of those send signals - it is more detailed than is here.

MR. KEMPER: It is.

MR. SIEBER: It sends signals to two series relays, and you've got to pick up both relays for coincidence. Are those two series relays on the output of the ESFAS part of the current Oconee design, or were they added as part of the TXS mod? In other words if you go to the current plan does ESFAS channel A only pick up a single master relay to start HPI pump A, let's say, whereas here both of those voters need to pick up two series relays to start that pump? Are those two series relays added as part of this mod?

MR. KEMPER: If I understand your question I believe those are added as a function of this mod. And the current analog system, two out of three channels have to trip to execute all of the actuation relays. So in other words one channel doesn't actuate part of the relays, and the other channel operate another part of it. Once you meet the trip success criteria for two out of three channels,

then all of the slave actuation relays if you will -

MR. SIEBER: But there is only a single slave relay for - if I'm HPI pump A, I only have a single slave relay, where in effect here I have two slave relays in series; I need to pick up both of those.

MR. KEMPER: Well, I'm not sure I'm following you 100 percent, but the voters have redundancy within them. And the voters compare their output, each one of them, each box of those, compares its output and ensures that it's consistent, and then it will execute a trip function and send it on.

MR. SIEBER: What I'm talking about actually shows up on your slide 9, but you are going to use slide 9 to talk about diversity. That's why I wanted to bring it up now because it is more of a function of how the basic system works rather than diversity. See the relays down below. That is the redundancy that you are talking about, the voters.

MR. KEMPER: That's correct.

MR. SIEBER: And what I was curious about were the, what you are showing is the contacts of the two relays down there. Was the second, essentially was the second series relay added as part of this mod, or was that already existing? And what I hear you

saying is that the second relay was added as a way to confirm that both of those redundancies within the voting logic indeed were giving positive output signals.

MR. KEMPER: Mike, you want to -

MR. BAILEY: I'll be glad to. Mike Bailey again from Oconee. We actually did add as part of this project add some additional relaying such that you actually have some redundancy in the relaying which we do not currently have in the currently existing ES system design. You have relays for the - just a single relay for the odd channel and a single relay for the even channel. Now we actually have a dual set of relays from each set of voters.

MR. SIEBER: But those are series relays, so you have to pick up both of them now.

MR. BAILEY: That is correct.

MEMBER BROWN: That's really -

MR. SIEBER: You've doubled the unavailability of the start signal.

MEMBER BROWN: Well, John in other words look at it. I'm not saying this is right or wrong. If you have a failure of a relay you won't inadvertently start anything either.

MEMBER BROWN: That's right. This -

well, part of my observation was, there are a lot of features of this new system that are indeed designed to prevent spurious actuation. This is one of them.

MR. SIEBER: That's what it looks like.

MEMBER BROWN: Preventing spurious actuation many times reduces the reliability of a valid actuation which this does.

MR. SIEBER: Yes, but you can also argue -

MEMBER BROWN: I just wanted to find out whether those two relays were part of the existing design or whether they were new. If they are part of the existing design you haven't really changed anything from what was there.

MR. KEMPER: It sounds like they were added.

MEMBER BROWN: John, by having a second set, you can - I'm not sure because I haven't gone through it in that much detail yet, you could argue that the point you just made, you have asked for an additional thing to have to happen to initiate it, but it protects you from an unreliable, spurious -

MR. SIEBER: That's right.

MEMBER BROWN: The second set is there

also, and it's in parallel, it will still also provide that -

MR. SIEBER: But that always was, that was always train B, for example. We always had train A and train B.

MEMBER BROWN: Well, that is true. But in this case, train - no, let's go on. Go on.

MR. KEMPER: All right, moving right along here. The next slide here - as I say I don't mean to rush you. We will certainly answer your questions. But in order to explain the system -

MEMBER BROWN: Yes, we are on slide 5, we only have 20 to go, so we need to move along.

MR. KEMPER: We're on slide six now. So this next slide provides - shows the communications links and the pathways supported by the Oconee design for safety to nonsafety communications. The box labeled MSI, the big blue box, is the central communications link for the system. MSI stands for monitoring and service interface.

The MSI provides the communications interface to all the signal processing computers, and it provides the communications pathway to the nonsafety service unit and external systems via the gateway and operator aid. Up here, those are the

devices to the right here as you see.

It's important to note that communications between the safety related channels do not come through this path. That's what we showed in the previous diagram; they go directly point to point to each channel.

MEMBER BROWN: This is all output?

MR. KEMPER: Say again.

MEMBER BROWN: These yellow lines, whatever they are, those are all just taking information and sending them out some place else?

MR. KEMPER: Two directions, actually. So the idea is, you have two directions for communications. You see the device that is called a service unit down on the right hand, lower right hand side. That is a computer that we'll cover in more detail here during Rich's presentation. And it has the ability to send signals acquiring information from the safety-related channels and the - if it's the right information to the right question, it will also send information back to the service unit.

Now the net optics port tap device, which is the dark blue box there, provides a bidirectional communication path to the service unit, and a one way communication path to the operator aide communication

computer through the TXS gateway. A gateway is also a TXS computer.

The service unit is located within the protected area, and it is used by operators to perform system maintenance and surveillance functions such as bypassing a channel for maintenance testing.

The RPS just to explain everything that is on here, the RPS channel E functions are nonsafety related. It performs a system alarm and annunciation functions, and provides an interface to the plant integrated control system.

Even though the MSI is shown as a single - in this figure as a single component, it actually consists of redundant computers so it's not a single point of failure as you might think it would be from this drawing.

And also there is a little Ethernet switch there that provides - which is provided to keep the net optics communications active if the service unit is offline or disconnected. Next slide.

MEMBER BROWN: Not quite. You've got black lines outlining some of the yellow lines, and some of them don't have black lines. Is that supposed to mean something?

MR. STATTEL: No, those are just - that's

just the way it's showing up on the slide.

MR. KEMPER: The thing to get from this slide is out on the right side it is nonsafety, on the left side of the big blue, MSI, it's all safety.

MEMBER BROWN: Yes, but it's all bidirectional.

MR. KEMPER: Some of it is bidirectional; some of it is one directional.

MEMBER BROWN: I got that.

MR. KEMPER: We'll talk about that in detail when Rich talks and you get his pitch.

Okay, this next slide I'd like to get into diversity and defense in depth aspects of the application. We will start by reviewing the current requirements for diversity and defense in depth for digital systems.

There are three primary documents that define these requirements, which are based on the guidance provided by the SRM for SECY-93-087. NUREG-6303 describes a method for analyzing a common cause failure of a computer-based nuclear safety system, and it's potential effects on the overall plant safety analysis.

This analysis is intended to identify coping strategies for plant design vulnerabilities

such as software common cause failures of the RPS and ESFAS system primarily.

This NUREG also identifies four echelons of defense for diversity and defense in depth, which is the control system, reactor trip system, engineered safety features actuation system, and the monitoring and indication systems that the operators would use to take manual action.

MEMBER APOSTOLAKIS: This is from 1994, right?

MR. KEMPER: That's correct. I think it's `93 actually when that NUREG came out. I believe so.

BTP 7-19 provides guidance for evaluating an applicant's D3 assessment, using if you don't mind I'll use D3 instead of diversity and defense in depth - it's a common term that we use here - and also for evaluating the design of automatic and manual controls and displays for use as a diverse actuation system, or DAS as we call it.

ISG-02 provides acceptable methods for implementing diversity and defense in depth in digital I&C systems, and the ISG also clarifies the criteria staff would use to evaluate whether the system is consistent with our guidelines.

It also provides guidance for what constitutes acceptable manual operator actions that can be credited to cope with common cause failures. And again the ACRS has seen this ISG in the past. And specifically the ISG prescribes a 30 minute criteria for manual operator actions as follows.

Manual operator actions may be credited for responding to events in which the protective system subject to a common cause failure is not required for at least 30 minutes, and the plant response is bounded by BTP 7-19, recommended acceptance criteria. Next slide please.

So the Oconee diversity solution is consistent with BTP 7-19. The new Oconee digital protection system replaces the four original actuation functions which are listed on this slide: reactor building cooling and isolation; reactor building spray; high pressure safety injection actuation; and low pressure safety injection actuation system. This makes up the ECCS system for Oconee.

The new system design also includes an automatic diverse actuation system for both the high pressure and the low pressure diverse actuation systems, excuse me, diverse safety injection functions.

VICE CHAIR ABDEL-KHALIK: Where is aux feed in this list?

MR. KEMPER: Pardon me?

VICE CHAIR ABDEL-KHALIK: Aux feed water?

MR. KEMPER: Aux feed water? Not part of this, not for a B&W plant. It has its own emergency auxiliary feedwater system, actuation system.

The diverse - I want to note though the diverse actuation for reactor building cooling and isolation, and reactor building spray, are still manual actuations that are not required for at least 30 minutes.

MEMBER APOSTOLAKIS: So when it says, Oconee's new automatic diverse actuation systems, this high pressure injection pass did not exist before?

MR. KEMPER: That is correct. This is a brand new system, and I'm going to explain it in some detail here in just a minute, that Oconee has invoked, because they did their D3 analysis as I just said for 6303, and they determined that in order to cope with all of their design basis accidents and still maintain their acceptance criteria under BTP 7-19 guidelines, it was necessary to actually have automatic diverse actuation systems because there wasn't sufficient time for manual actions is what it

boils down to.

MEMBER APOSTOLAKIS: Okay.

MR. KEMPER: Now the digital reactor protection system also has a DAS. However that is implemented in the existing Oconee ATWS system, the anticipated transient without scram system, which provides a trip function to initiate a scram that is diverse from the existing reactor protection system, and Oconee has maintained that diversity with the existing ATWS system and our new safety system. So it serves the role as their DAS for RPS. Next slide.

MEMBER BROWN: Go back to that, I just want to inquire on part of it. The ATWS, that is not changing?

MR. KEMPER: That's correct; it's not changing.

MEMBER BROWN: So it stays and it's a current analog pristine whatever it is?

MR. KEMPER: That's right.

All right this next slide shows - gives a little graphical representation of the diverse actuation system. This figure illustrates how the low pressure DAS interfaces with the safety system. This is typical of the high pressure DAS as well. They are very similar. In fact they are identical except for

the set points.

The low pressure DAS uses conventional analog bistable trip units, and a two out of three logic actuated on low reactor coolant system pressure. As you can see the two out of there voting logic is accomplished via hardware relay logic.

The diverse actuation system shares reactor coolant system pressure sensory inputs with the safety system that is shown here. This is okay, because the sensors are isolated and are not digital devices; and therefore, they are not subject to common cause failures.

The proposed system will be a combination of safety and nonsafety related equipment. The bistable devices, the two out of three logic relays, and the annunciator circuits will be supplied as nonsafety equipment; and wired for the Oconee Nuclear Station design requirements for separation and isolation.

The power to the DAS bistables and relay logic will also be nonsafety related. The interface components, the diodes depicted here between the safety related ESPS and the DAS actuation circuits will be safety related. That's required in order to meet 603 criteria.

MEMBER BROWN: Where is the boundary for your safety and nonsafety, can you show it?

MR. KEMPER: Right there. See where the arrow is right there? That is the boundary.

MEMBER BROWN: Upstream or downstream of the dot?

MR. STATTEL: The diodes themselves are safety related. So everything upstream on the right side of that would be nonsafety related.

MR. KEMPER: Right, and it has a proper isolation as I said per Oconee's design standards to meet 603 requirements.

The diodes shown here will provide an OR function between the DAS and the ESPS actuation systems. And this configuration, the failure of either system cannot prevent the actuation of the other system; that is very important here for a diverse actuation system.

ES components are configured, by the way, to energize to actuate, and also the DAS system will be configured the same way.

Also the diodes for the manual actuation function, there are no reliance on computer, and software based components. So there are three ways to actuate the ESPS system. One is through the primary

automated system. Second is through the automated diverse actuation system, which is nonsafety. And the third is through the diverse manual initiated system.

VICE CHAIR ABDEL-KHALIK: Just for my own information, I guess the aux feedwater system is not a part of the engineered safety features at B&W plants. Is there anything being done as far as the control system for aux feedwater at this time?

MR. KEMPER: Not in this license amendment. I don't know, maybe Oconee, have y'all got any insights on that?

MR. BAILEY: Mike Baily again. On our emergency feedwater system we've got a separate safety related control system that is analog that we actually utilize to actuate emergency feedwater. And we have no plans at this point in time to do anything with it from an upgrade standpoint.

MEMBER BROWN: Where is the manual actuation?

MR. KEMPER: On the left side. This right here is the manual activation.

MEMBER BROWN: Okay, there are two blue boxes.

MR. HILAND: Yes, there's two of them there, right.

MR. KEMPER: Yes, there's one here, and there's one here.

MEMBER BROWN: They say channel three and four.

MR. KEMPER: And you can see how those tie in downstream of the voters. So there is no software involved with the manual trip, which is a very good design.

I'd like to also point out that on the right-hand side there is an orange block there which is the emergency override feature for the DAS. The Oconee design does implement switches that they can bypass or disable the DAS anytime they desire, and there is no preconditional requirements such as tech specs that control that that I'm aware of.

Yes.

MR. SIEBER: A couple of questions. You said that high pressure and low pressure are identical. But I notice that the high pressure doesn't have the - at least the pictures that I have and the text that I have didn't mention the override for high pressure. Is that simply an oversight in the document? Does high pressure also include the override on the DAS?

MR. KEMPER: Yes, both DAS systems have

override. It might just be a clarity issue on the drawing.

MR. SIEBER: Yes, I'll tell you, the drawing does not show it for high pressure. And the text and the discussion, at least in the two documents I read, doesn't mention it. It mentions it explicitly for low pressure, so I was curious about why low pressure had it, and whether that was a conscious decision. Thanks. I want to talk about overrides later.

MR. KEMPER: Okay, well, as I said, there are no administrative requirements such as tech specs for that. So the staff will be reviewing the administrative procedure controls that govern the operations of these switches.

MR. SIEBER: Is it better to talk about - I want to talk about it not so much in terms of the DAS but in terms of the main system. Because the main system has an odd and an - an override.

MR. KEMPER: Oh, yes, well, they have bypasses. Those are operating bypasses.

MR. SIEBER: Not a bypass; an override. It's different from a bypass.

MR. KEMPER: The safety system? The primary safety system?

MR. SIEBER: That's what I read.

MR. KEMPER: The safety system bypass operation, my understanding, correct me if I'm wrong, please, it has the same basic design philosophy as the current system. In other words you can bypass the systems once the primary system is put into a configuration that enables that bypass to occur.

MR. SIEBER: That's different, and we might as well bring it up because I opened it up now. I read through this two or three times to try to understand how it works. And the bypasses and the resets, the things that are called bypass and reset, in the text and in the drawings, seem to be functionally the same as what is in the current analog system.

However in the system descriptions there is something called an ESFAS emergency override push button that is something different. There is one for the odd side of the plant, and there is one for the even side of the plant, as part of ESFAS. And as far as I read this, I can read the text here, but it says, new ESFAS emergency override features ensures that the operator is capable of taking control of all ESFAS actuation devices should there be inadvertent ESFAS actuation. Two new emergency override push buttons -

MR. KEMPER: That's a good pickup.

MR. SIEBER: I have a couple of questions. If that is a feature, can the operator push that one push button and effectively disable half of safeguards actuation at any time? Regardless of whether - the bypasses as I understand it you can only enable the bypass after an actuation has already occurred. They are not enabled until you have an active signal, so therefore the operator can't prevent anything from happening.

I didn't read anything like that with these overrides, that it sounded like if I'm an operator and I want to prevent safeguards actuation from occurring at all, I can run up and push two push buttons and nothing will happen. Is that true?

MR. KEMPER: My understanding is, that is not the case. Sean, you want to expound on that.

MR. KELLY: Yes, this is Sean Kelly with AREVA. Both the odd side and the even side have an emergency override, and that is to be used in case of a failure within the TXS system where the output boards fail energized. So in order to return the control of the plant back to the operator, they can push the button and cut power to those output boards.

MEMBER BLEY: But they could push them -

MR. SIEBER: Let's say the plant is operating normally, and something - I see something that doesn't look just right. And I'm the operator, and I interpret that as a malfunction, and I want to make sure that I don't get a spurious operation. Can I actually go up to the board, push both of those buttons, and safeguards is now automatically locked out because all of the output relays are deenergized. Can I do that?

MR. KELLY: Yes. You get - but when you push the button you get stat alarms and annunciators in the control room.

MR. SIEBER: Fine, but I knew I wanted to do that. I know that I'm going to get the alarms, because I actively decided that I wanted to disable all safeguards. Thanks. The important thing to me was, I wanted to understand that I could do it at any time, that I didn't need a preexisting actuation before I could do it. Thanks.

MR. KEMPER: Okay, thank you. Next slide. Manual operator actions.

The Oconee system does depend on some manual actuations as I stated a moment ago. The incorporation of the automatic DAS with the new Oconee digital protection system will provide a plant

response that does not require any manual actions for at least 30 minutes for all Chapter 15 accidents, with the single exception of a manual reactor trip during a small-break LOCA accident. This action is required within two minutes of the worst case small-break LOCA.

Oconee already has a requirement within its current licensing basis to trip reactor and reactor coolant pumps within two minutes during a small-break LOCA due to a minimum subcooling margin requirements. Therefore, even though this manual action is required in much less than 30 minutes, it is a reasonable exception to the D3 interim staff guidance criteria.

The basis for the two minute manual operator action is within the design basis for B&W plants, and was not changed by the addition of this digital system. In other words they will still have to do this manually until the end of time unless their current licensing basis changes.

MEMBER POWERS: That's the reason that you use the word, reasonable, there, is it is already existent?

MR. STATTEL: Yes.

MEMBER POWERS: It's not the product of reason.

MR. STATTEL: It's been in existence for almost 30 years at that plant.

MEMBER POWERS: It's the product of - it's been accepted in the past.

MR. KEMPER: Exactly. The operators have been trained for nearly 30 years to trip the reactor coolant pump.

MEMBER POWERS: It was just a choice of words.

MR. KEMPER: Well, reasonable assurance - reasonable acceptance - excuse me, reasonable assurance is a term we use all the time.

MEMBER POWERS: It's reasonable assurance, not reason this out logically and by dint of some mathematical relationship. I understand.

MR. KEMPER: Poor choice of words. Thank you.

MEMBER POWERS: It's not poor; I just wanted to understand it.

MR. KEMPER: Okay.

MEMBER ARMIJO: What is the fundamental reason why this has to be manual as opposed to automated?

MR. KEMPER: Well, good question. I was just going to cover that as a matter of fact. This

was invoked as a lesson learn. This function was invoked as a lessons learned from TMI, 1979, and for B&W plants, because of the once-through steam generators, they have a different configuration obviously than the U-tube or the boilers, and it turns out that during some transients it is not prudent necessarily to trip the reactor coolant pumps all the time. So a conscious decision was made many years ago to maintain that as a manual operator action. And the operators were trained that in some cases they tripped these pumps and tripped the reactor; in other cases they trip the reactor and they run the pumps, and basically they are like fans, just pushing through two phase flow through the loops trying to maximize the flow -

MEMBER POWERS: It's not a complicated evolutionary thing?

MR. KEMPER: No.

MEMBER POWERS: So this is very special.

MR. KEMPER: So really this is unique to B&W technology. It is an institutionalized current licensing basis activity. So we feel as though it's appropriate to credit them for this single exception.

MR. HILAND: This is now a slow news item as you know, when the digital I&C steering committee

developed the ISG, and we discussed in several meetings the 30-minute line in the sand. Industry reacted in several areas, not quite positive on that. And then all of a sudden we get an application that is a lot less than 30 minutes.

So we looked at it. It went in the HOV lane, and we looked at it, and if any other plant has 30 years of experience with a two-minute application, we would certainly consider it.

MR. KEMPER: So next slide.

So our current assessment is as follows. The inclusion of the diverse high pressure and low pressure injection DAS systems into the Oconee design provides an acceptable degree of diversity to address common cause failures in both digital actuation channels.

Also the manual actions greater than 30 minutes to address common cause failures of the RPS and ESFAS actuations are compliant with ISG-02 and provide adequate means of response to a software common cause failure.

VICE CHAIR ABDEL-KHALIK: So absent that 30 years of experience this two-minute manual operator trip would not have been acceptable to you?

MR. HILAND: We couldn't give that answer

without - we would look harder if they didn't have the data to support the statement or the assertion that this was a simple evolution.

MR. KEMPER: Yes, I wouldn't want it to get out that you've got to have 30 years of experience or nothing. But certainly the litmus would have to be made -

VICE CHAIR ABDEL-KHALIK: That's the rationale for your acceptance.

MR. KEMPER: Exactly. Exactly. So in this particular case they have a very compelling argument to substantiate a good strong - or to support their arguments that they are going to execute this function faithfully every single time. That's what it boils down to.

MEMBER APOSTOLAKIS: I am trying to see what conclusions I can reach beyond the slide. When you say in the first bullet, the best cross failures of those digital actuation channels, these common cause failures occurred to the hardware?

MR. KEMPER: Software.

MEMBER APOSTOLAKIS: Software?

MR. KEMPER: Right. Primarily what we are talking about here is software common cause failures. Because all four redundant channels are

executing software that is identical. That is why you have to assume that all four primary channels fail simultaneously for RPS, and all three of the primary ESFAS channels fail simultaneously. They could have done it differently. In fact we are working - we're going to have a NUREG here soon that is going to provide some ideas for how to build into diversity into a primary system.

MEMBER APOSTOLAKIS: Those common cause failures alone don't necessarily occur in just software. You just have a diverse system, so no matter how they fail -

VICE CHAIR ABDEL-KHALIK: But in this case there is an obvious potential common cause failure that drove them to that decision.

MR. KEMPER: Yes, exactly.

MEMBER BROWN: Well, but, how do you mean - what do you mean by that?

VICE CHAIR ABDEL-KHALIK: The same software is used in both.

MR. KEMPER: Yes, the software is identical in each channel, and so -

MEMBER BROWN: I am very familiar with software in every channel. I said it the other way once, and we rejected it all times after that.

Because it got too hard. Very very expensive, and the V&V is just brutal. So that is something I have learned. Y'all haven't gone to do that, and that is the first time I've been able to ask that question, that you do not have multiple sets of software in the multiple channels. I didn't see that in the ESBWR design. Maybe I missed it. Or US APWR for that matter of fact on the MilTAC or whatever? So that's - you guys are already - if you want to change it, you are already accepting - there's three designs rolling down the road that all have the same software. So for all the functions, at least based on my knowledge.

I understand your point. We wrestled with this in 1979.

MR. KEMPER: That is correct.

MEMBER BROWN: With how to do these, and how often. So we did a lot of different things to see what paid off and what didn't. The answers were not real clear. But there were actually some studies done down at Georgia Tech where they ran - authored out of your old place, where they issued, they sent out some major problems, and in other words, you want to go from point A to point B, and gave it to 25 or 30 different programmers, asked them to go program the stuff to see what diversity - it turns out that

everybody choked down to - at certain points in the solution they call came down to the same approach.

MEMBER BLEY: Went through the same programming class.

MEMBER BROWN: Well, these were all West Coast, East Coast, I mean it was all over the place. And so the judgment was made, in those papers that were issued, that software diversity may be a 5 percent benefit but not a 95 percent benefit. You can argue whether it's 5 or 95 - 5 or 10, but it's definitely not a lot. How valid is that? I'm not a programmer. But it's interesting; that's a good question.

MR. KEMPER: So at any rate what we are trying to say here is that at this point this is pre-decisional, but at this point we see no reason not to approve the Oconee diversity and defense in depth strategy of their application.

So as we speak we are writing the SE, in that manner. The next slide is just intended to show the path forward, and this is my last slide. There was some additional information that Oconee did OS, whi9ch is set point actuation, set points, and also some additional information to describe their built in conservatism for their D3 analysis which supports the

claim for operator action not being needed for greater than 30 minutes. We received that, we reviewed that, and so basically we are ready to move on with that.

VICE CHAIR ABDEL-KHALIK: How about the point that was raised by John about the operator sort of intentionally disabling all engineered safety features?

MR. KEMPER: Well, we are going to look at that real close. I'm sure there is going to be - obviously there are tech specs that have to be adhered to. I mean you know there is a number of ways you can disable a safety system right now in every plant. But of course it would be a violation of their operating license.

VICE CHAIR ABDEL-KHALIK: This is an awfully easy way to do that.

MR. KEMPER: Right, but I mean this obviously will have to be administratively controlled in some fashion, tech specs for example. So it is there for a reason. We have computer based systems now. The concern is that the computer will fail.

MR. FREUDENBERGER: I'm Rich Freudenberger from Oconee Nuclear Station. The current system for engineered safeguards has similar bypass that is on a per component basis, so in a

situation where you have a small-break LOCA for example, and you get the ES actuation, during the event you would take control of discharge valves, throttle back HPI, when you get full. So there is a need to have control for some events.

MR. SIEBER: I understand that, and I want to make sure that I understand the design, so I'm not overreacting. I understand that, and the RZ modules I think they are called where you take individual control afterwards. But that is possible only after you've had an actuation signal, right, that you can essentially remove that automatic actuation signal from the pump or the valve so that you can take manual control of it, which is in my understanding, in the new design, functionally equivalent to the new bypass reset - let's say bypass function.

So that - if I'm understanding the design correctly what you are talking about is function - in the existing design, on the RZ modules - is implemented by the individual I'll use the word channel, it's used a lot, the individual channel bypasses now that are only enabled after an actuation signal has occurred. Then you can bypass the channel. That will allow you to take manual control of all equipment associated with that channel. Is that

correct?

What I'm talking about, there are things called bypasses, and things called overrides.

MR. FREUDENBERGER: I just want to check the answer before I give it to you so we make sure we are accurate.

MEMBER BROWN: Should we go on or do you want to wait a minute?

MR. FREUDENBERGER: I just wanted to confirm, wanted to make sure that we were in agreement on this answer. The question was more on the current system for me. The current system as well, for the RZ modules, if you go up to the RZ module and put it in manual for an individual component today, it will go into manual and you will bypass actuation.

MR. SIEBER: Prior to an actuation system?

MR. FREUDENBERGER: Prior to an actuation system. So it's not a difference between the systems. It's all - it would be indicated. It would be an op normal condition. And it is not allowed by tech specs.

MR. SIEBER: But you would have to consciously do that for all pieces - I mean you would have to consciously walk up and do that.

MR. FREUDENBERGER: And that is the difference.

MR. SIEBER: High pressure pump, low pressure pump, in both trains, and all valves and fans and stuff like that.

MR. FREUDENBERGER: And that is the only difference between the systems is that in the current system you can only take manual control for individual components. But typically the way it's implemented during the EOPs in the control room, I was recently licensed, is that you would take a channel at a time, so it delays the operator doing multiple push buttons to take control of a channel at a time, then coming back around to the front panel to be able to control it.

In the new system you have one push button that lets you take control and be - and not have to go to the back panel, and be able to control at the front station.

MR. SIEBER: I understand that, but I am still trying to make sure that I understand it completely. If today you walk up - nothing is happening in the plant, normal operation, and you walk up to an RZ module, and you put that in manual, does that disable a future ESFAS signal from starting that

pump? Or can you only put that in manual after - in other words how does the interlock work?

MR. BAILEY: It doesn't disable it.

MR. SIEBER: It does not or does?

MR. BAILEY: The ES would still allow you to start it.

MR. SIEBER: Okay, and that function is logically the same as the new system's bypass function, whereas to essentially take manual control of let's say today all equipment in channel one, what you call channel one, you would actually have to go up and push maybe half a dozen different RZ buttons, and in the new design you would only have to push one button.

MR. BAILEY: That is correct. That is correct. And the intent is just for spurious actuation to allow you to override it and respond as well as during emergencies to override it and take manual control if needed. When you hit that button it doesn't stop anything that has been started, so the override would actually let everything continue to run until the operators actually stopped one of the individual switches.

MR. SIEBER: You used the word, override, and I'm trying to be really careful about the words

I'm using. Because I read in the design about a push button that is called a bypass push button, and there are eight of them, one for each of the channels. So I have bypass for channel one, I have bypass for channel three, five, seven, nine, and two, four, six, eight.

MR. BAILEY: Correct.

MR. SIEBER: As I understand it, the new design, I can walk up to the control board now with my plant operating at 100 percent power, push those buttons until I am blue in the face, and they don't do anything. They are only enabled after I have a safeguards actuation, the new design. I have to have a safeguards actuation; then I walk up to channel one push button, push it, and that then allows me to take manual control of all of the equipment associated with channel one. Is that correct?

MR. BAILEY: On the new system or current?

MR. SIEBER: New system.

MR. BAILEY: New system, I believe it's correct. I'm trying to piece together the exact scenario.

MEMBER BROWN: Can NRR take this as a question? So we can move on and get a nice clean description. It's a very good point; we need to get

that resolved.

MEMBER BLEY: I have a high level question about the same thing. John has brought up a couple of things, both are aimed at doing the spurious actuations of supposedly very highly reliable new digital systems. In one case we give an operator the ability to, if he thinks it's going wrong, to defeat it. And then the other we take what I assume are two old fashioned electromechanical relays, and now failure of one out of two instead of one out of one. I suspect if somebody does a reliability in house, that is going to be driving the reliability of the system.

Was there a history of spurious actuations at Oconee that led to this? Or is this a general approach that is kind of going to be in all of these kinds of systems, where you worry about spurious actuation?

MR. KEMPER: I can't answer for Oconee directly, but I can tell you that there is a concern within the industry with automatic diverse actuation systems being spuriously actuated. It has been verbalized to us on many occasions in public meetings and so forth.

So the Oconee design, by using a two out

of three coincidence logic has provided a pretty good engineering solution to that. So that is minimal opportunity, as I see it, there is minimal chances of that system being spuriously actuated. You would have to have two active failures in order to do that.

Now I don't know what kind of history Oconee has with spurious actuations, but it sounds like it's just good design engineering practices to me if I can speak from my industry experience once upon a time.

MR. SIEBER: The other question would be not necessarily concern among the industry, but experience in particular, because this is a Teleperm design feature, it's not - I don't get the impression that this is - I'm not sure about the overrides, but I don't get the impression that this has been added as an Oconee-specific function, whether it be the Teleperm system itself has a history of generating spurious signals. If it's being expressed from the industry, well, obviously everybody is concerned about spurious actuations. But they'd be concerned about spurious actuations all from mechanical relays also.

The question is, if the system has been designed so carefully to avoid spurious actuations, where you need so many coincidences both voter logic

and two out of three and a series of relays and so forth, is there actual - I mean they have been operating the system for awhile, if it is designed well you don't really get a spurious actuation, but you'd have an awful lot of alarms, which are probably not tracked. That is the problem. It wouldn't show up in failure space, because the system design prevents you from getting the spurious actuation, but a lot of failures.

MEMBER BROWN: Can we go on? Thank you.

MR. KEMPER: Okay, so I think I'm done. What I'd like to do now is introduce Rick Stattel as the next speaker. This is the first time Rich has spoken to this group as an NRC staff member. He has been here as a vendor before.

Rich joined the NRC last year. He is one of our lead reviewers with the Oconee application. Rich before joining the agency most recently he worked for General Electric Hitachi as a software projects lead engineer for the ESBWR plant, and also prior to that Rich worked at Calvert Cliffs as a digital controls and reactor protection system engineer for about 15 years. During this time he also served as a digital feedwater system engineer, as well as a system engineer for the Westinghouse CommonQ platform

implementing a post-accident monitoring system. So with that, Rich, I'll turn it over to you.

MR. STATTEL: Okay, thank you very much.

The next topic is digital system communications. And this slide here shows the principal documents that constitute the available guidance for digital system communication.

First on the list is IEEE standard 603, and that is directly referenced from 10 CFR 50.55 alpha. Okay?

This standard provides criteria for independence between redundant portions of safety systems, not just communications. But it also provides independence - guidance for independence between safety systems and other nonsafety related systems. So we will talk about, we will cover both of those areas in our discussions.

The second standard listed here is IEEE 7-4.3.2, and it added to the 603 criteria that data communications between safety channels or between safety and nonsafety systems should not inhibit the performance of the safety function. And I think our upcoming slides will demonstrate that.

Okay, finally the digital I&C steering committee formed task workgroup number four to clarify

the guidance of those two documents. The resulting interim staff guide provided 20 adherence points for evaluating digital safety systems compliance with the NRC communications guidance.

The ACRS has reviewed that interim staff guide.

So ISG#4 was used to evaluate the Oconee license amendment request.

The next slide shows a figure - this figure illustrates the pathway that is used for communication between safety channels and with the voters. Two different communication paths. This communication path is necessary to support fault tolerance features of the system; was mentioned before, the second min second max functionality. Remember every sensor channel is aware of the sensor inputs from the other two channels, right. So if I'm channel alpha, I'm aware of what the signals are from channel bravo and channel charley, and I use those three channels, and I take a second min function for a low trip, and a second max function for a high trip. And I use the resulting signal to perform my bistable actuation.

That function is implemented via these communication links. Okay this communication protocol

also supports the transfer of channel trip status information from the voter logic functions. If you refer back to slide #5, the figure on slide #5, the second min second max functions, those communication links are the horizontal green lines that you see there, and of course the voter communications would be the diagonal lines shown on that drawing.

What I'm going to discuss now are the characteristics of this particular link. The link supports two-way communications. Fiber optics are used to provide the IE isolation, and that is shown at the center of the diagram here.

Communication isolation is achieved by using communication buffering circuits. These circuits use what we call a dual-ported random access memory, and a communication processors, PROFIBUS controller is shown there in the figure.

These communication processors operate independently of the safety function processors which are shown on the outside portion of that diagram.

Their sole function is to transfer communication data to and from the dual ported random access memory locations.

Communications uses a PROFIBUS protocol and data buffering using this dual-ported random-

access memory.

The safety system processors maintain independence because the communication between different safety processors is via independent communication processor. And this is in accordance with the guidance in ISG#4. So in the diagram, what is shown here is this would be channel alpha on the left side of the diagram. That is the safety function processor that is performing the safety functions. And then on the far right would be the safety function processor from channel bravo.

Now deterministic behavior, the way that is achieved, first of all all communication is performed cyclically. There is no interrupt-driven communication used in this particular pathway.

All messages have individual fixed message characteristics, such as the length of the message, the format, the ID, et cetera. Memory locations are preassigned within the random-access memory location, and the communication load is constant.

Any questions on that figure?

MEMBER BROWN: Yes, when you say communication load is constant, do you mean that the exact same sequence of communication bits and bytes is the same in every cycle? In other words they are

sequentially the same, so it runs through almost like a main operating loop across the board?

MR. STATTEL: That is correct.

MEMBER BROWN: It cycles through on the same time base completely?

MR. STATTEL: That is correct, and the concept of using the dual ported memory really serves to perform that function. So basically as the safety function processor executes its program it will go and read that data, the communications data, from the dual ported memory, right, regardless of what the communication processor, it is writing that information up to the dual-ported memory, so it's going to read whatever is in that memory location.

MEMBER BROWN: Does everybody understand what he just said?

MR. KEMPER: Yes, graphically we've got two processes going if you follow my little mouse here, okay. There is a communication processor; here's a safety function processor. These guys are operating continuously, around and around and around, just circulating data, dumping it into the dual-port RAM locations. The safety processor goes through and it reads that information, whether it's been updated or not. It just goes to the same place and looks for

the same information and processes it the same way.

MEMBER BROWN: Okay, I just wanted that explicitly stated. That's like a - it acts like an interface which isolates the software and the communications from the software in the safety processing. That

MR. KEMPER: And what a dual-port RAM does, you can read on one side input, and change on the other, and it doesn't affect what is going on, it doesn't change the deterministic nature of the beast, because they both have fixed cycle times.

MEMBER MAYNARD: And it doesn't matter how fast the data may be changing or not changing or anything.

MR. STATTEL: It reads whatever happens to be in there.

MEMBER BROWN: Good data or bad data.

MR. KEMPER: And the cycle is about 30 milliseconds for the safety processor, and every 30 milliseconds it grabs its data, processes it -

MR. STATTEL: There are checks in there, so if the data is not updated, like if the communication processor stops updating the memory locations, the safety processor would be aware of that, and it would basically flag that signal as being

a failed signal, and it would operate on the remaining -

MEMBER BROWN: The key point is that the safety processor processes information that it's got, and does not stop its safety function processing.

MEMBER BLEY: When you are presented something that says, claims independence, how far do you chase that in the review? Do you get down to things like is there a common ground? Are these going to be in place with a single room chiller that goes out, temperature is going to take out the system, that kind of thing?

MR. KEMPER: Well, okay, it depends on if you talk about hardware, the equipment qualification program is what deals with that primarily. In other words the equipment has to be qualified to survive any environment during Chapter 15 accidents where it's located.

MEMBER BLEY: Typically that assumes the HVAC is running. That could be the failure if the HVAC fails.

MR. KEMPER: Not necessarily. No typically what I've seen from our environments, the envelope of the high temperature assumes that there is no ventilation in that room. Most control rooms

envelope at about 115 to 120 degrees. That's based on at some ventilation not being available.

MEMBER BLEY: Most plants I've been in and asked to see the calculations on room heat and HVAC, they have a lot of trouble finding it.

MR. KEMPER: It's a very intense exercise. I spent a lot of hours of my life at Calvert Cliffs trying to deal with that very issue once upon a time. It's a very - it's a hard thing to deal with calculation wise.

MEMBER BLEY: And you did things like a common ground connection?

MR. KEMPER: Well those are design standards, okay. That's where you end up with separation and every plant has got their own design standards to ensure that separation is maintained between each channel.

MEMBER BLEY: But you count on the plant standards to take care of that? That's something you'd review.

MR. KEMPER: No, we wouldn't - that would be an inspection thing. That's an insulation thing if you will. So if that was going to be reviewed the inspection forces would look at that in the regions from a licensing standpoint. They make a commitment

that it will be isolated per 603, and we look of course at the drawings and whatnot they provide to us and we approve it accordingly from that.

MR. STATTEL: But from the perspective of the communications isolation, again, we use the ISG, the 20 points that are listed in the ISG, and we really are looking at the safety function processors being able to maintain those functions regardless of what happens with those communication lines, okay.

MR. HILAND: This - the NRC's oversight and review of this system includes two parts as Bill references. We are doing the licensing part, and we are going to make a decision whether this is available to the licensee to install. We work with region two, and we are still working with them, to develop what are their - if you remember the construction days, what is your inspection procedures going to be, and they will have the lead. And that was one of the first steps that we took last year was where do we divide and stop licensing review, and let the inspection forces take over.

Some of the information was very hard to let go of from our office. We wanted to do everything. No, you've got to stop. We have trained inspectors out in the field; let them do the work.

But I remember inspecting grounds in my life.

MEMBER BROWN: Back on slide five you show these green communication lines. Some go - pass through without a little square when they hit the box. Some have a little square when they go from box to box. I couldn't quite figure out, does channel A information go to box B, C and D?

MR. KEMPER: Yes, there is not enough definition there unfortunately. Every channel communications all of its information -

MEMBER BROWN: Okay, that's fine, stop right there. One other point I wanted to make for you all, at least from my aspect, where there is no definition, is that the deterministic nature of it and the data doesn't mean that the data that is being transmitted can't corrupt the other channels. Because you are sending data from channel A to channel B, C and D.

MR. KEMPER: But it's via this pathway right here, for this logic here.

MEMBER BROWN: All that does is - but the data is still doing it. If you have corrupt data from channel A which gets into the processing side that somehow corrupts the processing for a function in B, C

and D, you have just lost all four channels.

That is a question that has to be answered.

MR. STATTEL: Well, not necessarily, but that is addressed in the failure modes.

MEMBER BROWN: All I'm saying is, we are running out of time right now. I just wanted to - what we've seen is necessary but not sufficient to define independence of channels. That is the only point I wanted to make.

MR. STATTEL: The previous figure showed the channel to channel and channel to voter communications. This figure that you see here on slide #15 provides an architectural view of the safety to nonsafety system communication pathways.

The safety related monitoring and service interface which we talked about before, the MSI, the blue box here, provides a qualified propagation barrier that is consistent with IEEE 603. The communication path between the safety system and the service unit, which is the green computer workstation shown there in the lower right part of the screen, is bidirectional in nature. The service unit is used for testing, equipment health monitoring, and for providing design changes to the digital system.

Some examples of how the service unit will be used, performing surveillance and maintenance testing, monitoring diagnostics indications for failed components or failed input signals, performing software updates which would be done with the system offline; and performing set point changes and again, the channel would have to be bypassed or the system offline to do that.

These tasks are performed by authorized personnel using administratively controlled key switches, as well as user log in password to the service unit itself.

The communications path between the safety system and the gateway computer which is the yellow box in the upper right part of the diagram, is one way. The gateway computer is an interface to the operator aid computer, so basically the plant computer for the plant.

VICE CHAIR ABDEL-KHALIK: Where is the service unit physically located?

MR. STATTEL: It is inside the protected area.

MR. KEMPER: It's in the control complex itself. It will be in the control room or a room contiguous with the control room. And of course

access to it is controlled by the operators. This is all part of their security process, which we are not going to talk about that in detail in this environment.

MR. STATTEL: So the operator aid computer is really your only pathway to the Internet and the outside world. And that is one way communication, and we will talk a little bit about how that is enforced.

Okay, the safety system integrity is additionally ensured by the NetOptic port tap device, again that is shown in the dark blue box, and this enforces a strict one-way communication path to the gateway.

The media converter, I think we already talked about this, the media converter simply converting from optics to electrical signals. And the Ethernet switch that is shown between the service unit and the net optics device is necessary because it maintains an open communications pathway to the gateway when the service unit is turned off.

MEMBER MAYNARD: I take it the service unit is a dedicated unit. It's not a laptop or something somebody can carry up there.

MR. STATTEL: It is dedicated, but it is

a nonsafety related device.

The next figure illustrates the communication pathway that is used for the communications between safety and nonsafety systems. It kind of goes along with the previous drawing.

In the center here, those three blocks you see in the center represent the internals of the MSI, okay. As you see the link shown here supports both two-way and one-way communications as we just described. One way for the case of the plant computer or the operator aid computer, and two-way communications for the service unit alone.

Fiber optics link again provides the 1E isolation between the safety and nonsafety systems for electrical isolation. And communication isolation is similarly achieved using communication buffering circuits that use the dual-ported random access memory locations that we discussed before.

The safety system processors are independent from the nonsafety because there are no direct communication between the safety processors and the nonsafety equipment. You can see that this scheme facilitates that.

In order to achieve deterministic behavior for this pathway, again, communications are performed

cyclically. There is no interrupt-driven communication. All messages have individual fixed message characteristics. The nonsafety service requests coming from the service unit will have a lower priority than safety functions. And these service requests are executed only after the safety functions have completed their safety execution cycle.

Any questions on that?

VICE CHAIR ABDEL-KHALIK: How many remote shutdown panels are there at Oconee?

MR. KEMPER: Remote shutdown panels?

VICE CHAIR ABDEL-KHALIK: Right, and would they be affected by any of this?

MR. KEMPER: I don't believe so. There is no interface with remote shut down panel in these computer based safety systems being put in. That wasn't part of the license renewal request, and it makes no mention of that.

MR. STATTEL: All right.

The current NRC assessment for communications basically, the license amendment request appears to adequately address each of the 20 adherence points listed in the ISG with one exception, and that is item #10. In the ISG it states that the service unit or the equivalent should be physically

restricted from making changes while the channel is performing its safety function. It also goes on to say that the restriction, the physical restriction, should be by means of a physical cable disconnect, or by means of a key lock switch that either opens the data transmission circuit, or interrupts the connection by means of hardware logic.

In the Oconee design a software based key lock switch is provided to enable changes via the service unit under certain administrative controls. If you like I can go into what those administrative controls are. But the design is an exception to the ISG guidance. The staff is still reviewing this feature to verify that it provides a reasonable assurance against unauthorized changes to the system. So again this is one that we are currently working with right now.

The second point -

MEMBER POWERS: What have you -

MR. STATTEL: I'm sorry?

MEMBER POWERS: I come back to the question of reasonable assurance on administrative controls. How do you judge those things?

MR. STATTEL: With regard to isolation, basically the way the system is configured there are

key switches that are located in the individual cabinet, so if you want to make a set point change for example, to channel alpha, high pressure trip, you would go to the channel alpha cabinet, and you would turn a key switch, and that key switch toggles a bit within the program which gives a permissive for the service unit communication path to go in and make that set point change. That is a deviation from the ISG guidance, because the ISG guidance is basically saying that you have to cut the communication path, and they are not implementing that.

So we are still kind of reviewing this to try to get that -

MR. HILAND: Let me help answer the question. He asked the question how do we make a reasonable surveillance decision. In this case while they take the exception, it's just guidance. They can make suggestions to do other things. We have a principal reviewer who goes through our qualification program. He makes a decision to recommend approval or not of that design.

Then we have a peer level reviewer. That peer level reviewer will look at that decision. Then those two decisions will be reviewed by their branch chief, and eventually signed off by me.

That I think gets to your question. I don't have a definition of what is reasonable assurance of this toggle switch if they don't meet the ISG.

MR. STATTEL: If I may, had they had an obvious switch that broke the communication path like we stated before, that would have been a fast path to approval. In the case of the software implementation here, we expect our path forward, we expect to go and perform an audit and actually review the line by line coding. So we have to go into a lot more detail on that aspect in order to get that reasonable assurance.

MEMBER POWERS: You have a database that you can go compare against. And what you are saying is, now I have to go down into the details.

MR. STATTEL: It takes a lot more effort to get there if the guidance is not followed.

MR. KEMPER: The licensee just stepped out of the HOV lane and they are on the service road now. So it is going to take longer and more effort for us to review this. So yes we are going to have to review the V&V effort, make sure it was absolutely stellar; the code, review the administrative requirements to be sure that they are absolutely intact and appropriate. And that will support our

reasonable assurance determination.

MEMBER POWERS: If I went back, if I wanted to plunge into this detail, I would go back. The primary reviewer would have mapped out his logic. His peer reviewer would have checked that, probably his engineering calculation or analysis or something that gets signed. I could track exactly how this decision was made if I cared to.

MR. KEMPER: It actually will be documented in a safety evaluation very explicitly.

MEMBER POWERS: Sometimes those are a little glib. Sometimes they say, we found this to be reasonable.

MR. KEMPER: This is not going to be glib. This is going to be very transparent. In fairness, though, a lot of things we are doing with this application is going to be precedent setting. So that is why it is important for us to labor the details on the safety evaluation. This will probably be - it will have some pretty good poundings to it before we are done with it.

MEMBER POWERS: And I think you probably want to think seriously about having done it, go back and say now did we learn any lessons here.

MR. KEMPER: Oh, absolutely.

MEMBER POWERS: You will have set a precedent, and maybe in the end you say I didn't want to set that precedent.

MR. KEMPER: Exactly. As a matter of fact, this is a segue, I don't want to open it up too much.

MEMBER POWERS: Yes, don't open it up anymore. Let's regain control of the process here.

MR. STATTEL: Okay, the final point on this slide is the Port Tab device. It appears to provide an acceptable one-way communication solution, but again we want this to be as transparent as possible, so we have asked Duke to provide the technical details, some of that being proprietary, to support the state of functionality of that device.

MEMBER BROWN: Next page is just a summary isn't it?

MR. STATTEL: It's pretty much just a summary.

MEMBER BROWN: Can we just pass that one and go on?

MR. STATTEL: Okay.

MEMBER BROWN: Is that okay with everybody? The next page is really a summary. We ought to just go on to page 19.

MR. STATTEL: The final topic is the changes that were made to the TSX platform. I stated earlier the platform safety evaluation was issued in May of 2000. Since then the TXS - since that was issue, several changes have been made to the platform. The majority of these changes were not really very significant. However some of the changes were significant, and we have asked, and Duke has provided, summaries of what the changes were, or AREVA has provided that.

The staff must - our position is that the staff must review all of these changes to ensure that they are acceptable, and to ensure that the previously issued safety evaluation conclusions are not adversely impacted.

The next three slides list those significant changes, and we can go into those details made in each of those areas. We're talking about hardware changes, software changes and procedure changes, which were all part of the original TXS safety evaluation.

Slide #20 talks about the - this slide highlights the significant hardware changes made to the TXS platform. First of all the safety function processor, a pretty critical component of the system.

The component that was evaluated in the original topical report was replaced with a new safety function processor, which of course is faster and has more memory.

This change also resolved an unavailability of components issue, an obsolescence issue. So there were various reasons for making the changes.

The communications module was also changed to accommodate for the new safety function processor. Some IO modules have changed to increase the resolution, because - and we expect these changes are generally good because they improve the system performance. Not all of them are done for that reason however.

The subrack was also changed to relocate the power supply to the top of the rack to accommodate U.S. conventions.

Any questions on the hardware changes?

All right, on the software side, we break this down into two - there are basically two types of software. The topical report -

MEMBER BROWN: I had one question. I presume there was some effort at - whatever the basis for qualification of that hardware environment,

whatever it is, I presume they passed on that information also. I presume it was requalified so it still meets the original safety evaluation?

MR. KEMPER: That is correct. And what we will do is we will sample some of those qualification -

MEMBER BROWN: I just wanted to make sure you were doing that.

MR. STATTEL: Yes.

Now the software side the topical report discusses two different types of software. First is - first off is the software that was used in the application development process. They have a tool they call SPACE, which is the acronym spelled out here. Specification and Coding Environment, and it's basically what the developer is using on the computer when they are building the function block diagrams and actually performing the development, the software development process. So changes to that are also very important, and we have to ensure that they still meet the requirements that they were originally specified for.

Second type of software is the software that is actually delivered with the system that supports the application software. What we are

talking about here is the operating system, or another term would be the run-time environment for the TXS system.

The space tools were updated -

MEMBER BROWN: Before you go on, is that a - the operating system on which you operate, is that a main operating loop type system where every function, every algorithm, everything is process in every 30 millisecond or 50 - whatever the sample time issue is? Or is it more of an executive system where it decides I'm going to do a little bit of this now and a little bit of that now, setting aside the self test which is always incrementally done typically? Or is it interrupt driven?

MR. KEMPER: It is continuously circular driven. Every 30 milliseconds, all the application software -

MEMBER BROWN: Every application function -

MR. KEMPER: Every application is implemented if there is time -

MEMBER BROWN: Every piece of data is sampled.

MR. KEMPER: Right.

MEMBER BROWN: Whether it's good data or

old or whatever it is.

MR. KEMPER: Whether it is good, bad or indifferent, and it will annunciate whether it's good, bad or indifferent - whether it's bad or indifferent. If there is time left in the cycle, then the self testing and diagnostic routines are run. Then if there is still more time then - what's the last thing? Service unit, I'm sorry. Yes, the priority is the cycle time for the safety system, the service unit task and then the self testing.

MEMBER BROWN: Okay, but any one of those, once it finishes that, it does not stop. If it's doing something with the service unit, it does not slow down the operating cycle.

MR. KEMPER: It stops where it is and goes on, saves that to a memory location and goes on.

MEMBER BROWN: Okay, and if it locks up what happens?

MR. KEMPER: Pardon me?

MEMBER BROWN: Is there a watchdog timer in the system?

MR. KEMPER: There is a watchdog timer that is set with each - right, exactly.

MEMBER BROWN: Okay, and if it locks up does the watchdog timer reset it? Does it trip the

channel?

MR. KEMPER: If it locks up you get an alarm, and my understanding is the channel is tripped.

MEMBER BROWN: Does it produce a reactor trip?

MR. KEMPER: I'm trying to think of the status the channel goes into.

MEMBER BROWN: I don't care, I just want to know which one it is. I didn't see that.

MR. STATTEL: I think you would fall back to a 2 of 2 logic.

MEMBER BROWN: Two of three.

MR. STATTEL: Well, if one of the channels goes out.

MR. BAILEY: This is Mike Bailey again. On the watchdog timer, if it is RPS and it times out it will trip that channel.

MEMBER BROWN: But that is a trip signal. In other words it provides a reactor trip, one of two of four that you need to trip it.

MR. BAILEY: That is correct. On ES it will not, since it's an energized actuated system.

MR. KEMPER: It's a failed input. It annunciates that. The operators know that.

MEMBER BROWN: Now does it have to be

manually reset, manual reset so it stays in the trip mode, it doesn't reset itself?

MR. BAILEY: That is correct. It has to be manually reset.

MEMBER BROWN: All right, thank you.

MR. STATTEL: The SPACE tool software changes included the development environment was ported to a new operating system. Again this is the development environment, not the actual application operating environment.

And a change to the database management system was made. The TXS system proposed in the Oconee LAR uses a newer version of both of those types of software. So we are evaluating that on a sampling basis.

On the procedure changes front here, there were some significant procedure changes made. The NRC policy is that approval of the digital computer based safety system includes a determination that a high quality development process was used. And that process involves several procedures that are outlined in the standard review plan.

In support of that development process determination for the TXS platform several procedures were reviewed as part of the original topical report.

So changes to those procedures are what we are currently working on reviewing and evaluating the impact.

Processes and procedures were changed to add details to include experience with programming of the TXS software, enhancements in the C++ programming guidelines, and adaptation of AREVA'S corporate document guidelines.

The Oconee LAR includes additional hardware qualification testing requirements to address plant specific action items in the topical report, safety evaluation.

Another enhancement was the improvement of the configuration control, configuration management, by adding a change control board review to their process. So what we have seen so far in the document reviews is that they have made improvements to the processes, their developing processes. And that is ongoing as well.

MEMBER BROWN: That is a summary slide there, right?

MR. STATTEL: Right, the next one is a summary slide.

MEMBER BROWN: Can people read that? We are almost running out of time. There are two

proprietary slides, but they are really kind of computer weenie stuff. By that I mean they are super detailed, you get some data in, and you get a buffer - I don't think they are overwhelmingly necessary for this discussion.

So I was going to suggest, if it's okay, that we would go ahead and entertain any other questions? Is that satisfactory? I don't think we had anything but the summary.

MR. KEMPER: That brings us to our last slide.

MEMBER BROWN: So the protocol here is, does anybody else have any - oh that is an overall summary. I'm sorry, go ahead, you can do that one I guess.

MR. KEMPER: Well, again, this is just a repetition of what we have already told you. So I can read through this, or we can entertain any additional questions you may have at this point. This is just a chunk of information associated with this application. But it's a pretty good chunk. Inter-channel communications is a big deal. That is the heart and soul of the integrity of this system quite frankly. And I think the application does a good job of complying with the ISGs, both one, two and four.

We haven't talked about cyber security yet, because this is the wrong environment to do that. But basically I think we are on a success path here of reviewing this with a positive conclusion. Again, that is pre-decisional, so don't hold me to that as Pat said at the beginning of this thing. As new stuff arises we may change our thinking on certain things. But at this point things look promising.

MEMBER BROWN: If there is anybody who has any questions?

MR. SIEBER: I just wanted to clarify one thing. Since we accuse people of being not very precise in terminology, I fell victim to not being very precise. In the detailed discussion we had going on earlier I kept referring to something called bypass, and we were comparing it RZ module. What I should have been talking about is something that's called an auto manual function for each channel. Just to clarify that. We don't need to go back into the discussion, but it's the auto manual per channel versus the current RZ as one issue. And as a separate issue something that is called an override. But just to make sure, because there is something else called a bypass, which is not what I should have been talking about.

MEMBER BROWN: Somebody else?

MEMBER SHACK: I'd just come back to this two-minute question. What is the guy thinking about in the two minutes that the computer can't think about in the two minutes and make the decision? What is my analog computer doing that my digital computer can't?

MR. KEMPER: Well, let me just try that, having some experience with that myself. The first thing an operator is trained to do is look at subcooling margin. Okay that is the heart and soul of an operator's awareness of what is happening inside of the reactor vessel itself.

As you know, head boarding is a problem at B&W plants because of the design, so that's why subcooling monitoring is very important. So the operators look at that, and of course they have to assess what accident basis they are being confronted with. So a decision has to be made very quickly whether to trip the pumps or not trip the pumps. It's a conditional statement. It's a conditional decision. It depends on what is happening in the plant. And this computerized trip system doesn't have that information built into it. So it still takes the human being in this particular environment to analyze that. And they are trained rigorously to do that. I

hope that answers your question.

MEMBER MAYNARD: Just a quick question. Some of the improvements they made in hardware that you are having to review, is that something that you see coming down the line for most of these digital systems, that every 10 years or so people are going to be coming in needing approval for an updated processor?

MR. KEMPER: Absolutely, it absolutely is. In fact I was just called by Triconex people two weeks ago and Westinghouse people three weeks ago kind of talking about if we make a submittal to amend the approved platform that we have, when can it get reviewed, what are the logistics, blah blah blah. So all the vendors are thinking about that. But we are also promoting that. Quite honestly that is our viewpoint.

Because you see the way it's being done with Oconee is, much of the burden of the regulatory burden is being placed on the shoulder of the licensee. There is just no way of getting around it. Because we are approving two things. We are approving the site specific application and the upgrades to the platform.

So I personally try to preach, whenever I

get a chance in a public environment, for vendors to be pro-active and go ahead and do this on their own.

MR. STATTEL: Also a lot of the documentation that we are needing in order to perform these change or delta reviews we are asking - we are kind of putting it out publicly that it would be a lot easier if you submitted those with the original application. And we are trying to lock that process down so they know what they need to submit, identify what the changes are, identify the significance of those.

MEMBER BROWN: Any other questions?

MEMBER RAY: John, you have pursued the ESFAS lock out feature here a lot. I'm not sure where you end up.

MR. SIEBER: I think it's still a little open.

It's open. We've got an action item for them. My problem is, I think I know how it works but I might be completely wrong.

MEMBER RAY: My question was going to be, do you know why they put it in there?

MR. SIEBER: You know, Harold, this is my own personal opinion, what I see, what I read anyway, is - and we mentioned this earlier - is many features

of the system that are designed specifically to prevent spurious actuation. Now the reason for that I don't know. But there seems to be a very large sensitivity to prevention of spurious actuation, anywhere from the way that the voters are configured with the two series output relays to these override push buttons to things like that.

MEMBER RAY: That is an inference you have drawn, probably correct. I just wondered if you had any other questions about why is it this way, so that we don't speculate later.

MR. SIEBER: I don't know why. I mean that was a question about, has there been experience with the TXS earlier versions of the TXS.

MEMBER RAY: That may be one way, or maybe somebody just thought this is a good idea. I just thought since they are here, somebody might want to speak to that.

MR. SIEBER: Nothing that I know from my experience over in Switzerland, I haven't really thought about this end of the thing over there at all.

VICE CHAIR ABDEL-KHALIK: I guess the question in my own mind is whether or not this is a desirable feature to have.

MEMBER RAY: Yes, but in order to judge

that I would like to hear somebody explain why it is the way it is. But I'm not smart enough to ask the question. That's why I asked John.

MR. SIEBER: The first thing to make sure is that from this side of the table have the correct interpretation of -

MEMBER MAYNARD: We are all guessing at something here. I think we first of all need to understand how it works and the rationale for that.

MEMBER BROWN: What I am hoping, what I'd like to do is suggest that I take an action, and then we'll prepare a white paper or whatever, a letter to you all, to try to give you some information on that.

MEMBER ARMIJO: If you would just put in why it's a good thing, and why there isn't a down side to it.

MR. STATTEL: From a reviewer perspective, we really view these things as being features. And as long as - really the burden is on us to have assurance that those features don't have an adverse effects on the actual safety functions. So that's the way we, the reviewers, are looking at that.

MEMBER RAY: Yes, but when you say it that way, that may be the constraint that you live under, but when you said it doesn't have any adverse

impact, that's too strong. Obviously there is a tradeoff here, as we've all said. All we are trying to do - all I'm trying to do is elicit what the benefits are so that we can weigh them against -

MR. HILAND: We got it, we'll take it.

MEMBER BROWN: I would just like to thank the staff for the presentation. Really appreciate you doing this. And also the folks from AREVA for coming up and providing the additional information.

Personally I thought it was a very useful presentation with a lot of very good information that clarified a lot of stuff that is not intuitively obvious from reading all the papers.

So thank you very much.

MR. STATTEL: Thank you.

CHAIR BONACA: Thank you very much for the presentation. And we will take a break now until five after.

(Whereupon, the above-entitled matter went off the record at 2:47 p.m. and resumed at 3:05 p.m.)

Treatment of PRA Uncertainties in Risk-Informed Decision Making

Advisory Committee on Reactor Safeguards

February 5, 2009

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Presented by:

- U.S. Nuclear Regulatory Commission
  - Mary Drouin, mary.drouin@nrc.gov
  - Gareth Parry, gareth.parry@nrc.gov
  - John Lehner, lehner@bnl.gov
  - Jeffrey LaChance, jllacha@sandia.gov
  - Timothy Wheeler, tawheel@sandia.gov
- Electric Power Research Institute
  - Ken Canavan, kcanavan@epri.com
  - Don Vanover, devanover@erineng.com
  - Doug True, detrue@erineng.com

Objective of Meeting

- Discuss US Nuclear Regulatory Commission (NRC) and Electric Power Research Institute (EPRI) work
- Future work
- Request letter

Outline

- Purpose of Program
- NRC and EPRI Collaboration
- Scope and Limitations
- Changes to the Reports
- Detailed Example
- Future Work

Purpose of Program

- Provide guidance in support of the requirements addressing uncertainty in the ASME/ANS Probabilistic Risk Assessment (PRA) Standard
- Provide guidance on how to treat uncertainties associated with PRA in risk-informed decision making

NRC and EPRI Collaboration

- NRC and EPRI work start with consideration of the decision under consideration, the PRA standard, and the supporting PRA model
  - NRC focus is from a regulatory perspective
  - EPRI focus is from an industry perspective.
- NRC and EPRI efforts provide guidance on parameter and model uncertainties
- Regarding parameter uncertainties
  - NRC NUREG provides guidance on characterization and propagation
  - EPRI report provides guidance on detailed and approximate methods

NRC and EPRI Collaboration

- Regarding model uncertainties
  - EPRI report provides guidance on the identification and characterization of the sources of uncertainty
  - NRC NUREG provides guidance on identification of sources of uncertainty key to the decision.
- NRC NUREG also provides guidance addressing uncertainties
  - From non-modeled risk contributors (referred to as completeness uncertainty)
  - In the risk results and insights so that they are treated in the integrated risk-informed decision making

Scope and Limitations

- Limited to addressing the uncertainties associated with the use of the results of risk assessment models for risk-informed decision making
  - Does not include guidance for uncertainties associated with other analyses
- Guidance not provided for sources of uncertainty associated with internal fire and external hazards, and for low power shutdown conditions
- Guidance provided on the process for identification and characterization, and for how to factor the results into the decision-making, is generic and is independent of the specific source of uncertainty

Scope and Limitations (cont'd)

- Guidance not provided for performing expert judgment or elicitation
- Guidance not provided for employing an expert panel
- Guidance focuses on currently operating reactors
- Process is applicable for advanced LWRs and non-LWRs, and reactors in the design stage
  - the screening criteria and the specific sources of uncertainty may not be applicable
  - sources unique to these reactors not addressed

Scope and Limitations (cont'd)

- A model uncertainty needs to be distinguished from an assumption or approximation that is made to limit scope of model (e.g., with respect to level of detail)
- These assumptions and approximations are generally not considered to be model uncertainties
- Methods for addressing this aspect are not explicitly included, but are addressed when assessing the validity of conclusions

Changes Since ACRS Sub-Committee

- Clarified scope and limitations regarding:
  - operating reactors, new or future (non-LWR) reactors
  - initiating events and power conditions
  - level of guidance (e.g., expert panel)
- Changed tone so that the guidance is for what needs to be done, rather than what is not needed
- Clarified that the guidance is how to deal with uncertainty in the context of making a risk-informed decision, rather than providing an assessment of the global uncertainty in CDF and LERF

Changes Since ACRS Sub-Committee (cont'd)

- Added guidance on presenting assessment of credibility of results from alternative assumptions
- Added discussion that the information in Table A-4 in EPRI 1016737 is a valuable additional resource and may be useful for specific application
- Added clarification regarding the uncertainty associated with the use of a single model, not because it's consensus, but because it's the only available model
- Clarified the term "uncertainty intervals" (term that is used in ASME/ANS Standard)

Changes Since ACRS Sub-Committee (cont'd)

- Added a warning about the impact of not taking into account state-of-knowledge correlation (SOKC) on truncation
- Renamed SOKC correlation to epistemic correlation
- Enhanced the guidance regarding relative screening so that focus is not screening on absolute value
- Clarified that the "estimate" is in the context of "in lieu of propagating" (impacts EPRI report)

Changes Since ACRS Sub-Committee (cont'd)

- Provided guidance to treat human reliability analysis (HRA) as a special case:
  - Unreasonable to expect use of different HRA models.
  - Sensitivity studies should reflect variability from different methods
- Identified the choice of standby failure rate model (EPRI report) as a source of model uncertainty rather than whether the parameter is the correct value
  - Guidance on need to justify model selection is provided

Overview of Appendix A

- Example implementation of the guidance
- Utilizes an AOT extension for the RHR system at a hypothetical BWR-4
- Attempts to exercise most aspects of the uncertainty guidance: parametric, modeling, and completeness
- Also provides examples of how compensatory measures can be used to address modeling uncertainties

A.1 – Scope of Results Needed

- Based on RG 1.177, Requires
  - ΔCDF, ΔLERF, ICCDP, ICLERP
- Considered At-power Only, Due to AOT Being Evaluated
- ΔCDF, ΔLERF maintained in Region III, so total CDF/LERF not required

A.2 – Scope of Risk Assessment

- Utilizes the Insights from the Internal Events PRA to Identify Important Risk-related Functions of RHR
- Quantitative Treatment (PRA) of Internal Events, Internal Floods, Internal Fires
- Quantitative Screening of Seismic
- Qualitative Screening of Other Hazard Groups

A.3 – Comparison to Acceptance Guidelines

Base Case Results Presented to Decision Maker

Figure of Merit	Total Value	Acceptance Guideline	Below Acceptance Guideline?
CDF_{NEW}	1.65E-05/yr	<1.0E-04/yr	Yes
ΔCDF	2.73E-07/yr	<1.0E-06/yr	Yes
$ICCDP_A$	1.15E-07	<5.0E-07	Yes
$ICCDP_B$	4.08E-07	<5.0E-07	Yes
$LERF_{NEW}$	<1.0E-05/yr	<1.0E-05/yr	Yes
$\Delta LERF$	<1.0E-07/yr	<1.0E-07/yr	Yes
$ICLERP_A$	<5.0E-08	<5.0E-08	Yes
$ICLERP_B$	<5.0E-08	<5.0E-08	Yes

A.3 - Potential Sources of Model Uncertainty - Internal Events

- Based on identification of the significant contributors to the results, the following are identified as relevant to the application:
  - Viability of CRD injection post containment failure
  - Various Human Errors:
    - Failure to depressurize RPV
    - Failure to bypass containment isolation
    - Failure to cross-tie IA to PCIG
    - Failure to utilize CRD for RPV Makeup
  - LOOP failure to recover probabilities
  - Credit for RHRSW pump repair
  - Medium LOCA partition factor
  - No credit for maintaining ECCS injection post-venting

A.3 - Potential Sources of Model Uncertainty - Internal Fires

- Most of the Potential Internal Event Sources of Uncertainty Also Found in Internal fires
- Sources of Uncertainty Unique to Fire:
  - Scenario initiating event frequencies
  - General conservatism of fire scenario treatment

A.3 – Parametric Uncertainty Evaluation

Result	Internal Events		Internal Fires	
	RHR "A" Case	**RHR "B" Case**	**RHR "A" Case**	**RHR "B" Case**
Propagated Mean Values				
CDF_X	6.56E-06/yr	7.31E-06/yr	1.57E-05/yr	3.05E-05/yr
CDF_{BASE}	3.80E-06/yr		1.25E-05/yr	
$\Delta CDF = CDF_X - CDF_{BASE}$	**2.76E-06/yr**	**3.51E-06/yr**	**3.20E-06/yr**	**1.80E-05/yr**
Point Estimate Mean Values				
CDF_X	6.53E-06/yr	7.23E-06/yr	1.57E-05/yr	3.03E-05/yr
CDF_{BASE}	3.73E-06/yr		1.25E-05/yr	
$\Delta CDF = CDF_X - CDF_{BASE}$	**2.80E-06/yr**	**3.50E-06/yr**	**3.20E-06/yr**	**1.78E-05/yr**

A.3 – Sensitivity Studies on Model Uncertainties

- Human Error Probabilities (HEPs) as a class
- Frequency of medium LOCAs that are too big for CRD makeup capabilities
- CRD survivability following containment failure scenarios
- Fire scenario initiating event frequencies

A.3 – Insights for Decision-makers

- Risk results below acceptance guidelines for all but two sensitivity cases (key sources of uncertainty):
  - Human Error Probability (HEP) Development
  - CRD survivability following containment failure
- Potential Compensatory Measures:
  - Perform pre-shift briefs on potentially important human actions
  - Pre-alignment of alternate injection systems as containment pressure increases.
  - Pre-shift briefs identifying the important fire scenarios or roving fire watches in areas with increased sensitivity

Future Work

- Two-day public workshop scheduled for May 5 and 6, 2009
- Gather insights and lessons learned from workshop
- Expand to address other scope items
- Expand to support new and advanced reactors

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DG-5021
Managing the Safety/Security Interface

ACRS Presentation

February 5,2009

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Discussion Topics

- Power Reactor Security Rulemaking
  - Currently with OMB (since 12/19/08)
  - Provided status to ACRS last summer
- Portions requiring ACRS review
  - § 50.54(hh) "Mitigative Strategies and Response Procedures for Potential or Actual Aircraft Attacks"
  - § 73.54 "Protection of Digital Computer and Communication Systems and Networks"
  - § 73.58 "Safety/Security Interface Requirements for Nuclear Power Reactors"
- This briefing focuses on the guidance for § 73.58
  - Staff requests ACRS to provide the Commission its views on acceptability of this regulatory guide

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

§ 73.58 Safety/Security Interface

- Addresses part of UCS petition (PRM 50-80)
- Makes explicit what is already implicitly required by regulation
- (b) Requires licensees to assess/manage potential for adverse interactions between security ↔ safety
- (c) Scope – Planned and emergent activities
- (d) Conflicts – Communicate conflicts and take compensatory and mitigative actions

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

§ 73.58 Safety/Security Interface

- Published in Federal Register July 24, 2007
- Public Meeting held; comments received
- Several public meetings held between Sept. 2009 and January 2009 to resolve and disposition comments

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RG-5021
Managing the Safety/Security Interface

- Focus of the guide:
  - The types of controls and process intended for review
  - Review of current management controls & processes
  - The program areas that should be considered

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RG-5021
Managing the Safety/Security Interface

- Focus of the guide:
  - The types of planned or emergent activities that should be considered
  - The screening process for safety/security interface
  - Training that is required

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary

- Staff requests ACRS provide its opinion on acceptability of the final rule provisions to the Commission

Digital Upgrade of the Oconee Reactor Protection System and Engineered Safety Features

Presented by: NRR / EICB

Pat Hiland Director DE
Bill Kemper Branch Chief EICB
Rich Stattel Technical Reviewer EICB

February 5, 2009 12:45-2:45 P.M.

Presentation Outline / Agenda

- **Introduction**
- **Overview of Oconee License Amendment Request (LAR)**
- **Diversity and Defense in Depth**
- **Communication**
- **Changes to TXS Platform**

Introduction
TXS Platform & Oconee LAR

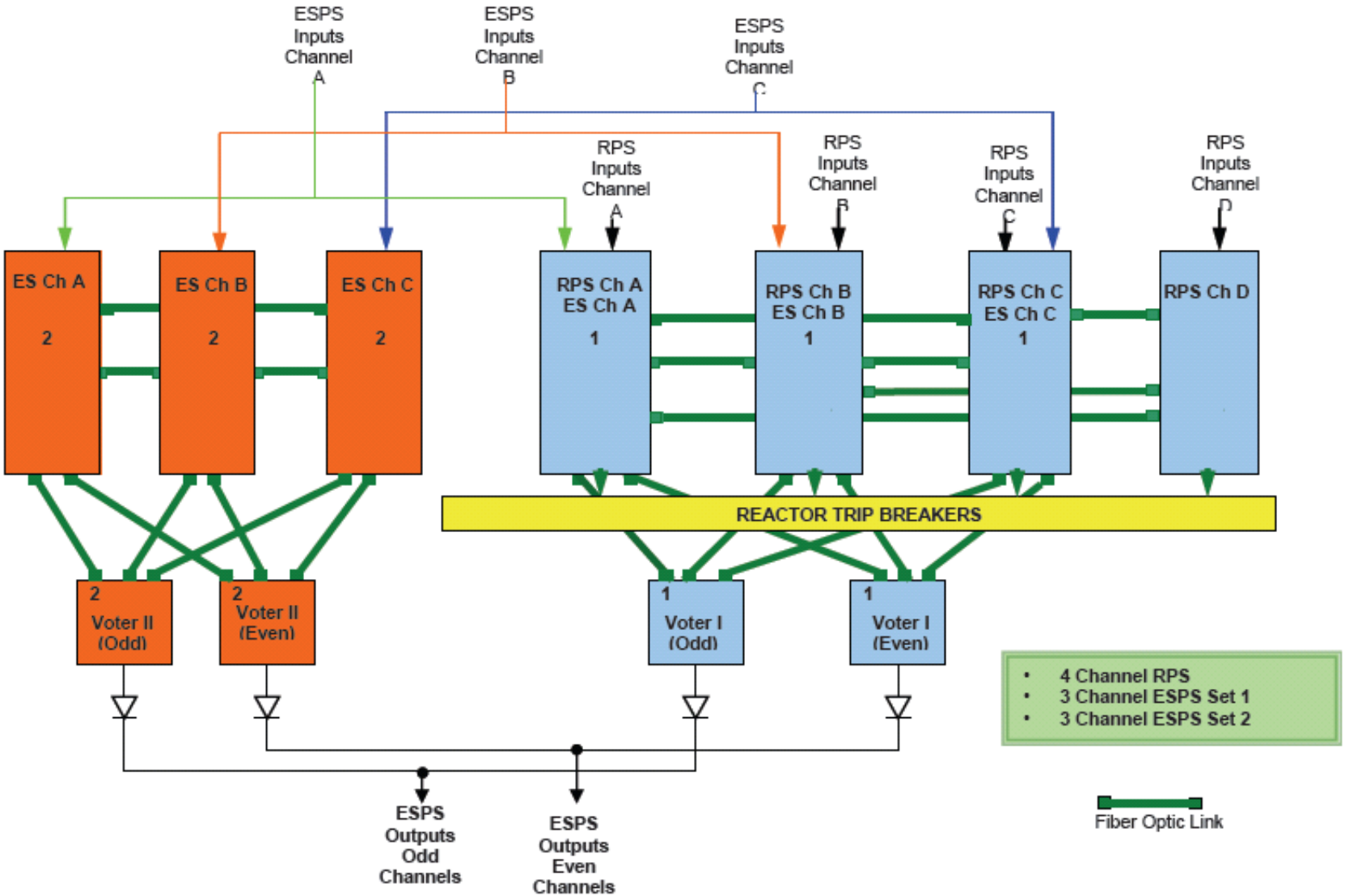
- On January 31, 2008, Oconee submitted a LAR to replace the existing analog RPS and ESPS systems with a Digital RPS/ESPS system.
- The Safety Evaluation Report for the Teleperm XS (TXS) Topical Report was Issued in May 2000.
- The Oconee Digital Reactor Protective System / Engineered Safeguard Protective System (RPS/ESPS) is Based on the TXS Platform.
- As part of the NRR acceptance review process the NRC accepted the LAR (April 24, 2008) for review and documented six issues that could present a challenge to approving the LAR:
  - (1) Diversity and Defense-in-Depth (D3)
  - (2) Bi-Directional Communications
  - (3) AREVA Software Program Manual (SPM)
  - (4) TXS Platform Changes since the approval of the TXS topical Report
  - (5) Verification and Validation (V&V) program / process
  - (6) Software Tools used for V&V
- The status of the review is considered to be Pre-Decisional Information.

Introduction
Review Process

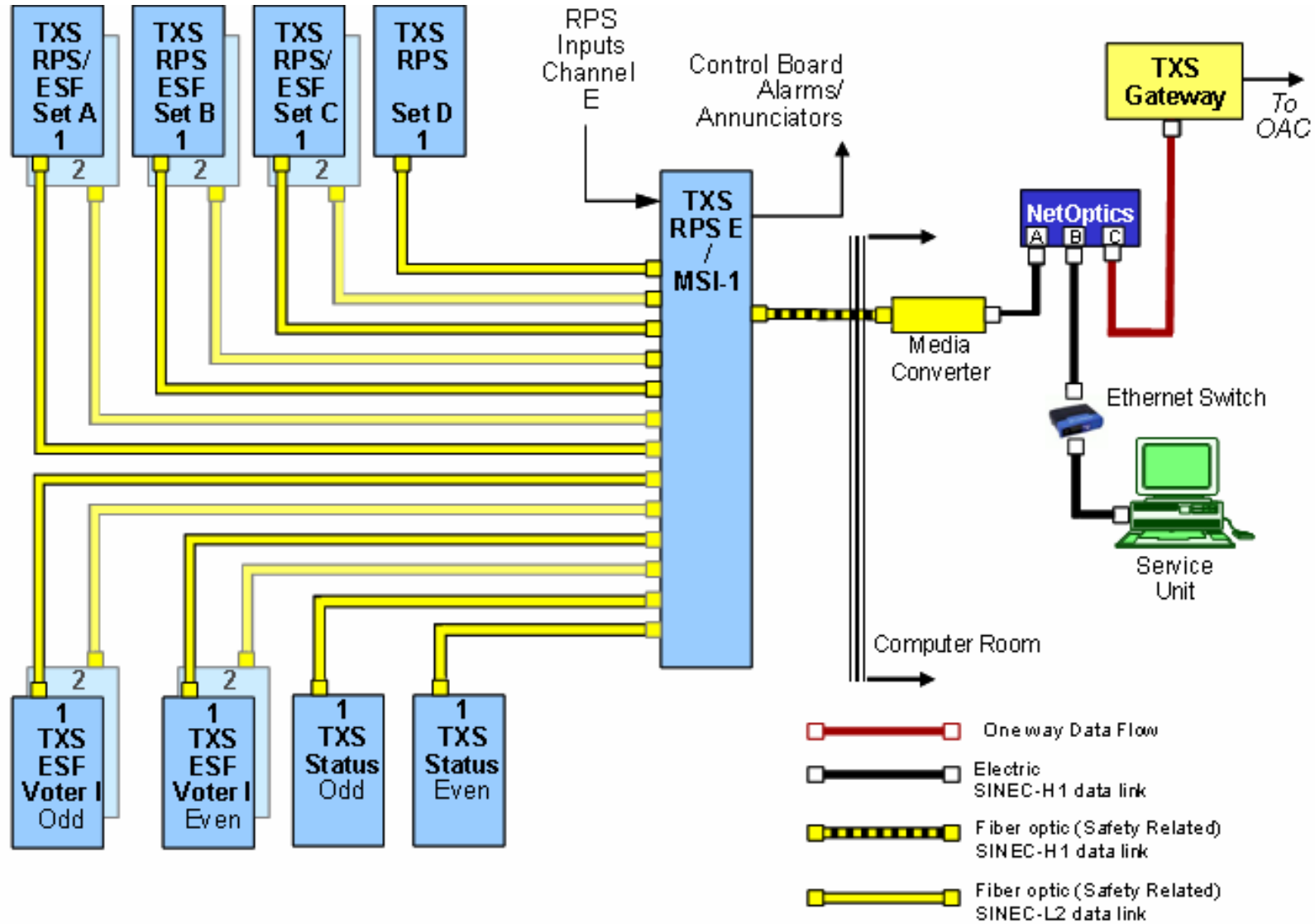
- **EICB is conducting the review in accordance with Standard Review Plan (SRP) Chapter 7 (NUREG-0800, Chapter 7) and LIC -101.**

- **Interim Staff Guidance (ISG) was developed by the Task Working Groups (TWGs) of the Digital I&C Steering Committee. Specifically:**
  - **ISG#1 is being used to guide the review of cyber security aspects.**
  - **ISG#2 is being used to guide the review of Diversity and Defense-in-Depth aspects.**
  - **ISG#4 is being used to guide the review of Communications aspects**

Overview of Oconee Application
RPS/ESPS System Architecture



Overview of Oconee Application
Safety to Non-Safety Communication Architecture



Diversity and Defense in Depth (D3)
Guidance

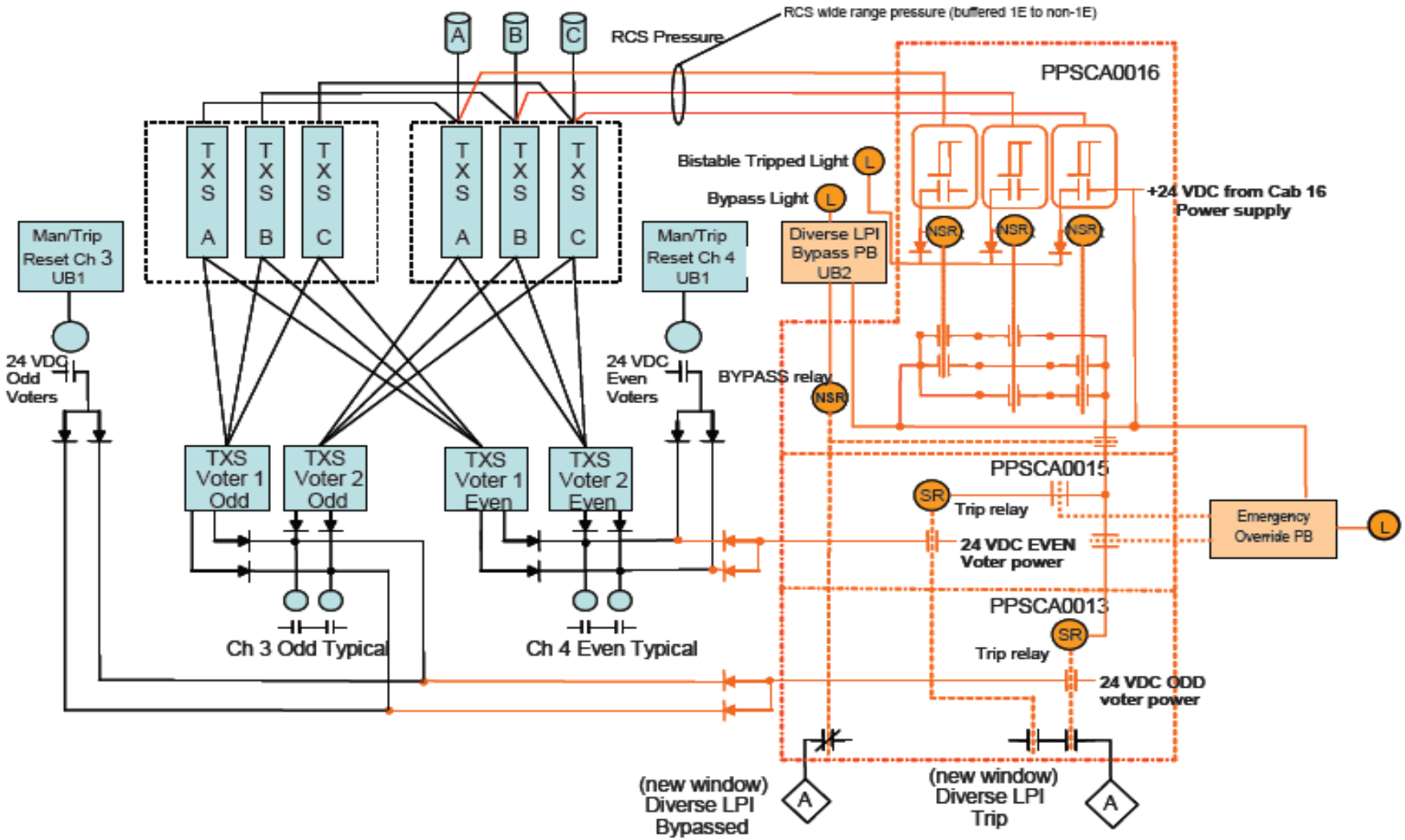
- **Guidance for Diversity Assessment**
  - **SRM to SECY-93-087 Item II.Q**
    Establishes NRC policy for Diversity and Defense in Depth
    - **NUREG/CR-6303**
      Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems
    - **Branch Technical Position (BTP) 7-19**
      Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems
    - **Interim Staff Guide (DI&C-ISG-02)**
      Diversity and Defense-in-Depth Issues

Diversity and Defense in Depth
Oconee Diversity Solution

- **The Oconee ESPS Safety System Actuations**
  - **Reactor Building Cooling and Isolation**
  - **Reactor Building Spray**
  - **High Pressure Safety Injection Actuation System**
  - **Low Pressure Safety Injection Actuation System**

- **Oconee's New Automatic Diverse Actuation Systems**
  - **High Pressure Injection DAS (HP DAS)**
  - **Low Pressure Injection DAS (LP DAS)**
- **ATWS – The Oconee existing design already includes a diverse Reactor Trip system.**

Diversity and Defense in Depth
Diverse LPI Actuation System (DAS)



Diversity and Defense in Depth
Manual Operator Action

- **The new Oconee Digital Protection System will provide a plant response that does NOT require any manual operator actions for at least 30 minutes for all chapter 15 accidents with the single exception of a manual reactor trip during a Small Break Loss-Of-Coolant Accident (SBLOCA)**
  - **This action is required within 2 minutes of the transient.**
  - **Oconee already has a requirement to trip the reactor and reactor coolant pumps within 2 minutes during an SBLOCA (Minimum Subcooled Margin Requirement)**
  - **Therefore, even though this manual action is required in much less than 30 minutes, it is a reasonable exception to the D3 Interim Staff Guidance criteria.**

Diversity and Defense in Depth
Current NRC Assessment (Pre-Decisional)

- **The inclusion of Diverse High Pressure and Low Pressure Injection DAS systems into the Oconee design provides an acceptable degree of diversity to address common cause failures of those Digital actuation channels.**
- **Manual Actions >30 minutes to address CCF's of RPS/ESPS actuations are compliant with ISG2 and provide adequate means of response to a Software Common Cause Failure.**
- **The Manual Action of 2 minutes for the Reactor Trip in the case of a Small Break LOCA is acceptable.**

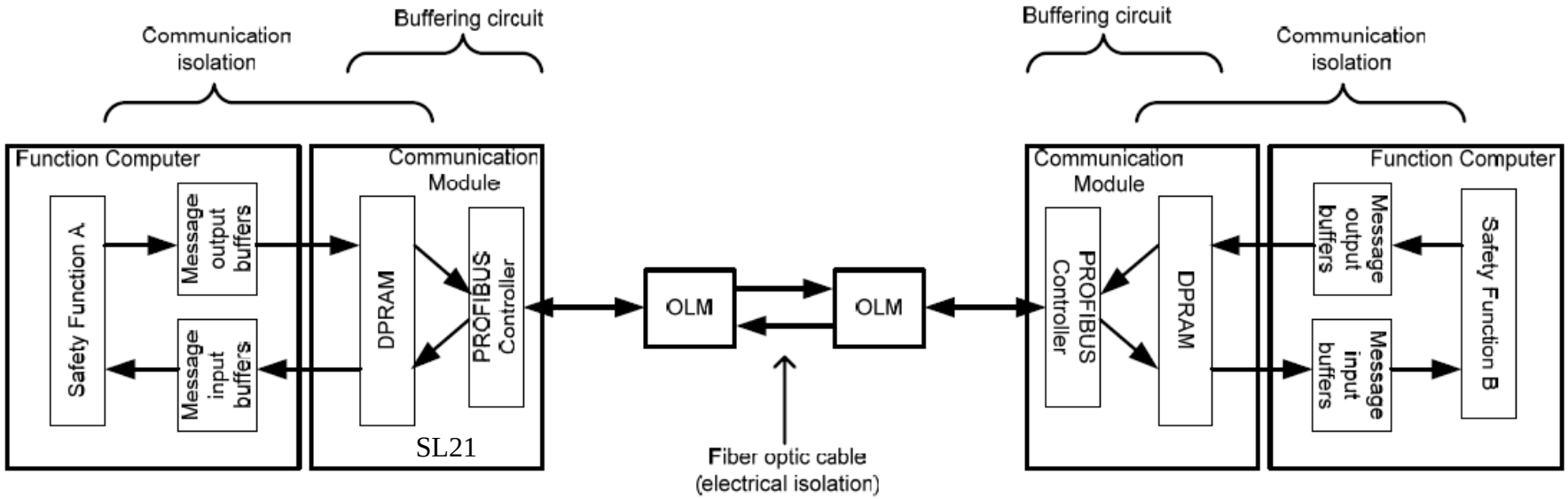
Diversity and Defense in Depth
Path Forward

- **Duke provided the necessary documentation to support the stated conclusions.**
  - **Setpoints for the High Pressure and Low Pressure Injection Diverse Actuation Systems to support the Diversity and Defense in Depth strategy.**
  - **Description of the built-in conservatism of the D3 analysis program.**
- **The NRC staff is in the process of writing the D3 Safety Evaluation**

Communication
Guidance

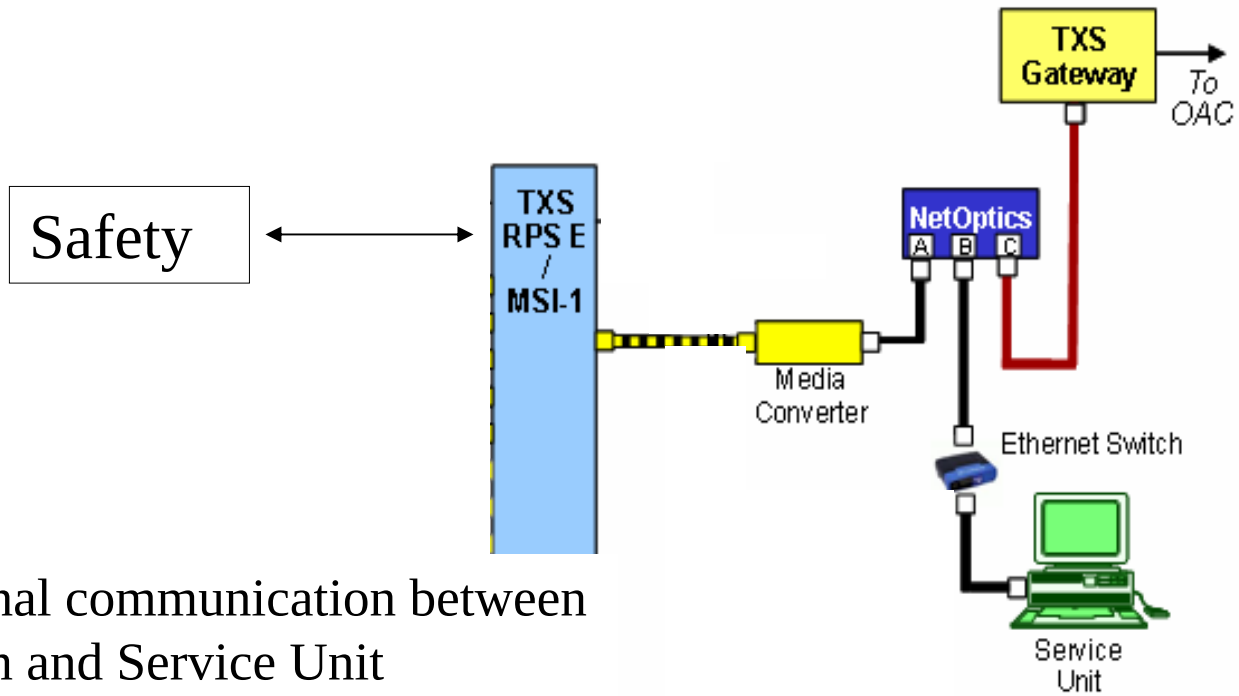
- **Guidance for Communication**
  - **IEEE 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"**
  - **IEEE 7-4.3.2, "Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Station"**
  - **ISG#4, "Highly Integrated Control Rooms-communication Issues"**

Inter-Channel Communications
Oconee Solution



- Provides electrical isolation between Safety Channels
- Provides communication isolation between Safety Channels
- Deterministic in nature

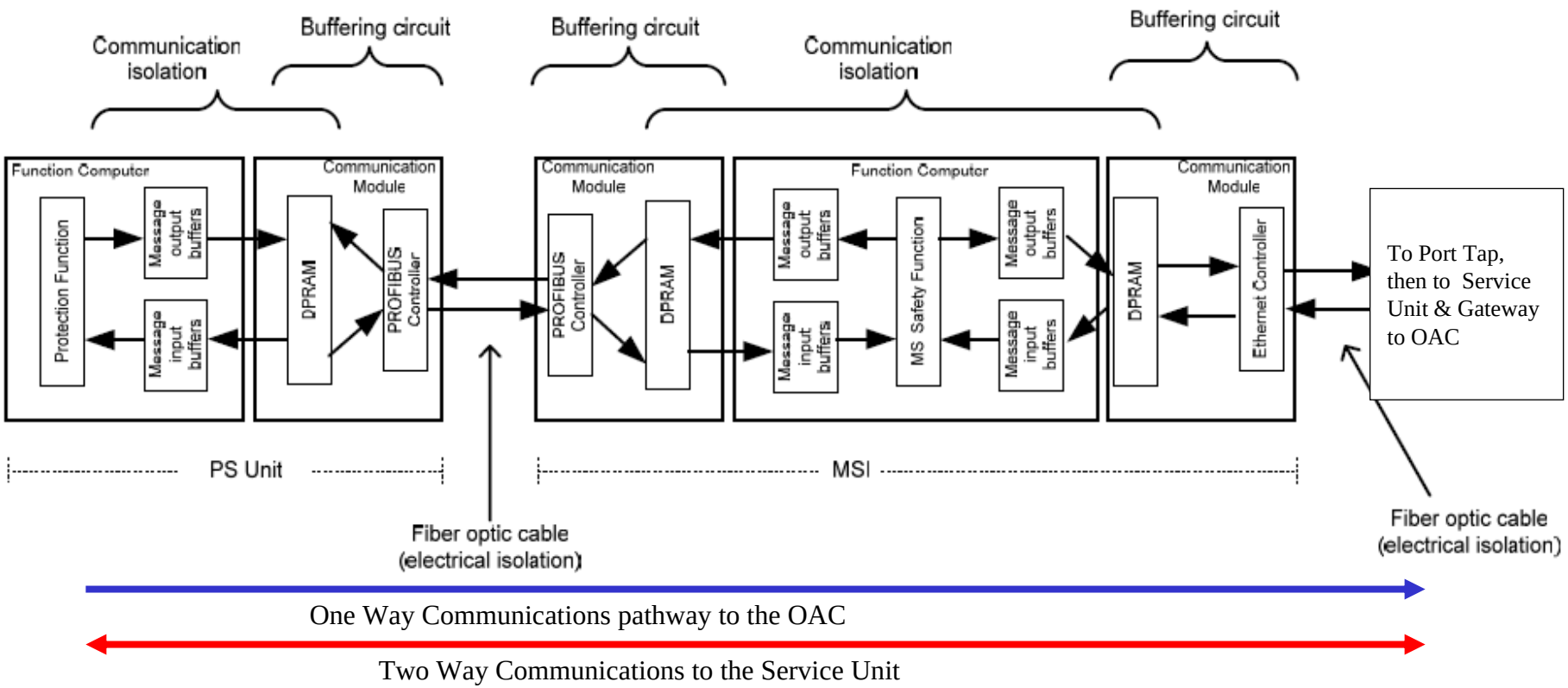
Communication
Between Safety and Non-safety Systems



- Bi-directional communication between safety system and Service Unit

- One way communication between safety system and gateway to OAC

Safety to Non-Safety Communications
Oconee Solution



- Provides electrical isolation between Safety and Non-Safety Systems
- Provides communication isolation between Safety and Non-Safety Systems
- The MSI serves as a Safety to Non-Safety Boundary
- Deterministic in nature

Communication
Current NRC Assessment (Pre-Decisional)

- **The Oconee License Amendment Request appears to adequately address each of the twenty adherence points listed in ISG#4 with the exception of one Item.**
  - **ISG#4 Item 10 - Deviation in Oconee LAR**
    - **The Service Unit will be connected to the MSI during plant operations.**

- **The Port Tap device appears to provide an acceptable one way communications solution for the SR to NSR communications pathway but not all of the supporting information has been accepted by the staff.**

Communication
Path Forward

- **The NRC review staff is currently documenting the evaluation for each of the 20 ISG#4 adherence points in regard to the Oconee Design.**

- **Oconee will provide additional proprietary information to support the stated functionality of the Port Tap device. As an alternate the Staff may conduct an audit at the vendor facility.**

Changes to TXS Platform Criteria

- **The Teleperm XS (TXS) Topical Report and Safety Evaluation were issued in May of 2000**

- **Since then, numerous changes to the approved platform were necessitated due to obsolescence and advancements in digital technology. These changes include:**
  - **Hardware**
  - **Software**
  - **Procedure**

- **A Review of these changes to the approved platform is necessary to assure that the changes are acceptable.**

Changes to TXS Platform
Significant Hardware Changes

- The Safety function processor was replaced with an updated safety function processor
- The Communication module was changed
- Some I/O modules were upgraded
- A change was made to the Subrack

NOTE: All of these changes were incorporated to enhance the performance of the platform.

Changes to TXS Platform
Significant Software Changes

- **Software types in TXS Topical Report**
  - **SPecification And Coding Environment (SPACE) - Tools**
  - **TXS Platform Software**
    - **Operating System (OS)**
    - **Run Time Environment (RTE)**
- **Software Changes**
  - **Updated SPACE**
    - **Ported SPACE to new Operating System**
    - **Changed Database Management System**
  - **Updated TXS Software (Necessitated by the Hardware Changes)**
    - **Operating System (OS)**
    - **Run Time Environment (RTE)**

Changes to TXS Platform
Significant Procedure Changes

- **Several changes were made to the plans and procedures that were addressed in the TXS Topical Report.**
- **These changes were made in order to maintain the high quality development process.**
  - **Procedure changes were required to:**
    - **Add Detailed Requirements**
    - **Address Plant Specific Action Items called for by the TXS Topical Report SER.**
    - **Improve configuration management control**
  - **Procedure Evaluations are being conducted on a sampling basis.**

Changes to TXS Platform
Path Forward

- **Hardware Changes**
  - **Review is Complete**
  - **Sample of hardware test reports to be reviewed**
- **Software Changes**
  - **Review to be completed by April 2009**
  - **Sample of software changes to be reviewed**
- **Procedure Changes**
  - **Review is Complete**
  - **Sample of procedure changes to be reviewed**

Overall Summary

- **Summarize path forward D3**
  - **Duke has provided all of the necessary documentation to support the Oconee D3 Position.**
  - **The Staff is reviewing this documentation and is in the process of drafting the Diversity (D3) portion of the Safety Evaluation.**
- **Summarize path forward Communications**
  - **The NRC review staff is currently documenting the evaluation for each of these 20 ISG#4 positions in regard to the Oconee Design.**
  - **The Staff needs to evaluate the NetOptics device technical basis.**
- **Summarize path forward TXS Changes**
  - **The review of the hardware and procedure changes is complete**
  - **Review of the software changes is still in progress**
  - **Samples of the changes will be reviewed.**

Backup Slides
RPS Relay Voting