Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, August 20, 2009

Work Order No.: NRC-3021 Pages 1-344

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.
Washington, D.C. 20005
(202) 234-4433

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, as reported herein, is a record of the discussions recorded at the meeting.

This transcript has not been reviewed, corrected, and edited, and it may contain inaccuracies.

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS SUBCOMMITTEE MEETING

+ + + + +

THURSDAY

AUGUST 20, 2009

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

SUBCOMMITTEE MEMBERS PRESENT:

GEORGE APOSTOLAKIS, Chairman

SAID ABDEL-KHALIK, Member

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR., Member

JOHN D. SIEBER, Member

JOHN W. STETKAR, Member

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU, Cognizant Staff Engineer

NRC STAFF PRESENT:

DEBRA HERRMANN

MICHAEL WATERMAN

BILL KEMPER

RUSSELL SYDNOR

SUSHIL BIRLA

PAUL REBSTOCK

STU RICHARDS

JEANNE DION

ALAN KURITZKY

ANTONIO DIAS

ALSO PRESENT:

RAY TOROK

VICK FREGONESE

LOUIS CHU

T A B L E   O F   C O N T E N T S

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

(8:29 a.m.)

CHAIR APOSTOLAKIS: We are back in session. I understand Mr. Torok wants to finish a few things.

So what are you going to do, Ray?

MR. TOROK: I was asked just to touch on the final wrap up from our presentation, the part that you missed. That doesn't include any of the details of the DAS evaluation or that discussion. It is just the final comments from it. Right, Christine?

MS. ANTONESCU: Right, correct.

MR. TOROK: We want to do this so we can get to the next presentation.

CHAIR APOSTOLAKIS: So you are on number 57?

MR. TOROK: That's right.

CHAIR APOSTOLAKIS: Okay, go ahead.

MR. TOROK: This of course wraps up Dave's discussion of his DAS results. There was a lot of detail discussion. Your colleagues can fill you in on that. It was really good, actually. And it showed that this group had read the reports and read them very carefully, which was very good.

Anyway, the bottom lines are first, we

believe it is possible to generate useful risk insights right now, using existing PRA techniques and I think we showed you an example of how that could be done yesterday, right down to the low level details.

Now in regard to the actual analysis we did and the results of that analysis, it was for this automated DAS. And the results of the analysis basically were that the DAS, as analyzed for the events it applied to was shown to have little or no benefit and for a number of reasons. One of them is, it turns out the DAS would just be applied to low frequency events, so-called rare events, large pipe breaks and so on for which there are already significant provision measures in the form of pipings built to code and inspected and all those kinds of things. And there is also significant mitigation in the form of high quality ESFAS and that is really what was driving the results of the analysis.

Oh, and one more thing, those two pipe break and the common cause failure in the ESFAS are independent and they have to stay independent. And if you have all that, then it turns out that the results of the risk analysis is going to be that the DAS is not going to have much benefit. It may have some small increase in due to the potential spurious actuations.

In general, the conclusions were insensitive to the assumptions that went into the analysis, especially the controversial assumptions about the level of modeling detail and the assumed failure probabilities.

And another sort of overall conclusion when you step back from that analysis and look at the results, you conclude that if you are looking for where a DAS is going to be beneficial or adding defense in depth, it is going to have more benefit for high frequency events than low frequency events.

So, those were the technical conclusions. Now, in terms of recommendations based on these conclusions, we are hoping that you will encourage the staff and industry to continue to develop PRA methods and to apply them now where it is possible to do that. And there is some indication here of what that means. Where the results are insensitive to the assumptions, that is a good indication. And we think they are applicable both for licensing actions and for specific analyses such as the one that was done for automated DAS.

It may also be helpful to consider revising the BTP-19 guidance such that it considers both frequency and consequences when it is looking at adequacy, defense in depth and adequacy of protection against common cause failure. What that means is, it would allow a graded approach in which both the solution and the protective measures are proportional, in some sense, to risk.

Let's see. Oh, and we also think it is important, but one of the things that the PRA analysis is telling us is that prevention measures are really important. So we shouldn't be talking about just mitigation when we talk about protection against common cause failure. Really, we should be talking about both. So we really encourage that.

Now the last bullet on there refers to, and I think I brought this up at the beginning of the talk yesterday, refers to a number of ACRS statements that are out there in various places, basically expressing skepticism in terms of how far you can go with risk methods for digital systems at this time.

And what has been somewhat problematic is some of those statements have been interpreted to mean that the kind of analysis we did is either inappropriate or impossible. And in light of what we showed and discussed yesterday, we think it is possible and you can get reasonable results. And we would hope that ACRS would take a look at those statements and decide whether some additional clarification may be appropriate. So that was a recommendation based on the DAS results.

And all we have now is a recap of the high level conclusions for each area we talked about. In operating experience we said from what we looked at, software has been no more problematic than other common cause failure contributors, which means the measures being taken to prevent those kinds of problems in software are working pretty well. What we ought to do is capture them and make sure we understand what they are and make sure we keep doing them.

In regard to digital failure modes, we think, basically that this notion of mechanisms versus modes versus effects needs to be taken into consideration in all of these analyses so that we use those terms and those concepts at the level of abstraction that is appropriate for the analysis being done.

Let's see. And specifically in regard to PRA, it appears that failure mechanisms are typically not of great importance in terms of PRA modeling. They may be helpful when you are trying to assess failure probability but you shouldn't expect to see individual failure mechanisms probably modeled in a PRA model.

In regard to, oh I just said this about prevention and mitigation. Both are important. And as I said, PRA insights are possible now. Let's keep doing that.

So this is the final recap here. We are basically requesting ACRS concur with our findings where it is appropriate to do that. One of them is motherhood. It says, continue to gather and apply OE lessons learned on failures. But we are a little more specific. The causes, the corrective actions and the preventive measures are really important to focus on those things.

And also we think it is important to develop a consistent taxonomy or language, terms and definitions for doing this, because those things are very important in terms of affecting the results. And we are never going to see much agreement in terms of overall results until we get together on what some of these terms mean and what makes sense in terms of binning.

For defensive measures, we think it is really important to credit defensive measures. Not in regard to showing that common cause failure is not credible or anything like that. It is to credit defensive measures in terms of protecting against common cause failure as a very effective mechanism for doing that and to use it in concert with diversity attributes, where that makes sense. What you would ideally like to do is use some combination of those things and for specific instances, you would use whichever one is more appropriate.

I already said this. Let's use risk methods more where it makes sense. And then the last thing there is just encouragement to, I am hoping you will encourage staff to participate more in these technical exchanges to resolve issues with technical discussions. Like it would have been nice to do that on the OE and DAS work. We were unable to do that. The good news is now Dan Santos has been doing a lot of work to get this MOU in place between EPRI and Research so we think that is going to work better in the future.

I think that is all I had. Did I get through it fast enough?

CHAIR APOSTOLAKIS: Any comments from the members?

(No response.)

CHAIR APOSTOLAKIS: Thank you, Ray.

MR. TOROK: Thank you.

CHAIR APOSTOLAKIS: I understand the staff has a few comments to make. Would you please come here? You have 40 slides to make a few comments?

I hope there will be enough time to discuss the plan.

MEMBER BROWN: There will.

CHAIR APOSTOLAKIS: Okay, would you tell us who you are for the record?

MS. HERRMANN: Debra Herrmann, NRO, Division of Engineering.

MR. WATERMAN: I'm Mike Waterman and I am in the Office of Nuclear Regulatory Research in the Division of Engineering.

MR. SANTOS: Dan Santos, Office of Nuclear Regulatory Research, Division of Engineering.

MS. HERRMANN: We are here to present the NRC comments on the EPRI reports. EPRI requested that we review both the CCF and the DAS reports. All four offices participated in this review, NRR, NRO, Research, and NMSS. Multiple divisions participated in the review. In NRO, we had DSRA, DCIP, and NDE. So, it was a concerted effort and we appreciate the opportunity provide comments to EPRI.

We look at this as input to the collaborative research, which will be discussed later during the research plan.

CHAIR APOSTOLAKIS: So EPRI has seen these comments?

MS. HERRMANN: Pardon me?

CHAIR APOSTOLAKIS: They have seen these comments that you are about to make?

MS. HERRMANN: We discussed the comments at the all-day meeting with EPRI about two weeks ago.

CHAIR APOSTOLAKIS: But they have not seen the report or anything?

MS. HERRMANN: The handouts, no.

CHAIR APOSTOLAKIS: Okay.

MS. HERRMANN: NRC policy in this area and how it was developed was documented in the letter from Jack Grobe to NEI last November. Our policy has not changed. Today we are providing technical comments on the EPRI reports.

CHAIR APOSTOLAKIS: NRC policy. Which policy is this?

MS. HERRMANN: This is the various SECY papers. The SRMs, the BTPs that were all listed yesterday regarding D-3.

CHAIR APOSTOLAKIS: Okay. Then we are not to assume that we remember too much.

MS. HERRMANN: Okay. It was a long day.

The EPRI report makes the statement that software is not a significant source of CCFs. We don't believe that is the correct way to frame the question, particularly because it doesn't address a key problem and that is the lack of understanding of digital system failure modes, particularly as they relate to the nuclear industry.

The primary concern when migrating from digital technology is that a new source of failure may be introduced. And that is, software CCFs The other sources of CCFs, as we discussed yesterday, hardware, human error, etcetera, remain essentially the same. So we think you need to reframe the question to what is the prevalence of software CCFs in digital systems, so that you can understand the appropriate prevention, mitigation and verification activities that need to be undertaken.

We believe that determining the percentage of software CCFs as to the total CCFs experienced in the plant is not as useful to a digital system engineer.

CHAIR APOSTOLAKIS: And why is that?

MS. HERRMANN: Because it dilutes the

data. In other words, if you are a digital system engineer designer, you want to know the failure modes of a digital system. You are not as interested in the external events.

I think a good analogy is the EPRI study is an epidemiologic study, whereas, if you are trying to determine the prevalence disease in a specific ethnic group, you only sample data from that ethnic group.

MEMBER STETKAR: Didn't they only look at failures in digital systems? They didn't look at software failures out of all common cause failures in the plan. It was software failures out of digital system common cause failures, as I understood their analysis.

MS. HERRMANN: Yes, but if you go through the --

MEMBER STETKAR: It isn't an epidemiological study to me.

MS. HERRMANN: It is but what we are saying is that you need a pathological study. Because if you look at the 322 events, only 24 of them were classified as software failures.

MEMBER STETKAR: Okay, that is classification. That is your classification versus mine.

MS. HERRMANN: Right.

MEMBER STETKAR: That is a different issue.

MS. HERRMANN: Right.

MEMBER STETKAR: You are talking about the scope of the underlying data and what it is trying to tell us.

MS. HERRMANN: Yes.

MEMBER STETKAR: Okay.

MS. HERRMANN: It is the classification, the data-binning error.

MEMBER BROWN: Well, I am hesitant. I guess I don't understand the difference between bullets four and five. In one you say the question that NRC needs to answer is the prevalence of CCFs in digital systems. Then you say determining the percentage of software CCFs is of no interest.

MS. HERRMANN: Plant-wide. Outside of the digital systems.

MEMBER STETKAR: They didn't try to do that.

MEMBER BROWN: All right.

MEMBER STETKAR: Did EPRI try to do that?

MS. HERRMANN: Well, if you look at a lot of the events, human error, other things that aren't software failure proper. And this gets back to the definitions, which we will get into later.

CHAIR APOSTOLAKIS: But that fraction of three point something percent they denied yesterday. I thought it was common cause failures, the fraction of common cause failures in software, digital software. And I asked them, you know, is the PRA guide going to use that and they said no.

But it was limited to software, as I remember.

MEMBER STETKAR: And in digital systems. The fraction of digital software failures versus motor-operated valve hardware common cause failures.

CHAIR APOSTOLAKIS: Now are you saying, Debra, we can't take digital software systems of different missions and do different things, and do what EPRI did? Maybe that it what you are saying.

MS. HERRMANN: No, what I am saying is that the focus should be on the software events, the 24 software events and not the whole pocket of the 322.

CHAIR APOSTOLAKIS: Oh, that I agree.

MS. HERRMANN: Yes.

CHAIR APOSTOLAKIS: That was broader.

Anyway, let's go on.

MS. HERRMANN: We talked about this one briefly yesterday, the separation of the 1E and the non-1E events and Mike is going to address this.

MR. WATERMAN: As you recall from our March 2008 meeting, Dr. Stetkar pointed it out first and I amplified his comment was that I don't think you can really segregate the non-1E and 1E systems because a lot of those process systems that are included in here were important for plant availability, which would have classified them up in a software integrity level scheme of around three our four if you used the scheme that was introduced in IEEE Standard 1012, 1996 and all future ones, where they use a software integrity level scheme to determine how much effort you put into the quality of the software product you are developing.

In the case of plant availability systems, the impact of the failure for plant availability is that the business is going to lose a lot of money. So that makes it a major, major event, if you will, if a plant shuts down. Because for example, feedwater, a digital feedwater system fails and you can't run a plant until they get it fixed. So as a consequence, you want a high level of quality to be put into that system.

But what we found in the EPRI report was they said well now, the 1E systems have a higher quality than non-1E and so you can't compare those. But actually, if you look at the data that was presented yesterday, for example in slide 19, which is non-1E software mechanisms and you compare that with slide 17, which is the 1E non-failure mechanisms, instead of just saying how many software common cause defects out of the total number of common defects, if you compare software common cause failures out of the total number of non-1E events, you find that you get about one failure per seven events in non-1E systems. And if you go over and you do the same comparison of software common cause failures out of total 1E events, you get about one software common cause failure in every eight events.

So, one-eighth, one-seventh, seems to me that they are fairly equivalent. So I don't know that you can actually segregate your 1E stuff from your non-1E stuff, which was one of the things that was done in the report is there is a reason for only considering the 1E software common cause.

CHAIR APOSTOLAKIS: So are you saying that the quality assurance requirements during the design phase for 1E and non-1E system is about the same?

MR. WATERMAN: Well, the quality assurance requirements are probably more stringent for 1E.

CHAIR APOSTOLAKIS: Yes.

MR. WATERMAN: But performance of that may not be equivalent to the requirement.

CHAIR APOSTOLAKIS: So the quality --

MR. WATERMAN: The performance proves process. And so it is one thing to lay down a set of requirements and say this is how we are going to build this system, it is quite another to actually build it.

For example, you know, in an extreme example, you can say here is all the requirements to build a Boeing 747. And then you take ten people and tell them to build it.

CHAIR APOSTOLAKIS: But I remember, I am playing the devil's advocate here, years ago when the stuff came with the first guidance on the digital I & C, the whole focus was on the design cycle or process. And there was an implicit assumption or presumption that if you control the process, the product will be highly reliable. But now you are saying even if you control your process as much as you want, I don't know about the performance.

Sounds like a little bit contradictory to me.

MR. WATERMAN: Well, process and performance are two different things. Process is what is promised to be done. Performance is how well that promise is met.

CHAIR APOSTOLAKIS: So was the Agency misguided then? Yes, sir?

MEMBER BROWN: Years ago, we had a concern relative to the ability on quality assurance processes for software development and this was 20 years ago.

So we did some analysis and found when you are trying to make sure software is right, it is very, very difficult. And you kind of achieve a level of defects that are still there based on time you put into it. And the commercial systems have these. They just go troubleshoot, you know, they remove, remove, remove until the defect level. This was 20 years ago. I can't say what is going on today.

When you get down, you are only finding a few things every now and then, and define every now and then as whatever you want, they quit. It is just well, that is good enough. We will just let the other stuff pop up. You get to that same point where you are doing the higher level. More fail, more detailed type stuff.

It is just a question of whether software can be done and troubleshot and defects removed that well.

CHAIR APOSTOLAKIS: That is just the process. I mean there is extensive testing afterwards.

MEMBER BROWN: But you can't test all the points. That is the problem. You cannot test all the input and output conditions.

MR. HECHT: Isn't one of the issues the difference between the 1E and the non-1E systems, the architecture and the degree of complexity, and whether or not to use asynchronous versus a deterministic time slot?

MR. WATERMAN: That is true but if you look at the data, they appear to be failing at about the same rate.

CHAIR APOSTOLAKIS: Which is what some people have been saying about safety-related and non-safety related components for a long time.

MEMBER BLEY: But there is a related thing. I have said this to them yesterday and I will say it to you today. It doesn't seem to me it does much good to talk at that gross aggregate level. When we get down to parsing out what we were called yesterday failure mechanisms, at that level, you can tell whether the failure mechanisms apply to the one you are interested in or not. And so you can use the data from both if you have a good categorization scheme to go after one of those mechanisms. And I think it is about time we started doing that.

And if you look at those old Idaho National Laboratory, they called them risk studies but they went back at operating data and something seemingly simple like a diesel generator. They broke into its pieces and showed that some tests tested one part, some tests test the other part. And you can't just use general data from everywhere. You have to kind of break your data into modules, too and fit into those modules of your subsystem.

So it seems to me we are at the point that it is time to start looking a level deeper and trying to match up those failure mechanisms and draw the data from whatever source is appropriate for each one of them.

CHAIR APOSTOLAKIS: Which by the way is the central theme also, that old common cause failure study. We did EPRI and NRC where they said, you know, here is what happened in the past. We are not going to give you any statistical information. When you analyze a particular system, go back, look at each one of these and declare this one is applicable, this one is not, which is essentially what Dennis is saying. You go back to the mechanism earlier.

So, that sounds very reasonable to me.

MR. WATERMAN: And not all non-1E systems are a single-point vulnerability. For example, variable frequency drives in BWRs recirc pump A train, recirc pump B train. Right? Those are two different systems.

And if you take a look at the Browns Ferry event that occurred on March 26, 2003, that was a common cause failure. Two different computers. The recirc pump A tripped because a microprocessor software fold led the system to believe there was a ground fault. It tripped pump A. Pump A went offline, the reactor down-powered to run on pump B. Pump B microprocessor software, and this was an event that was reported by INPO, microprocessor software error tripped pump B before the operators could fix pump A.

That is a case where that is essentially the same thing as a Class 1E system. Right? You have independent trains running the same software.

Well, Mike, so you can't just say well we will take all the class, the non-class 1E as segregate for the class 1E. You have to look at the architecture and determine where we have redundant architecture, you have to lump it all together.

CHAIR APOSTOLAKIS: What is the -- I mean, okay, you made this comment. What is the practical implication of this?

MS. HERRMANN: That is on the next page.

CHAIR APOSTOLAKIS: It is? I guess you figured out the question was coming. Right?

MS. HERRMANN: Right.

MR. WATERMAN: Forty-nine events were related to the 1E systems, such as reactor protection, this is what EPRI stated, engineered safety features, diesel load sequencer, post accident monitoring, etcetera. However, this is sort of misleading because you don't have really a lot of digital reactor protection systems out there. As a matter of fact, I think Oconee is going to be the first one that is actually putting in a full digital RPS, ESFAS.

And so you could say well what about Eagle-21? But Eagle-21 is not totally digital. Just only parts of it are digital.

So there really isn't --

MEMBER BROWN: That is not all there.

MEMBER BLEY: Yes. It's not all there.

MR. WATERMAN: So there was really a low level of safety-related digital systems in current operating reactors. You could probably a back of the envelope calculation, actually, estimate how many digital safety systems are in our plant fleet. And it would probably work out to maybe, I don't know, a thousand, total, just for a ballpark number.

CHAIR APOSTOLAKIS: These are still comments. My question was in terms of practical applications, what do you want me to do? Okay, you disagree with EPRI. What are we to do?

MR. WATERMAN: I think what we need to do is recategorize.

CHAIR APOSTOLAKIS: I'm sorry?

MR. WATERMAN: I think what we need to do is recategorize those failures.

CHAIR APOSTOLAKIS: And go to the mechanisms?

MR. WATERMAN: And go and look at the architecture also. What kind of things can have common cause failures because, in an architecture that has redundant transfers.

MR. SANTOS: This is Dan Santos from the Office of Research. The answer is we are going to undertake a research project that will deeper look at that classification categorization of failure modes and detailed assessments of the systems. So we will discuss that in more detail later today. I am going to bring it up. That is where this is leading to.

CHAIR APOSTOLAKIS: Is anything, any results that EPRI presented yesterday, should I say no, this is not right because the staff disagrees, as a result of your comments?

MS. HERRMANN: It is not that we disagree with the results. I mean, they went through their methodology and the rationale for it. It's just that we believe that the question should be asked differently and we believe in a different categorization scheme. So, we are asking a slightly different question than they are asking, basically.

MR. WATERMAN: And hopefully, the MOU will be able to work out that.

MR. SANTOS: And we do plan to use EPRI's work to leverage and insights that we can extract from that to compliment our research moving forward.

MEMBER BLEY: That means you are going to start with the data they have already collected?

MR. SANTOS: Absolutely.

MEMBER STETKAR: Let me ask a broader, so we can keep moving here because we are obviously not going to get through 40 slides and look at different categories of different events.

EPRI said that they made an effort to find backup documentation for the LERs that were originally identified by RES. And they couldn't find backup documentation for a 182 of them. Now, 182 events, additional events in the database would increase the whole size of the database by about 60 percent. That is a measurable fraction. Why is that? Why couldn't they find that? Are they not real events? Did you guys look into that all?

MR. WATERMAN: I went back and took a look at the list of events I had. And when I made the original list, I didn't put in the OER report number. So I thought okay, I'll put in report numbers now.

When I got to 1993, all of those events were gone out of the database. I don't know what happened to them. It was very discouraging.

MEMBER STETKAR: And most of the 182 events have --

MR. WATERMAN: I don't know about most of them. I am still working my way back up through the list, starting from the earliest data first to get the report numbers. But it seems that the database is being scrubbed or something. I mean, some of the events are recorded. I couldn't have possibly made them up.

CHAIR APOSTOLAKIS: But as part of the MOU, you would agree with EPRI finally on a database?

MR. WATERMAN: Oh, yes.

MR. SANTOS: And reconcile some of that.

MS. HERRMANN: I get to that when we go through the independent standing.

CHAIR APOSTOLAKIS: So my level of understanding, really continues to understanding. Doesn't it?

MS. HERRMANN: Yes. Like I said, this is input to --

MR. KEMPER: If I could interject something, please.

CHAIR APOSTOLAKIS: Yes.

MR. KEMPER: Hi. I'm Bill Kemper. I work in NRR.

When I was in the Office of Research a few years ago, we undertook a project called COMPSIS. I'm sure you all probably heard about that, which was designed to collect this very information that you are asking for. It is an international joint, six or seven different countries participated in it. And what we found in trying to gather that information was from the LER database, the LER as you all know, are usually produced within a certain time frame. You know, within 30 days of the event. So the recalls investigations that are actually going on at the utility sites themselves, is generally not completed. It is very common for them not to be completed. And there is also no requirement for them to send that to us as a result of that.

So what we see often is LERs is the first blush, if you will, a further detailed look but not all of the details. In other words, actually going in and dissecting semiconductors and things like that, which is often done to try to determine what the failure mechanism actually was for a system.

So, we had the same problem in the COMPSIS arena, as we were trying to populate that database. Really, we have to depend on resident inspectors to gather that information from us and it turned out to be a very arduous, difficult task to do. So that is why that most of the information is not available, associated with LERs.

MEMBER STETKAR: It is an arduous difficult task but it is an absolutely necessary task. Because what we found in our common cause experience was that if you didn't have the actual detailed information that was available only at the plant, you really couldn't understand anything. You drew, in many cases, very, very misleading conclusions from that very brief summary information, especially if you had predefined categories that you were trying to throw those individual summary events into.

So, I think we are saying the same thing is that you need that backup information. And trying to draw any inferences from simple LER summaries is --

MR. KEMPER: It is very difficult.

MEMBER STETKAR: Yes, at best. It is very limited.

MR. KEMPER: You could come to the wrong conclusion.

CHAIR APOSTOLAKIS: So, what you want to say something?

MR. SANTOS: No, move on.

CHAIR APOSTOLAKIS: Mike, go ahead. I'm sorry, Debra.

MS. HERRMANN: Yes, we talked about this yesterday, the difference between failure mechanism and failure mode. I don't think we have anything new to say there.

The same thing on the -- we talked about yesterday the difference between potential versus actual CCF. It is important to capture the potential CCF in the a priori analysis because it is a latent defect.

MEMBER BLEY: Do you agree with the way they organized that and categorized those events, those non-common cause, potential common cause, and actual common cause?

MS. HERRMANN: Yes and no. The first two columns we agree with. The last two columns we kind of start from the point that a CCF is a CCF, depending if you are doing the a priori or the post-event analysis that the potential CCF becomes important and needs to be counted. So there is that distinction there.

MEMBER BLEY: I think that is what they did, their last two columns they treated equally.

MS. HERRMANN: Yes, as a CCF. But it is at different points in time the distinction becomes important.

MEMBER BLEY: How about the middle column, the one that had the condition that had no triggers?

MS. HERRMANN: That one we are still debating, I will say.

CHAIR APOSTOLAKIS: But coming back to the potential CCF, I still think that what was done for hardware associates with the little guide is something that would be very useful to both teams.

MS. HERRMANN: Yes.

CHAIR APOSTOLAKIS: It is not going to revolutionize what you are doing but I think you can build on what these people have done.

MS. HERRMANN: Yes, there is a lot of insights there.

CHAIR APOSTOLAKIS: Okay, good. But I am not sure I agree that the distinction between failure modes and failure mechanisms is an artificial boundary. I don't know.

MS. HERRMANN: If you remember the chart that came out of the NUREG, it kind of stair-steps through where it will be a failure mode of one level of abstraction and then it becomes the failure mechanism at the next level of abstraction. So, it flip-flops as you go through the different levels of abstraction. So it is a terminology thing. But I think we --

CHAIR APOSTOLAKIS: What ultimately matters is the failure mode.

MS. HERRMANN: Yes, and that is what we need to zero in on.

MEMBER BLEY: It is what matters to put something in to a PRA. But what matters to understand how you get there and eventually if you want to try to quantify the likelihood of getting there is certainly not at that level.

MS. HERRMANN: It is lower, yes.

CHAIR APOSTOLAKIS: Yes, but ultimately means, actual operation. Ultimately, what I want to know is how it fails. Now, to understand that, I may have to do other things.

MEMBER BLEY: I guess I am uncomfortable with that because you aren't going to fix it knowing its impact on a system. You are going to fix it by understanding what has gone wrong inside. Ultimately, if you want it better, you can't stay here.

MEMBER STETKAR: Common cause failure stuff, you know, just quantifying a beta factor wasn't the purpose of that. It was to understand what was happening and do you alter your testing program, for example, to eliminate some of those causes? And without understanding those mechanisms --

CHAIR APOSTOLAKIS: Nobody is arguing we shouldn't understand anything. I don't know where that motion came from.

Okay, guys, the ACRS recommendation is do not understand. Just so.

MS. HERRMANN: Okay. Getting back to the question of wording we found, I guess these are probably some of the missing events. We did a query of the LER database. And yes, it is being scrubbed and updated. So I imagine your EPRI report cut off at December '08 and this query was run in June. So I imagine we picked up some events here.

MR. TOROK: Excuse me?

CHAIR APOSTOLAKIS: Sure.

MR. TOROK: Ray Torok. We cut off in 2007.

MS. HERRMANN: Right. I mean your report was published in 2008 but the data cuts off in 2007.

MR. TOROK: That's right.

MS. HERRMANN: Right. So our query was run later this summer. So we picked up some events and these are probably some of the missing events.

We also question the value of the data prior to 1996, like the '87 to '96 because that technology is really, really old and we are talking like 8086s and I don't think you want to draw too many inferences from that type of data when you are looking at the new reactors coming down the pike.

MEMBER BROWN: They had to be programmed.

They had software. They had their standards to which the program had been compiled. So I wouldn't --

MEMBER BLEY: The requirements were the same and if you look at failure mechanisms, they are probably going to be the same.

MEMBER BROWN: I mean, we had a lot of 386s. All right? And the early systems that I was familiar with before we spring boarded to the latest technology is 386s, which was already superseded by the next 15 generations, by the time we got around to using the 386s.

So, I don't think you can throw that out.

MS. HERRMANN: I wouldn't throw it out but I don't think it is as --

MEMBER BLEY: Software quality assurance is a problem regardless --

MS. HERRMANN: Oh, definitely.

MEMBER BLEY: -- of a particular microprocessor.

CHAIR APOSTOLAKIS: I guess it depends on what you mean by questionable value. Does this mean you discard it or you are more skeptical when you read it?

MS. HERRMANN: More skeptical. It is more of a weighting factor. The older the data, I would weight it less value. Number one, you are getting to software quality. I think people have learned a lot about software quality in the last 20 years that they didn't know in the '80s. There is all sorts of different design techniques.

CHAIR APOSTOLAKIS: What is up there?

MEMBER BROWN: What the hell is up there?

CHAIR APOSTOLAKIS: We have all this software.

MS. HERRMANN: We all did the best we did then.

MEMBER BROWN: I meant that in a nice manner.

MS. HERRMANN: Okay, good. Well, I did some 8086, too.

CHAIR APOSTOLAKIS: So, these are general comments.

MS. HERRMANN: Yes, right.

CHAIR APOSTOLAKIS: Obviously you are --

MS. HERRMANN: I am leading up to something.

CHAIR APOSTOLAKIS: -- telling me what EPRI has done and you are making these comments.

MS. HERRMANN: Right.

CHAIR APOSTOLAKIS: You have not

implemented anything of these. Right? So let's not take it literally.

MS. HERRMANN: Right. This is input to the collaborative research.

CHAIR APOSTOLAKIS: Okay.

MS. HERRMANN: Things to think about.

CHAIR APOSTOLAKIS: So starting with the right foot. And then you want them to use the LER abstracts verbatim?

MS. HERRMANN: Remember on the database screens, there is that text field. And it was explained yesterday that that was just kind of a notes field. We interpreted that that was summarizing the abstract. So that was a disconnect. We understand what happened there so we can ignore that one.

CHAIR APOSTOLAKIS: But you agree that you can't always go with the verbatim.

MS. HERRMANN: Right. Well, the point here is that you don't want to read the LER abstract. You want to read the entire LER and the backup data because the abstract often is not an abstract. Often it is just the first paragraph. So we just ignored the LER abstracts and we looked at the entire report and the backup data that went with it.

I think we need some LER writing training for the industry.

MEMBER BROWN: That will never work.

MS. HERRMANN: Well, we can recommend it.

Okay, on the root causes, in the report there is bar graph where they show the distribution of the different types of root causes. We had some concerns or questions there because the categories of root causes that are given are not mutually exclusive.

For example, one of the items listed is ineffective change management. Ineffective change management includes inadequate requirements, inadequate testing, inadequate CM, inadequate V and V. If you look at it the other way, V and V is supposed to present or prevent all of your errors. So V and V would include inadequate requirements, inadequate testing, inadequate CM. You could say everything is the result of inadequate V and V.

So what we are recommending, this gets back to the categories. The categories, if you are really going to analyze root causes, you need to get down to the lowest level. You need to have categories that are mutually exclusive and need to be at the same level so that that way you can start deriving some meaningful intelligence.

CHAIR APOSTOLAKIS: And you are convinced that EPRI did not do this or it is something you want to make sure they did?

MS. HERRMANN: This is something, again this is a recommendation going in to when we start working together.

CHAIR APOSTOLAKIS: Okay.

MS. HERRMANN: What EPRI did is they reported the root causes as they were on the reports. They didn't makeup the categories. So again, this gets back to we need some LER writing training. Let's get these categories --

CHAIR APOSTOLAKIS: Is a root cause the same as a mechanism?

MS. HERRMANN: Not always.

CHAIR APOSTOLAKIS: So a root cause leads to a mechanism that leads to a failure mode?

MEMBER BROWN: It leads to an effect.

MS. HERRMANN: Which could have a trigger.

MR. HECHT: The root cause is generally what I call the seven deadly sins. You know, gluttony, vice, laziness, things like that. But ultimately, the root cause could be a failure to understand, implement, manufacture, install. Basically, human.

CHAIR APOSTOLAKIS: And what would be an example of a mechanism that results from this cause?

MR. HECHT: A mechanism might be that the limits on a input variable aren't properly set because the root cause was that the people who wrote the requirements didn't understand the proper range of the variable.

CHAIR APOSTOLAKIS: And then the failure mode?

MR. HECHT: It might be a crash because the software couldn't process the input variable.

CHAIR APOSTOLAKIS: Very good.

(Laughter.)

MEMBER BROWN: You better write that down.

CHAIR APOSTOLAKIS: It makes sense.

MEMBER BROWN: That is on the transcript? You had better print that out.

CHAIR APOSTOLAKIS: Okay.

MS. HERRMANN: Same thing, there was a bar graph on the corrective action. And again, EPRI was just reporting what was on the reports. They didn't make the categories up. But the categories are not mutually exclusive. One of them was given as analysis and analysis is not a corrective action. You do analysis in order to determine what corrective action to take.

So again, we are getting back to we need to have the classification levels that are at the appropriate level and there is no overlaps in order to really determine what is going on here.

I think I mentioned yesterday some of the events that were not counted as CCF in the statistics. Actually, we are CCFs, we found three where the text described it as a CCF but the box wasn't checked and counted. So we went over some of those yesterday.

Same thing, there were three events that were not counted as potential CCFs where it is described as a potential CCF. So that is part of the data scrubbing we can do when we start working together on the database.

There is one analog system. I think that was just a fluke. And then there was one event where it had a bogus LER number. EPRI yesterday indicated that that is a typo. We have got that one squared away.

So we decided to do an independent study of the LER data and kind of see if we could reproduce the similar results. And we used the LERs because there is a threshold for reporting LERs and the reporting is mandatory.

On the approach, we did a query based on, we were trying to answer the --

MEMBER BLEY: I understand what you said but the reasons you use the LERs, is that something you intend to take forward and just stick with LERs? I mean, you are missing an awful lot of data if we do that.

MS. HERRMANN: Oh, LER plus the backup data.

MEMBER BLEY: But the only things to get rebuilt is LERs.

MS. HERRMANN: For this independent study. Not the future research.

MEMBER BLEY: Not the future.

MS. HERRMANN: Right.

MEMBER BLEY: Okay.

MS. HERRMANN: Yes, this is --

MEMBER BLEY: I thought you were making arguments that you will want to hold to.

MS. HERRMANN: No.

MEMBER BLEY: Okay.

MS. HERRMANN: And I should point out here is the other thing we did is we only used -- like Bill brought up the point that there are interim LERs. We only used the final LER. Because the interim, like you know, you are in the spur of the moment, panic. You know, it may not be the accurate assessment. So we paid no attention to the interim. We only did the final LERs. And a lot of times there was a big gap between the interim and the final. So we only used the final ones to help get a little closer to reality.

And we only went back to November '97. We figured a 10 to 12 year period was kind of more accurate of what is going to happen in the future. Sorry about the 8086s.

CHAIR APOSTOLAKIS: Well you can always go back later and --

MS. HERRMANN: Yes, I mean, the LER database goes back a long ways. You know, we just did a snapshot.

MEMBER BROWN: You need to go back to Z-80s.

MS. HERRMANN: No. I did like Ralph Underman. He was a very creative person.

MEMBER BROWN: Z-80s were up and operational in reactor clients in 1984.

CHAIR APOSTOLAKIS: I think it really comes down -- I mean these are artificial distinctions. It all comes down to what we said earlier. Something happened, you know in Athens in

500 B.C. If that is relevant to today, you use it.

MS. HERRMANN: Yes.

CHAIR APOSTOLAKIS: Whether it is ancient or not I think is irrelevant, unless you can make a good case that this now because of A, B, C, is impossible to happen.

I think that that really, I mean, the basis should be the actual mechanism and the causes. The root causes.

MS. HERRMANN: Root causes, yes.

CHAIR APOSTOLAKIS: Thank you. Don't you think that is a reasonable thing to do? Then you take away all this criticism. You know, you stop at '97.

MS. HERRMANN: If the data is relevant.

CHAIR APOSTOLAKIS: Absolutely. Yes, that is what we are saying. The conditions are more or less the same and you judge that this thing could happen today, then you use it.

MS. HERRMANN: Yes.

MEMBER BROWN: One of the arguments you could make is that the architecture of the microprocessors themselves are far more high quality relative to their structure, than they were 30 years ago. And that is a relevant fact in terms of the way you construct your software when you build it. I mean, that would have been a better argument than just it is old.

I mean some of us think that being old is not necessarily all bad. Right?

CHAIR APOSTOLAKIS: I have to agree with that.

MEMBER BROWN: Yes, I think that is right.

CHAIR APOSTOLAKIS: Okay.

MS. HERRMANN: Okay. So this is where there is a distinction between the EPRI report. We included within software failures the final items. This is requirements errors, design errors, algorithm errors, implementation errors, interface errors and parameter errors. And here we mean software parameters, i.e., constants. Parameter has a different meaning in the overall plant. And then timing errors.

MR. HECHT: Debra, can I ask a question? You have used the term failure and you have used the term error. Are those the same thing?

MS. HERRMANN: What this is capturing is the error in the software product, yes. And these are from the IEEE standard, since we use --

MR. HECHT: The IEEE standard?

MS. HERRMANN: Pardon me?

MR. HECHT: Which IEEE standard?

MS. HERRMANN: 1044 or excuse me 1045, I think it is. It is where it classifies software anomalies.

MR. HECHT: I see, okay.

CHAIR APOSTOLAKIS: Would the --

MS. HERRMANN: It is either 1044 or 1045. I can't remember. I will check that out. But it is a classification scheme for software anomalies.

CHAIR APOSTOLAKIS: In the context of root cause mechanism and so on, where does the term error fall in?

MS. HERRMANN: An error could be a root cause.

MR. HECHT: Well this appears to be --

CHAIR APOSTOLAKIS: It could be a mechanism, too?

MS. HERRMANN: Again, where it is in the architecture, yes. But what we looked at is these errors, if you will, in the software product as a root cause and that is how it shows up in these statistics.

MR. HECHT: It looks like they are causes, ultimately. In other words, the software didn't do something you expected it to do because it wasn't designed properly or the interface was wrong.

MS. HERRMANN: Yes.

MR. HECHT: So it is kind of a cause.

CHAIR APOSTOLAKIS: A cause.

MR. HECHT: So there is a defect which led to the error. Is that -- to the failure.

MS. HERRMANN: Yes, these are your classic error of omission/error of commission type.

MR. HECHT: Wow. Well, as usual, those terms also need to be defined.

MS. HERRMANN: Yes, and we excluded human error and operator error from the software failures.

MR. HECHT: By the way, how would you -- there is this thing called a timing error there at the back. I guess there would be a timing error where it came, you designed it to come later than it did and there might be a timing failure where you didn't necessarily design it to come later than it did but it did anyway for another reason.

So which one is that? Which one is that timing error? The former? In other words, you were wrong about when you said something, you told it to wait 15 seconds and it should have been to wait seven seconds or something?

MS. HERRMANN: No. This would be a timing error at an integration point between --

MR. HECHT: Well then that isn't quite consistent. Because a timing error at the integration might be because of something different than the software, which might be considered an algorithm error.

It sounds like it is more like a failure. It is a result of some other kind of error. Are you with me? Let me try again.

If you are talking about integrating two things, let's just say you are talking about integrating one processor talking over some kind of digital connection to another processor. And the information doesn't come over in time because there is some contention on that network or something is happening and it stays in the buffer until it gets over to the other side. That is a different kind of phenomenon than one where you said hold it in the buffer because the software is telling it to and then send it over and it comes late.

MS. HERRMANN: Right. Okay, in this case the latter category is what is considered a timing error.

MR. HECHT: Okay. So the fact that it came late because of some external --

MS. HERRMANN: External.

MR. HECHT: -- circumstance, that would be a failure.

MS. HERRMANN: Right.

MR. HECHT: By the way, how would you distinguish a design error from an algorithm error?

MS. HERRMANN: An algorithm error is a specific case where the calculation is wrong. The design would say multiply X by Y, or whatever, determine that, and then it actually got implemented some way wrong. I have examples of each of these coming up.

And we defined software, I think, a little bit broader than EPRI did. It is all of the above. Operating systems, utilities, applications, firmware, and data. And again, this is consistent with IEEE nomenclature.

And we looked at four categories of CCFs. Failure of primary and a back-up, multiple systems operating in parallel, multiple units at a single location, and then another category, which is a common vendor's product that failed at multiple locations.

MEMBER BLEY: Just to be clear. Because you are not doing maintenance errors, a plant maintenance person reinstalling the wrong, out-of-date software isn't --

MS. HERRMANN: Isn't captured here, no.

MEMBER BLEY: Got you.

MS. HERRMANN: That got put under human error.

MEMBER BLEY: Okay.

MS. HERRMANN: Because we wanted to really zero in on what is wrong with the software.

Okay, the query we ran, we got 45 records. And you can see the distribution here.

MEMBER BROWN: You say that only one of these was included in the EPRI report. Is that one subsequent to 2007 or is that one in the entire 1997? Are you saying all other data is, they missed 40 -- I mean, they said they had 49, out of this 1E stuff.

MS. HERRMANN: This is everything that meets the threshold for reporting LER data. The one overlap record was from 2005 and that was identified as a software failure.

So this, I think, is part of the missing 160 that you couldn't face for whatever reason.

MEMBER BROWN: And yet you still came up with 27 software errors --

MS. HERRMANN: Yes.

MEMBER BROWN: -- as opposed to common defects, the way they classify them.

MS. HERRMANN: Right. So this is the distribution. If you take out the seven that aren't hardware/software, you get a different distribution. Software still leading the pack. And then if you take the software failures and split them into common cause versus non-common cause, about 78 percent.

CHAIR APOSTOLAKIS: So let me understand this business. The 45 LER records involved software.

MS. HERRMANN: They --

CHAIR APOSTOLAKIS: They were in response to your search --

MS. HERRMANN: Yes.

CHAIR APOSTOLAKIS: -- for software. Then you looked more carefully to see whether it was really a software problem or something else.

MS. HERRMANN: Right.

CHAIR APOSTOLAKIS: And you concluded that 60 percent of those were in fact legitimate software failures, according to your definition.

MS. HERRMANN: Right.

CHAIR APOSTOLAKIS: And of these 60 percent --

MS. HERRMANN: Then you throw.

CHAIR APOSTOLAKIS: I understand this. How about the next slide?

MS. HERRMANN: Okay.

CHAIR APOSTOLAKIS: Seventeen, what does it say now?

MS. HERRMANN: This is throwing out the seven that are not hardware or software. That is when we went from the 45 to 38. There were seven of them where software was not part of the problem but it was mentioned in the LER.

CHAIR APOSTOLAKIS: Okay. But the number of legitimate software failures remains the same.

MS. HERRMANN: Yes.

MEMBER BLEY: So that other one is just because your search for the LERs gave you something that wasn't --

CHAIR APOSTOLAKIS: It was really broad.

MEMBER BLEY: So that is not a very interesting --

MS. HERRMANN: Yes, we threw those out.

MEMBER STETKAR: Did you look for LERs that didn't have key words that were perhaps related to digital failures?

MS. HERRMANN: We ran a variety of different queries to get, you know, kind of zero in on the data set.

CHAIR APOSTOLAKIS: So the real data are

on 17. Is that correct?

MS. HERRMANN: Oh, page 17, yes.

MEMBER BLEY: I'm sorry to hang on this one little thing. If the maintenance guy installs the wrong software, that is not a software error. But if a clerk at the vendor sends out the wrong software, that is a software error in your classification scheme.

MS. HERRMANN: If there was an error in the software that the vendors sent out, yes.

MEMBER BROWN: No, that is different.

MEMBER BLEY: That is the way they classify it.

MEMBER BROWN: She said if there was an error in the software. You said if they sent out the wrong software version? That is not an error in the software. It is just a wrong version.

MS. HERRMANN: Yes.

MEMBER BROWN: There is a difference in terminology. That is all. I just want to make sure she is answering the question you phrased. So, you want to answer that again?

MS. HERRMANN: Okay. If there was an error in the software and the vendor shipped it out, that is considered a failure.

If the vendor sent out the UNIX and they were supposed to send out Windows, that was not counted.

MEMBER BLEY: Yes, but if they had a version out. They made a new version. Instead of sending the new version, they sent out one three versions ago.

MS. HERRMANN: Yes, that is not counted.

MEMBER BLEY: Okay, thank you.

MS. HERRMANN: Can't blame that one on the software.

CHAIR APOSTOLAKIS: Okay.

MS. HERRMANN: Now if we take the 27 software failures and split them between common cause and not common cause, you get this distribution.

MEMBER BLEY: Now, did you define what you told me earlier, I think is what you would call common cause here would have been the two right-hand columns of what EPRI called the common cause.

MS. HERRMANN: Yes.

MEMBER BLEY: Okay.

CHAIR APOSTOLAKIS: And these are actual common cause.

MEMBER BLEY: No. These are potential or actual.

CHAIR APOSTOLAKIS: No they said actual.

MEMBER BLEY: Well to them, actual is what EPRI called potential or actual. You had a common defect and you had a common trigger, such that if you had called upon it to work, it wouldn't.

CHAIR APOSTOLAKIS: Is that true with your case?

MR. HECHT: Now, look at the next slide and it looks like the affects actually happened.

CHAIR APOSTOLAKIS: I think they are actual.

MS. HERRMANN: Here is the distribution.

CHAIR APOSTOLAKIS: By the way, do you make such a distinction between trigger and defect?

MS. HERRMANN: No.

CHAIR APOSTOLAKIS: Or you are looking at the whole thing. Okay.

So again, to be clear, these are actual common cause failures.

MEMBER BLEY: The equipment didn't start or whatever.

MS. HERRMANN: These 21, yes.

MEMBER BLEY: So it is only EPRI's right-hand column.

MS. HERRMANN: Right. I think your

question, the way I answered your question earlier is we defined CCF. We include both. But this data --

MEMBER BLEY: But these were all real equipment that didn't start or didn't do what it was supposed to do.

MEMBER STETKAR: This is not a Licensee Event Report where a licensee reported an error in the software that had a demand for the diesels occurred, none of the diesels would have started.

MS. HERRMANN: No.

MEMBER STETKAR: Okay, this is none of the diesels actually started. Okay.

CHAIR APOSTOLAKIS: Wait a minutes. Then why is that so? I mean, if the diesels could not have started, why don't we care about that? I mean, --

MEMBER STETKAR: We are just trying to understand --

CHAIR APOSTOLAKIS: I know.

MEMBER STETKAR: -- what those numbers mean.

MEMBER BLEY: She said they would have counted. I'm sorry.

CHAIR APOSTOLAKIS: Well, see that is a computer error.

MEMBER BLEY: But it wouldn't have been

reported.

CHAIR APOSTOLAKIS: Would it have included those there? If they find that you know, again, we are giving you a hardware example, that the diesels could not have started but there was never a demand, would that be a common cause failure or not?

MS. HERRMANN: Well number one, it wouldn't have been reported in the LER data but it would be counted as an on-call figure, unless they had met or set the criteria for reporting an LER.

CHAIR APOSTOLAKIS: So there must have been an actual demand.

MEMBER SIEBER: The only way we come up this through Part 21 if somebody said this is a generic defect. We didn't have an event.

MEMBER BLEY: Or like the one EPRI talked about when they actually shut the plant down to investigate it.

CHAIR APOSTOLAKIS: Well, if it was found during testing, though, it would have been reported. Right, Jack, if it is found during the test?

MS. HERRMANN: During the audit.

MEMBER SIEBER: I don't think so.

CHAIR APOSTOLAKIS: I think it is reported.

MEMBER SIEBER: Well in some other way because it was causing a plant event.

CHAIR APOSTOLAKIS: I mean, you tried it and they don't start and you don't report it to the NRC?

MEMBER SIEBER: If it doesn't start, you report.

MR. WATERMAN: Yes, because if it is declared inoperable, you would have to report it.

CHAIR APOSTOLAKIS: Yes, that is what I am saying. It doesn't have to be an actual demand.

Okay, so these are actually the things do whatever they were supposed to do.

MS. HERRMANN: Right. Okay and then if we take the 21 common cause failures, this is how they split out. And then a couple of them hit multiple categories there.

MR. HECHT: Debra, I am looking at the EPRI data on page 13 of their presentation and they basically say there were no actual common cause failures due to software. And you are counting actuals and you seem to have 24. Do you have --

MS. HERRMANN: That gets back to the slide where we said we had 27 reports that aren't included in the EPRI data.

MR. HECHT: I see. Are those all between 2007 and 2009?

MS. HERRMANN: No, '97 forward.

CHAIR APOSTOLAKIS: Ray?

MR. TOROK: Just as a clarification, I am Ray Torok from EPRI, if I can make these comments. Our statement had to do with 1E systems only, where there were actual common cause failures. There were plenty on the non-1E side.

MR. HECHT: Right. Okay. Thank you.

CHAIR APOSTOLAKIS: So you are not -- all these failures are both 1E and non-1E.

MR. TOROK: Right.

MEMBER BROWN: So if I take the non-1E software where you came up with 20 and I add in your four 1E, that is 24.

Does that mean they really captured all of the ones you say they didn't capture?

MS. HERRMANN: No because our numbers didn't match.

MEMBER BROWN: So they found another 20 somewhere that you didn't count.

MS. HERRMANN: Not that we didn't catch them.

MEMBER BROWN: I'm not criticizing.

MS. HERRMANN: Remember they captured the INPO data and we did not query off the INPO data. We queried off the LER database.

MEMBER BROWN: Was your non 1E off the LERs or off the INPO data?

MR. TOROK: Ours were both. We used both databases and so I imagine we had both 1E and non-1E from both places.

MEMBER BROWN: So you still came up with the same number. That is kind of interesting.

CHAIR APOSTOLAKIS: They will reconcile those things. So, let's understand what this is.

MS. HERRMANN: We are looking for trends. The exact number is not important.

CHAIR APOSTOLAKIS: Yes, they will reconcile it. So, what was your conclusion on 19?

MS. HERRMANN: On 19? We just wanted to know what types of common cause failures were occurring. And it looks like the multiple systems in parallel and multiple units.

One thing we were trying to keep an eye on was the common vendors product failing at multiple locations. That could be problematic.

MR. HECHT: When you look at the classification, it is not really the mechanism. It is not really the mode. It is the effect in terms of whether it affected --

MS. HERRMANN: Yes.

CHAIR APOSTOLAKIS: So common failure of a common vendors product at multiple locations.

MEMBER BLEY: How did you find this?

CHAIR APOSTOLAKIS: Can you elaborate a little bit on that? What does it mean?

MS. HERRMANN: I don't want to name names here. This is a hypothetical example. If say a Common Q platform failed at multiple locations and it failed because of the same reason, --

CHAIR APOSTOLAKIS: But did you find other locations where did it not fail or it was just defective and whoever used it it would fail?

MS. HERRMANN: The latter.

CHAIR APOSTOLAKIS: The latter?

MS. HERRMANN: And it was interesting because if you sorted the LERs by date, you would see it failed here on Monday, Wednesday, Friday. So it was like generally the failures happened within the same time frame.

MEMBER BLEY: Were they common cause failures at multiple places or one failure at one place and one at another?

MS. HERRMANN: Okay, so it was a common cause at a location, as well as these particular -- you see the asterisk?

CHAIR APOSTOLAKIS: Yes.

MS. HERRMANN: That means it fell into both categories. So multiple units at and multiple locations.

CHAIR APOSTOLAKIS: So the product was defective, period.

MS. HERRMANN: Yes.

MEMBER BLEY: And it was common cause at each location where it failed. And that is how you found it --

MS. HERRMANN: Right.

MEMBER BLEY: -- because each of those reported it separately. So it may be sitting there failed at others.

MS. HERRMANN: Yes and not reported.

And then we --

MEMBER BROWN: Were the common cause failures different in each circumstance?

MS. HERRMANN: No, I wouldn't say so.

MEMBER BROWN: But they are all the same. So the product had an inherent failure mechanism which reproduced itself at each location and in some single locations, multiple times on multiple applications of that platform.

MS. HERRMANN: Right.

MEMBER BLEY: Can you tell us more about that one?

MS. HERRMANN: No.

MEMBER BLEY: We are kind of interested in that. Do you have more slides on that one?

MS. HERRMANN: No, I don't.

MEMBER BLEY: Sometime, we would like to see some information on that, I think.

MS. HERRMANN: Okay.

MEMBER BROWN: So I am just thinking. So if somebody had three applications of use your hypothetical Common Q platform, they all would have been expected to exhibit this particular failure. And I am not disagreeing with you because I have seen that in other compliments before.

MS. HERRMANN: And I think that situation highlights the need for industry to communicate among itself. So if something happens, industry talks to the other people who have the same platforms installed.

MR. WATERMAN: I think one example would be ultrasonic flow measurements on feedwater for calorimetrics. We have had some issues with how accurate that instrumentation is. It is installed in various plants. Wherever it was installed, it had the same accuracy issues. So, you could say well, your calorimetrics are failing, whether it be at multiple units, a Part 21 notice type.

CHAIR APOSTOLAKIS: So yet another question. I see all of these numbers and percentages and so on in several slides. Are these going to be useful to a PRA analyst or are you also refraining from giving that advice like EPRI did?

MS. HERRMANN: No. These are just, we are looking for trends. These are not numbers I would plug into any calculation.

CHAIR APOSTOLAKIS: But if somebody tells me that the probability of failure of a package is ten to the minus four and I have seen your numbers, I having great difficulty believing ten to the minus four. I really am.

MEMBER STETKAR: Well that's not true. That ten to the minus four is a number that got thrown in as an unavailability on demand. And you are just counting numbers of events here. You are not counting the number of unit installed digital system operating hours, nor the number of demands. You know, this has no information about the denominator. That is what we have always faced --

CHAIR APOSTOLAKIS: I still would be very uncomfortable. I appreciate that but --

MEMBER STETKAR: I wouldn't necessarily. I mean, look at what we did with D.C. Generators where suddenly if you counted the number of demands, keep the same number of failures and the real number of demands, you suddenly found that your diesel generator failure rate became one-third of what it was because you hadn't counted all of the real demands.

CHAIR APOSTOLAKIS: I appreciate that this is focused only on failures. But I see too much information here that really shakes my confidence in a ten to the minus four number, unless you do give me the denominator. If you don't give it to me, I don't believe it. That is too much going on here.

MEMBER STETKAR: I am not trying to defend the ten to the minus four number either. It is just that --

CHAIR APOSTOLAKIS: I appreciate that this is focused really on failures, things that could fail.

MEMBER STETKAR: That is the danger of just --

MEMBER BROWN: Well that is what you want to use. That is what you would like to get out of this, eventually. If you had enough information to get the denominator, --

CHAIR APOSTOLAKIS: Okay.

MEMBER BROWN: -- then that would give you a number.

CHAIR APOSTOLAKIS: But if I go back to the common cause failure evaluations for hardware, again, there they had the same problem. So they said okay, we will separate the actual successes and demands and focus on beta, gamma, delta.

MEMBER STETKAR: This is useful information in that sense.

CHAIR APOSTOLAKIS: So it does give you something regarding beta, for example. But yesterday EPRI said no.

MEMBER BLEY: It said that number wasn't --

MEMBER STETKAR: The numbers may not be relative but they didn't say you couldn't derive one that is certainly relevant.

CHAIR APOSTOLAKIS: Right. That is all I am saying. This is shaking up the confidence.

MS. HERRMANN: Sorry about that.

MR. HECHT: Did you forget that these are both 1E and non-1E systems that are continuously operating and some of them are not on a discrete event.

CHAIR APOSTOLAKIS: Put yourself in a situation where you have to make a real decision and if something goes wrong at San Onofre, you are responsible. If you see those numbers, are you going to say, yes, it is ten to the minus a hundred? No. This really makes me worry about it. That is what I am saying.

MR. HECHT: Let's just say that those are all Westinghouse numbers and San Onofre is a CE plant. All right?

CHAIR APOSTOLAKIS: Well, they didn't tell me that.

MR. HECHT: No, I am just saying that there are lots of reasons why you wonder without worry.

CHAIR APOSTOLAKIS: Anyway, I guess this is a different interpretation but I have a question for you, Myron. Do you see anything here that is really very different from your experience with the space business? Are we crazy? Are we consistent? Are we what?

MR. HECHT: What I see is that I am very

surprised at the low number of requirements/errors.

MS. HERRMANN: We were, too.

MR. HECHT: I am not surprised by the low number of implementation errors. And design looks high to me as well.

MS. HERRMANN: Yes, generally, the trend that you see is that requirements account for the majority. I agree that we were a little bit surprised with this.

MEMBER BROWN: You said requirements count for the majority?

MS. HERRMANN: If you read all of the classic papers and textbooks, they always say that requirements account for the majority.

CHAIR APOSTOLAKIS: That's true.

MS. HERRMANN: But this doesn't show this. And we compared this to the INPO Technical Report 8-3 or 8-63. And this distribution is very similar to what is in the INPO report and they highlighted design as a problem. They explained it as a lack of germane knowledge in moving from the requirements to the designers. I think that is a plausible explanation.

The other thing that happens and I think this more gets into business practices, a lot of times the importance of taking the time to do the design right and actually analyze all of the different ways you could design it, different options. That is not well understood and the design phase gets rushed. Let's get to coding. And so I think the rushing introduces a lot of errors.

CHAIR APOSTOLAKIS: The requirements --

MEMBER BROWN: They have to deliver a product in July.

MS. HERRMANN: Yes, schedule pressure.

CHAIR APOSTOLAKIS: The requirements are probably set by nuclear people.

MS. HERRMANN: Yes.

CHAIR APOSTOLAKIS: Then the guys who make mistakes they call in.

MEMBER BROWN: Well, they try to overcome this in contracts with what is called requirements traceability matrices. And I mean, I had very simple systems that I was working on and they were 57 pages. I mean, the guy actually, the vendor went through and pulled out every LAN out of the specification and laid it in. There must have been 500 requirements.

And they went and showed, this piece of software did this. This piece of hardware did that. This blank did blank. It really helps when you do that. It is expensive and it is time consuming because you have to have a defined hardware design to answer that question and you have to have a defined software architecture and you have to have a defined set of coding that you put in place to implement that architecture.

So, you don't just get that done in the beginning. It is something you have to do at the end and it is very time consuming, very engineering intensive, and people don't like to pay for it.

MR. WATERMAN: But it has been our experience in the NRC on the audits is that just about every system the NRC has looked at has had requirements traceability matrix backing it up.

MEMBER BROWN: Well, how thorough is that done? And how thorough is the audit of it? Because if nobody checks it, it is a form, if they did it, they put it in the file cabinet. If you don't review it and check it, --

MEMBER BLEY: George's comment might have sounded a little flip but if you go back 35 years ago or so when WASH-1400 was done, the guys who came over who brought fault tree analysis over from aerospace, were very surprised when they finished that analysis, they didn't find lots more single element failures and had to say we have never looked at an industry where you didn't find those in complex design.

So something about the standard approach you had been using, which was single failure analysis, really did a good job. Maybe the same kind of thing is going on here.

MEMBER BROWN: Yes.

MEMBER SIEBER: I think another piece of the problem is that the bulk of the instrumentation, the elements of it, come from other industries, the don't come from ours.

Now, if you go out to an instrument vendor, they used to sell them to the chemical industry, refineries and stuff like that. So everything is sort of a forced fit. It makes for an occasional problem.

CHAIR APOSTOLAKIS: Anyway, I think ultimately what will matter is how do we deal with these numbers. You don't have to answer that today. I don't know what we do with them but eventually we will have to have some idea where we are going with all of this. Right?

And I appreciate this is still the exploratory phase. We are still trying to understand, collect information. Yes, that is great. In fact, that is what we recommended, what, a couple of years ago.

So I really would like to understand, when I see those numbers, what I can do about them.

Yes, sir?

MR. HECHT: Well, I was going to ask, in light of the fact that the cause of the design failures was in fact inadequate understanding of the domain by the application engineers, that that implies that there has to be a second set of requirements. The first set of requirements might be called system requirements and the second set of requirements might be called software requirements.

MS. HERRMANN: Yes, that is sort of what is recommended in the INPO technical report.

MEMBER BLEY: Myron, let me ask you a question back to what George had asked you before and you were surprised by the imbalance between requirements and design. What about the shear numbers of them? Are there a lot fewer or more than you think?

MR. HECHT: Well we don't know the denominator. The denominator I need now are these lines of code.

MEMBER BLEY: Oh, I hope not. There has got to be a better denominator. Go ahead.

CHAIR APOSTOLAKIS: But I think our systems here are simpler than the ones you are used to.

MR. HECHT: Much simpler, yes.

CHAIR APOSTOLAKIS: Much simpler.

MEMBER BROWN: These are actually not. I mean, if you look over that is just a twelve year period.

MR. HECHT: That's true.

MEMBER BROWN: Actually I take that back because if you are including non-1E in here, the plant I&C systems might be as complicated.

CHAIR APOSTOLAKIS: Because of that feedback in control.

MEMBER BROWN: Well the process control system misinterprets control. For example, digital interpreting controls are pretty sophisticated systems on these.

MR. SANTOS: George, Dan Santos, Research, if I may go back to your question, what are we going to do with this. I think with the numbers, it will probably be more of a long-term answer. But today, we can use all this insight to help better focus the reviewers efforts and then help industry improve their own processes by getting who knows the insights we are deriving from --

CHAIR APOSTOLAKIS: From the end of process.

MR. SANTOS: Yes.

CHAIR APOSTOLAKIS: Okay.

MEMBER BROWN: What also helps, folks is the fact that your overall --

CHAIR APOSTOLAKIS: But at the same time you are telling me, Mike is telling me that performance and process are two different things.

MR. WATERMAN: Well, performance proves process.

CHAIR APOSTOLAKIS: The other way.

MR. WATERMAN: No. Performance proves process. When you go out --

CHAIR APOSTOLAKIS: Oh, proves.

MR. WATERMAN: Proves. Proves process. When you go out to look at something, you look at the performance and that tells you how good the process is, the actual process.

CHAIR APOSTOLAKIS: Okay. I'm sorry.

MEMBER BROWN: I was just going to echo that fundamentally what you find is that you are always going to have problems and, therefore, your overall system architecture is really is one of your main defenses is making sure the plant works right.

CHAIR APOSTOLAKIS: By the way --

MEMBER BROWN: So there is independence and redundancy and stuff like that that really plays into your --

CHAIR APOSTOLAKIS: I don't want to give the impression that I am at a loss here or I don't like what I see here. I am really very pleased to see what EPRI did yesterday and what you guys are doing today. I think we are on the right track now.

Looking at the evidence, we are questioning it, we have different interpretations, debating it.

MEMBER BROWN: Yes, we really need to get that MOU in place so that they can really, so they can --

CHAIR APOSTOLAKIS: That was the idea behind that ACRS letter whatever two years ago that said you know, let's look at failure modes and all of that. So, this is really a very nice effort, I mean both days. I mean the rest is questions, as usual.

So this is now a new way of presenting slides, looking at yellow stripe? EPRI did that yesterday. You guys are doing it.

MS. HERRMANN: We are consistent. Okay,

this is just some examples. I thought of this as just kind of an interesting side light here of our requirements error. And on this one it was the right position deviation monitor alarm. It was define to enunciate on a greater than, rather than a greater than or equal to setting. So that caused problems.

The design one I found really amusing. This was a control rod drive processor software and it was looking at minutes, seconds, hours, and day of year. And on the minutes, seconds and hours it did everything correctly. It did range checks, the whole nine yards. On the day of year, for some reason it assumed that it would roll over to a one instead of a zero.

Computers, since the 1940s have started counting from zero, rather than one. So I was a little surprised that this error occurred. Then it range checked everything else but it didn't range check the year. So when it rolled over to zero, all sorts of faults, you know, it went crazy from there. And this particular error actually occurred in 2008, 60 years after the first computer.

This one I would attribute to the designer rushed. Because he did it on the other three, didn't do the checking on this one.

The next one is a calculation error and this was a simple, they were dividing by 1.5 instead of 1.15. And the LER goes through all the math and this that and the other. But as a software engineer, I have to sit back and think did the guy just type it wrong? Maybe he got in a hurry and he typed a 1.5 instead of a 1.15. So if the calculation here may have been a typo.

The last two illustrate a common phenomenon in software engineering where you fix one problem and you introduce another problem. On the interface, there was an Arcnet coupler communication board installed and they were having some problems with it. So they said they would fix it by going to the next version of the Arcnet coupler and that introduced more problems and worse problems.

MEMBER STETKAR: That is interesting. So you found some of that. I was going to ask EPRI yesterday, one of the conclusions that I recalled reading in their report that people were doing an awful lot of software patches to compensate for both software and hardware failures.

MS. HERRMANN: Yes.

MEMBER STETKAR: And I was going to ask them whether they saw any evidence of quick patches resulting in --

MS. HERRMANN: Other problems.

MEMBER STETKAR: -- later problems.

MS. HERRMANN: Yes.

MEMBER STETKAR: So you found some of those.

MEMBER BLEY: This is more than a quick patch.

MEMBER STETKAR: Well, this is more than a quick patch. But that is right.

MS. HERRMANN: And the same thing on the parameter is they were trying to fix one problem, the control valve oscillation. So they changed the time constant. They fixed that problem and created another problem in transmitter delay.

So a lot of this gets back to I think rushing and not thinking things through.

MEMBER BROWN: Sometimes software architecture and where a piece of information comes from to be selected to make a decision has a play in that.

MS. HERRMANN: Yes.

MEMBER BROWN: So it is not just I am rushing to do that but there is a how you select a particular end result and from what input data can make a difference also. It can cause the same problem.

MS. HERRMANN: I mean, it is like when you do your boundaries of your change effect analysis, usually people do it too narrow and they need to let it go out.

MEMBER BROWN: Then that is the key point.

MS. HERRMANN: Yes.

MEMBER BROWN: You really have to walk your way forward and way backward to make sure you have caught all of the inputs and outputs.

MS. HERRMANN: Yes.

CHAIR APOSTOLAKIS: Well, let me interrupt here. Mr. Santos, all this time is taking away from your presentation on the plan, on which there will be an ACRS letter in September. Are you comfortable with this? You are not going to have tomorrow.

MR. SANTOS: Yes.

CHAIR APOSTOLAKIS: And I have to stop you at 4:00 because BNL is presenting something.

MR. SANTOS: Which is part of it. I am okay.

CHAIR APOSTOLAKIS: You are okay?

MR. SANTOS: Well after the break --

CHAIR APOSTOLAKIS: I see we have another

20 slides.

MEMBER BLEY: We have like two or three more. We are not going through the backup data.

CHAIR APOSTOLAKIS: Okay. We are going to take a break at 10:00. So, Debra.

MS. HERRMANN: Okay. The next step we did is we took the statistics from the LER independent study and we put them together with the EPRI data just to see what would happen. You see the 62.5 percent, if you take the EPRI, you combine the two, the EPRI and the NRC, you come out with a 70 percent rate. So we are still, I mean, it is consistent, even though we sliced it a little different.

DAS report, I think this was covered yesterday. A lot of the comments are OBE because it was based on earlier versions of the ISG.

And then we got into the discussion on spurious actuation. I am not sure we need to go into that. So, I will jump to the recommendations.

And basically what we are saying here is that we think we need to go through the research that is identified in the plan, particularly the MOU. This is all just input into that collaborative research.

We would caution from drawing real decisions from this data. This is a very small data set. We are very glad there has been few software failures but it is not a statistically significant sample. So orders of magnitude are probably okay, not much else. And then the recommendation we have talked about a lot as we need to come up with a very precise, accurate way of classifying the data so that there is not overlaps, gaps, or inconsistencies.

MEMBER BROWN: How do you get back to getting information reported via the LERs? I mean that seems to me that would be a big hole. If they are big or they are not inclusive enough. Is that your point with EPRI?

MEMBER STETKAR: The only way they can get it is through the collaborative work.

MEMBER BROWN: That is just a classic problem with getting reported events and failures.

MR. SANTOS: Yes, that is why we believe when we get to a more standard way of industry and --

MEMBER BROWN: Well, it is more work of industry to provide more detail, I would think. I mean that is what the classifying is.

MS. HERRMANN: You need a standard classification scheme that everybody is using in the same way.

MEMBER BROWN: Very common. I agree.

Okay.

MR. HECHT: Wasn't COMPSIS supposed to do that?

MEMBER BROWN: Who?

MR. HECHT: COMPSIS.

MS. HERRMANN: Bill, you want to address that?

MR. KEMPER: I'm sorry, I missed the question.

CHAIR APOSTOLAKIS: Ask again.

MR. HECHT: Wasn't COMPSIS supposed to address the problem of data standardization and classification schemes?

MR. KEMPER: It could have gotten to that, yes, but really COMPSIS was intended just to identify the failure on loads and have a good explanation to the person who is searching for the data what the root cause was, really. So some of those things could have been sifted and gathered from the data.

But the problem we have had, as I said earlier, the data is just not available or it is available and we can't get our hands on it. They won't release it.

CHAIR APOSTOLAKIS: Okay. Ray, you want to make a comment no more than three sentences?

MR. TOROK: Oh, wow.

CHAIR APOSTOLAKIS: Four sentences with semi-colons, if you like.

MR. TOROK: Three sentences? Would you give me five?

CHAIR APOSTOLAKIS: Start with three now and we will see.

MR. TOROK: Okay. Okay.

CHAIR APOSTOLAKIS: Well, I don't want to make this back and forth but I feel it is fair to give you a chance to comment on what the staff has said.

MR. TOROK: Sure. Yes, I guess this is working?

CHAIR APOSTOLAKIS: Yes, it is.

MR. TOROK: Well, I have to say for us, this is a lot of new stuff and we really haven't had time to digest it or discuss it with staff.

So and as far as I know, none of this is published yet. Is that right? I haven't seen anything.

CHAIR APOSTOLAKIS: This is not uncommon at ACRS meetings.

MR. TOROK: Oh, okay. So my point is we haven't really had a chance to digest it or to discuss it with staff. Still, I have a few reactions that I wouldn't mind sharing.

CHAIR APOSTOLAKIS: Okay, go ahead.

MR. TOROK: My first reaction was that you know a couple of years ago, staff told us that it wasn't possible to do this kind of evaluation because the data was insufficient to do it. And now I am really gratified to see that they are actually doing it. I think that is terrific.

There are many observations that they are making that I would say, yes we would agree absolutely. The big one is that we need to get a handle on the importance of software-related common cause failure contributors compared to other common cause failure contributors. That is absolutely true.

They said something about the low number of 1E digital systems in place. And it is true, there aren't that many. But on the other hand, there have been core prediction calculators out there for decades. So there is a fair amount of experience in some areas.

Now in regard to the pre-'96 data, I think the comment was already made, I wouldn't be so quick to throw it away because I think we have seen good lessons learned and so on, even though the data may not be as detailed, as more up-to-date on stuff. I think there are good lessons in there.

In regard to finding some errors in our report, I believe there are errors in our report. We thought we were doing pretty well but I appreciate them calling attention to those and we will look into that. Obviously, we haven't had time to do that yet.

One of the things that I know happened is when we went through our exercise of bringing people together to argue about how to disposition key events, in some cases, the initial assessment was changed, for various reasons as we discussed yesterday. And you saw how we struggled with those things. I don't think we did a good job in some cases of going back and doing configuration management on our records there and that is why there is some inconsistencies.

Also, there were cases where there was confusion about whether or not a spurious actuation is a common cause failure and it appears both ways in some of our records. And we should fix that. Okay? So there is some of that going on there.

In regard to the statistical results, well, their definitions in binning approach is very different from ours. And so obviously, the statistics coming out of that are going to be very different. So, I can't comment in detail.

There are a couple of things that I am not comfortable with here. I still don't buy this notion of combining 1E and non-1E events. In our experience, design errors in 1E systems are very unusual and for good reason. They are functionally very simple. And for the 1E systems, you really do go through all of this rigorous process, elements like requirements traceability matrices. Those are being used and have been for a long time.

So I think there are still important differences in 1E and non-1E such that you shouldn't just be throwing them all together.

Now, I really like the suggestion I think that came from Dr. Bley yesterday about identifying bins that are sort of a lower-tier bin compared to what was in the actual reports. Because we just took the words out of the report and we combined everything in terms of root causes and corrective actions. We didn't make judgments about which was the real root cause. We put all the causes in that had been identified. The same thing with all the corrective actions.

I think it is an interesting exercise to go to that next level and try to find bins that can be mutually exclusive and help you see more about what is going on. And that also may be a mechanism for combining aspects of 1E and non-1E and I think we should continue to look at that.

Now it made me uncomfortable to tell you the truth when they said out of 27 events, we only found one. I'm not sure how that can happen. So, I would like to find out more about that. And I don't see, I was looking for a list of those events in the handouts and I didn't find that but hopefully that will be coming out soon in publication somewhere along the line.

One thing I noticed in listening to the discussion is that I think that Mike and Debra are experiencing some of the same difficulties we had when we went to disposition these events, in terms of arguing about, you know, was it really common cause. Could there have been extenuating circumstances? And we argued among ourselves. It flip-flopped and everything else. And I think they are still in the middle of that. So, it would be nice to continue that discussion with them.

I think that would be very helpful because sometimes there is this tendency to try to do root cause analysis on the fly. You know, as an example, was that a typo? Did the programmer just missing something? What is going on. And lots of times it is difficult to figure that out. Sometimes there are hints in the write-ups that let you but it is not a trivial exercise. So, I think more discussion of those things is needed.

CHAIR APOSTOLAKIS: You are on sentence 17.

(Laughter.)

MR. TOROK: And in conclusion I would like to thank you very much for giving me the opportunity to comment.

(Laughter.)

CHAIR APOSTOLAKIS: Okay. Thank you all. As I said earlier, I am really pleased to see this effort both yesterday and today and on the issues that you raised, staff and EPRI. I think this is the way to go, unless my fellow members object to this. I thought that was very, very helpful, very useful. And with the MOU in place, I think we are going to get somewhere.

Thank you very much. We will recess until about 10:20. About. About. Don't comment.

(Whereupon, the foregoing meeting went off the record at 10:04 a.m. and resumed at 10:24 a.m.)

CHAIR APOSTOLAKIS: Okay, we are back in

session. Mr. Santos. Go ahead.

MR. SYDNOR: Good morning. My name is Russell Sydnor. I am the Branch Chief for the Digital I&C Branch in the Office of Research and I am here with Dan Santos, who is the Senior Technical Advisor for Digital I&C in the Office of Research. And Sushil Birla is also Senior Technical Advisor in the Office of Research right now on rotation NRR. He is going to present some of the research topics. And Paul Rebstock is the Senior Digital I&C Engineer and who also works in the Branch of Research and he will be presenting some of the topics.

In our bullpen over here, we have Mike Waterman, as you know from previous discussions. And I will introduce Jeanne Dion, who is a relatively new NRC employee but actually was real experienced in our work at Sandia on some of our cyber security research and some of the other research which you may have questions about. And Debra Herrmann, Senior Technical Advisor from NRO, who has been giving us lots of input on the research plan.

The agenda. In order to save some time, what I propose to do is the area that we are most interested in getting your feedback is the proposed research programs, obviously, the new plan. And so that is where we are looking for your insights and judgments and any notification of gaps that we may have missed.

So, I am going to shorten my discussion. We have 17 slides on background, history, and some of the process that we went through to develop the new research plan. And we will go through that after. I will try to curtail that to just what you really need to hear about.

So the purpose here to talk to the subcommittee, we are looking for a ACRS endorsement of the new updated research plan, digital research plan. And like I just said, we are obviously interested in our insights and about the research currently ongoing and it is going to continue into the new plan. Plus there are several key new research projects which we have formulated, some of which are influenced by advice from the subcommittee and the ACRS and other presentations on whether it was from the steering committee, discussions of the last two days, things like that.

Background information, I am going to go through this real quick just to save time. The subcommittee is very familiar with why Digital I&C system reviews are challenging.

CHAIR APOSTOLAKIS: We noticed that, yes.

MR. SYDNOR: You noticed that. You know, some new committee members, Research's role is, what we do is confirmatory and anticipatory research, testing and analysis. We develop tools, data and the local methods that licensing offices use. And also we lead national and international collaboration efforts in our area.

Research plans, there are different ways of coming to the Office of Research and getting us to develop or commit resources with research. One of the ways that we like to use is research plans because they are an excellent planning tool and provide for a resource, loading and budget and things like that. But it also allows us to communicate with the industry our broader intentions and get feedback from internal licensing offices and from ACRS on research directions.

The new plan that we are presenting today is essentially the third in a series of formal plans in the Digital I&C area that really had their basis in a 1997 National Academy of Sciences Report on digital instrumentation that you see there on the first slide. And that provided a lot of guidance to the industry and to NRC on the topics that we need to understand better to implement digital systems at nuclear power plants.

There was a research plan developed for the '01 through '04 time period. And the ones the committee may be more familiar with is the current plan, which we are currently implementing and was the '05 through '09 plan and it built upon the 1997 report, it built upon the '01 through '04 plan and then added some new topic areas that came from just changes in the industry, changes in technology, emphasis, new emphasis on new reactors, things like that. And so those are some of those topics.

Another thing I just wanted to mention briefly is that one thing that had a big influence on what research was doing in this time interval from '06 to even continuing to this point is the Agency formed the Steering Committee for Digital I&C. And that created, as you know, because the subcommittee has heard of all the work and is still hearing about some of the work on TWGs and ISGs that came out of that.

In that time frame, from 2006 to the current time, the Office of Research restructured our approach on what we were doing in a number of areas and the resources were committing to support that effort because it was essentially a fast, as it were, on creating some interim staff guidance that the industry was really asking for, for improved guidance. And so many of the issues in those, in the interim staff guidance and the issues in the TWGs we are dealing with were in Research topics in our plan. And in a much shortened timeline, we ended up refocusing the labs we had under contract to help work with the TWG efforts and help formulate the ISGs.

So the current plan, these are the seven areas in the current plan.

I really wanted to spend a little time and take some questions if there are some, on current status. The seven major program areas, as most of you are aware, those are somewhat arbitrarily divided up into 29 research projects and tasks. And actually, we ended up to implement those, we ended up dividing that into even more specific research projects that were, you know, commercial contracts, research with the universities, research with DOE, many DOE labs.

As of August, the items that were in the '05 through '09 plan, we have delivered 23 research projects. And those are things like reg guides, NUREGs, lab technical reports, letter reports, tools that we have developed, things like that. But I also wanted to highlight the fact that all of that work is not done. There are 17 of those projects are still in progress. Some are just starting but many are getting near to completion. Some the committee has heard about in other presentations.

An example would be Mike Waterman presented his research results on adequate diversity. We are hoping to wrap that one up. We are in the final stages of comment incorporation on that NUREG. So that is an example of one that has been ongoing for several years and we hope to drive to completion shortly.

Another thing I wanted to mention is that all these ongoing projects are being carried over to the new plan. So a lot of the discussions that we are going to have later when we get into the specific research topics, we are going to be giving you the opportunity to talk about that on-going research, hear a little bit about it at a high level, anyway, or ask questions if you have specific areas of interest. But also, primarily understand where we are going with it and what we hope to achieve.

Another thing I wanted to mention about current status is that there are eight project areas out of those 29 that were not started for various reasons, either priorities, research, resources, just going back quickly. Three of those we are carrying over to the new plan, Our first version that we put out for comments, we received some comments from the licensing offices, know we still have interest in those three items and so leave those in there and you will hear a little bit about those later.

Five that we thought did not need to be carried over into the new plan for a lot of different reasons, priorities, interest from the industry, interest from the licensing offices, need for new regulatory guidance, those type of things, these are the topic areas that were in the '05 through '09 plan. No significant work was ever started from the Research basis. And in fact, the most recent review as we updated the plan validated our determination that these did not need to go forward. And so if there are any questions on those.

Some of the challenges we experienced in the last several years in implementing the plan. And these are, obviously a lot of these, impact the whole agency. There has been a lot of staff turnover. Close to 80 to 90 percent staff turnover in my branch. Most of the branch, the Research Branch for Digital I&C are less than two years for the NRC right at this point. We have a couple of experienced engineers in

Paul and Mike but outside of that, most everyone else is relatively new, including myself.

There were other things impact, the ability to do the contracting, continuing resolutions, some conflict of interest issues with specific DOE labs that started and caused us to stop and restart research with different labs, things like that.

Some reprioritization, like I already mentioned, the Digital I&C Steering Committee and the work on those specific issues caused us to reprioritize our emphasis on where we were putting our resources. And we have had some new user need requests from other offices. A good example is the committee already reviewed and will be reviewing again a NUREG guide on cyber security and that has been an effort that we have been dedicated to for over a year now.

CHAIR APOSTOLAKIS: Now, before we move on to the new plan, what would be the two or three major accomplishments of the previous plan?

MR. SYDNOR: Well, I would list as one of the higher accomplishments our support of the steering committee. Because for instance, we have the diversity research that was ongoing at the time. It was very timely and influence at ISG. And the highly integrated control room research that was ongoing influenced the ISG-4 for communications issues. But there was significant research that was done.

The committee hasn't been presented the research but the research that was done to look at nontraditional PRA methods for digital systems. The Ohio State work looking at dynamic methodology --

CHAIR APOSTOLAKIS: Which you are not using anymore. And so you decided it is not worth pursuing it?

MR. SYDNOR: We have stopped the benchmark, the second benchmark, similar to how the other division stopped a second benchmark by Brookhaven looking at traditional methods, in part because of the redirection from the subcommittee that we really needed to take a step back and understand the inputs we would need to do valid modeling and digital PRA. But that research was completed, the first benchmark was completed. And so we gained a really good understanding of constraints and limitations of that and where we need to refocus it going forward.

And one of the directions we had from the subcommittee when Alan Kuritzky presented his findings for the Brookhaven work on traditional methods was that we needed to take a step back, look at failure modes like the discussion from the last couple of days. And also that maybe that the parallel paths of dynamic and traditional methods maybe in fact was superficial. And we ought to look, as we get back into methodology after we go back, and take a look at the basics and make sure we have our alignment on the basic inputs that you would need for this, that we look at a different way of managing.

And we have, I would say, closer collaboration with the other divisions' research at this point. Well actually, the discussion topics later in the day will cover that in significant detail.

There has also been significant research done by the University of Virginia on the fault tolerance testing methods for digital systems. Several years ago, we actually purchased an AREVA TELEPERM system and we just recently finished the fault tolerance testing on that. We just presented preliminary results of that both to AREVA and to internal licensing offices and received some excellent feedback on the direction of that research.

We are moving on to looking at other platforms, the Invensys Triconex platform, for instance.

CHAIR APOSTOLAKIS: So the agency is using this fault tolerance, what is faulty is objectionable.

MR. SYDNOR: Well, it is still in the formative research right now but like I said, we presented the preliminary results of our findings from the testing we did on the AREVA TELEPERM system. And really got some excellent feedback both from AREVA from the engineers that work with that system and also from the licensing offices, with the direction of that research.

And ultimately, it looks like that could be a viable method. In fact, the University of Virginia is considering commercializing the research because they have fine-tuned their methods for doing this work to the point that it could be a commercial application.

Now, we haven't presented that to the subcommittee because it is still on-going. It is sort of in the middle of a multi-year, multi-platform testing research program. But we could, at some point.

CHAIR APOSTOLAKIS: Well it was presented what, three years ago?

MR. SYDNOR: As preliminary.

CHAIR APOSTOLAKIS: Yes, and the major objection was to the reliability numbers.

MR. SYDNOR: Right. And certainly that is an area that is wide open for discussion.

MR. HECHT: Can I ask a few --

CHAIR APOSTOLAKIS: Yes, you can.

MR. HECHT: -- question on that? How can you do fault tolerance testing without the knowledge of failures?

MR. SYDNOR: Well actually, we are going to --

CHAIR APOSTOLAKIS: That is a detail question, perhaps.

MR. SYDNOR: That is a detail question.

CHAIR APOSTOLAKIS: Yes.

MR. SYDNOR: But we are going to cover that topic later in the presentation.

CHAIR APOSTOLAKIS: Okay.

MR. SYDNOR: So, we will cover the fault tolerance testing, bringing that up again. I am sure Mike could address the University of Virginia's approach on that.

MR. HECHT: Is the approach just random fault injection?

CHAIR APOSTOLAKIS: There is whole

methodology.

MR. SYDNOR: Not purely random.

MR. SANTOS: Not purely random. There is an element.

CHAIR APOSTOLAKIS: And we can always present the presentation from the University of Virginia, if you are interested.

MR. HECHT: Right.

MR. SYDNOR: Well then now we have actual results.

CHAIR APOSTOLAKIS: We will substitute the members because you were not here when we had that last time.

MR. SYDNOR: Now we have some actual preliminary results.

CHAIR APOSTOLAKIS: I hope not on the reliability.

MR. SYDNOR: No. On the --

CHAIR APOSTOLAKIS: On the methodology, I assume.

MR. SYDNOR: On the methodology.

CHAIR APOSTOLAKIS: What we learned about the system.

MR. SYDNOR: Right.

CHAIR APOSTOLAKIS: Okay, so where are we now?

MR. SYDNOR: Well, just real quickly. Dan didn't and I didn't create this plan last month. It is something that we have been working for a considerable amount of time. We have gone through a pretty extensive effort at the working level to get and receive feedback, and up to the Branch Chief level, to receive feedback from all of the user offices. We have gotten lots of comments and feedback from all of the offices you see listed there.

And so we have formally addressed all of those comments and transmitted that back to the offices. And so we are right in the process. We do not have formal office concurrence yet. We are really looking for ACRS input in advance of that, so that there is opportunity for the committee to influence direction of individual research programs.

CHAIR APOSTOLAKIS: Is that what we normally do?

MR. SYDNOR: That is generally what you are like.

CHAIR APOSTOLAKIS: Before office concurrence, we express a view?

MS. ANTONESCU: Yes.

CHAIR APOSTOLAKIS: Really? Okay. So but

you say that NRR and NRO have had answer?

MR. SYDNOR: Yes. There is a significant security.

CHAIR APOSTOLAKIS: Sure. So is getting concurrence a formality now, since you already have received a lot of input from them?

MR. SYDNOR: We always hoped that.

MR. SANTOS: That is the plan.

MEMBER BLEY: Did you get much guidance from NSIR?

MR. SYDNOR: In their area. Actually, as you are well aware, there has been a lot of give and take. We have been working very closely with them for the last year and a half on our cyber security research which we will talk a little bit about, as we get into the topic area.

These are just some of the comments we received, you know, that obviously the offices are interested in training, not just delivering a NUREG that may be difficult to understand. Some of these are your typical comments. But we did have, I will just point out, we had specific comments, very high level comments of the direction of research programs. No, we don't need this topic. No, we disagree with you dropping this one, so bring that one back. So we had significant comments. They were not casual comments.

CHAIR APOSTOLAKIS: Now when you say encourage industry, is the MOU with EPRI out of this?

MR. SYDNOR: Yes, it is interwoven into a number of their research topics, especially what we have been discussing.

CHAIR APOSTOLAKIS: So that MOU is kind of broad? I mean, you can pick any project from here that you feel is appropriate and collaborate with them?

MR. SANTOS: There are several topics that we have met for the past year with EPRI. Developing that MOU for some targeted areas and I will show them to you a little later. But one of them is an operating experience. So it is not everything.

One other point I want to make here is as we came through this, there was a lot of good research initiatives but none of them fit our regulatory scope. So, an example will be sustainability and obsolescence management. So areas like that we find are important for the discipline, then you have to ask the question is this regulatory research or some research of the industry.

So we try to collaborate with the industry to try to have them take the lead and leverage --

CHAIR APOSTOLAKIS: When you say industry, who do you mean?

MR. SANTOS: I mean most of it, I mean EPRI for the most part.

And also a challenge we have sometimes how much state-of-the-art research should be undertaken versus the industry. And that is a challenge sometimes.

CHAIR APOSTOLAKIS: Sushil, yes?

MR. BIRLA: I would like to add to that answer. Sushil Birla from the NRC.

Just to give you a little bit more on the MOU, it was initiated by the Division of Research Analysis. It was written up broadly but basically that was their interest, the PRA when they did research. And with Dan's initiative and counterparts on the EPRI side, interest was expressed in some topics of research and Dan mentioned EPRI is a very important one.

We have not yet had the detailed discussion meetings but as we enter into those discussion meetings, some of this is going to get sorted out. What is really purely non-NRC mostly EPRI side, what is joint, what is really more NRC side, will the exchange of information only give in certain cases we share information but EPRI publishes its own reports and NRC publishes. All that has yet to be discussed out.

MR. SANTOS: A new marriage.

MR. HECHT: I know that NRC and EPRI have cooperated for many years on many projects but how is any potential conflict of interest issues resolved in the MOU? I don't need to know the details but is that covered adequately?

MR. SANTOS: Yes, adequately. What is reviewed by the OGC, General Counsel, and there are several protocol you will follow, include transparency. And basically, bottom line is you can share data but you draw your own conclusions. That is kind of the bottom line. But we are following agency protocols and OGC advice to make sure because we are very aware of that issue and one that we respect very carefully.

MR. BIRLA: And EPRI, mind you, is a research institute. So earlier when the question came up what do you mean by industry, we need to make that distinction.

And would someone from EPRI like to clarify the distance they keep between research and industry interests?

MR. TOROK: Yes, this is Ray Torok from EPRI. When you say -- I am not sure if I understand the question correctly. But the point is that EPRI does research that is intended to support the industry. Could you be a little more specific?

MR. BIRLA: The boundaries of our MOU are purely research, without any direct connection with licensing issues.

MR. TOROK: Right.

MR. BIRLA: So we on the NRC side maintain that boundary, similarly you do. So our discussions of where this project goes, why under the MOU when we meet, we are meeting as researchers. You are not bringing in a physical discussion. Similarly, you are not bringing licensing officers.

MR. TOROK: That is right. And EPRI does both research of the type you described. And we also get involved in efforts to generate technical basis for a licensing position, that sort of thing. But in this case, we are talking about, you know, the research part of it.

And Dan's point was a good one is that the notion is that we can share data and discuss ways to deal with the data and so on. But in the end, we need to separately generate our assessments of what it means to the conclusions.

MR. BIRLA: We do plan to have the appropriate level of transparency also. So point well taken.

CHAIR APOSTOLAKIS: Okay.

MR. SYDNOR: Okay, just real quickly on this, the second comment slide, the first three bullets are examples of fairly major research initiatives where we have received comments to ensure that we included these. The first one we just discussed briefly.

The next one was really a new one that came from I think we received lots of comments from both NRO and NRR because of the new uses by vendors of automated software tools and how do we judge the validity of those and their use in a licensing submittal.

And obviously, the third bullet you are very familiar with. That was part of the reason that is in the plan is a feedback from previous ACRS discussions. And then you know, obviously specific deliverables. There is always an appropriate criticism of research that you know, you get a deliverable that is usable, not just research results that people are not sure what to do with.

MR. SANTOS: One thing we are trying to improve is not necessarily wait until the end. You know, to your destination but involve as knowledge get generated, try to through the journey of the research get the user officers more involved as we get let's say a significant finding. You know, get together and start discussing, instead of waiting for a final product that sometimes might have missed the timeliness for a nugget of information that we could not have provided to them earlier.

MR. HECHT: Is any licensee proposing the use of, you know, MATLAB or RHAPSODY for 1E systems?

MR. SYDNOR: Not that I am aware of.

MR. SANTOS: I will refer that question to some of the reviewers in the licensing office. Debra, if you can help with that or Mike.

MR. WATERMAN: Mike Waterman, Office of Research, perhaps not MATLAB or the other tool that you mentioned but for example, the TELEPERM X S system uses a product called CVAT, a simulation and validation tool, to help them verify a system they put together. I believe the representative is here and he can go into greater detail about CVAT.

Apparently, the issue arose as well, what is the qualification of that CVAT tool that you are using to verify that the software is really at a high enough quality to be acceptable to be used as a safety system.

So CVAT is one example of a tool that is being used to help develop a system.

MR. HECHT: And this is a verification tool, not a code generation.

MR. WATERMAN: Yes, it is a verification tool.

MR. SANTOS: I will cover that briefly but we are seeing automation at pretty much every stage of the lifecycle, all the way from requirements, management, doors, to code generation, to code transformers, to V&V activity, to flat automation. The trend is to move into more automation.

MR. WATERMAN: And part of what drives that is that IEEE Standard 7432, which was endorsed by Reg Guide 1.152 says that any tools used to develop safety related software should be qualified at the equivalent level of quality.

So you know, how do you go about doing that?

MEMBER STETKAR: I was going to ask this when you get into the individual topics but perhaps it is better at the higher level.

Kind of a pet topic of mine is I see very little in the plan for international cooperation. I have a two-part question. One is I know you have had some in the past. And I guess, what is your experience? Is there a benefit there? And I know the glib answer is well yes, of course, there is. I mean, is there a practical benefit? Is there information?

The sense that I have is that indeed the technologies are being developed in other countries so the actual experience, the applications have many years' operating experience in other countries. And I have talked to people in other countries and they claim that they have what they feel are fairly effective methods on assessing the reliability in other countries.

So, I am curious why we are perhaps now inventing our own methodologies simply because we live in the United States and have 322 events that we can point at.

MR. SANTOS: You want talk that one?

MEMBER STETKAR: Now, if your conclusion is there isn't much to be actually learned, that a lot of those assertions are simply thin air, that is fine.

MR. BIRLA: We could choose to discuss that now or wait for the topic.

MEMBER STETKAR: If you feel it is better in the topics then do that.

MR. BIRLA: Yes.

MEMBER STETKAR: As I said, I was kind of bouncing back and forth.

MR. BIRLA: There is a lot to be said there. Let's save the discussion until then.

MEMBER STETKAR: Thank you, Sushil.

CHAIR APOSTOLAKIS: Somebody said yesterday there is a CSNI committee that you guys are participating in.

MS. HERRMANN: COMPSIS.

MR. SANTOS: The OECD NEA COMPSIS. That is one of them. We will talk about that. We will cover that but that is an element.

CHAIR APOSTOLAKIS: The thing that -- well maybe we can ask questions as you go now to more specifics. But I mean, you said that you had significant input from the various offices, which is good. But did you also try to anticipate future needs, perhaps, that specific offices don't care about right now and do some anticipatory work that is there?

MR. SYDNOR: Yes, there is a topic that has been in all the previous plans and it really worked fairly well for us and we call it emerging technologies. But every two to three years, we initiate some research to look at that.

CHAIR APOSTOLAKIS: Okay, so we can look at these things as we go along.

MEMBER BLEY: And I just have one question on the overall. Are you going to talk anywhere about the things that have been dropped or is that, you are not going to get into that.

MR. SANTOS: Yes, we can go back to that, if you want.

MEMBER BLEY: Well you don't have to go back to it. If you are not going to talk about it again, I just wanted to ask because I saw some things in some work that I was doing with the Army where they have learned some things in the last ten years about lightning that were kind of surprising and lightning protection. And I see you have deleted the lightning program.

MR. SYDNOR: Actually, in the '04 and in the beginnings of the '05 through '09 research time frame, there was. Oak Ridge did some research in that area and there was actually a reg guide issued.

MEMBER BLEY: Okay, so you think it is pretty well caught up-to-date.

MR. SYDNOR: That is the lightning

protection.

MEMBER BLEY: Yes.

MR. SYDNOR: We have not, since that reg guide was issued, it has not been a topic that there has been any.

MEMBER BLEY: Okay.

MR. SYDNOR: But that was the thrust of that research and that reg guide.

MEMBER BLEY: Okay.

CHAIR APOSTOLAKIS: Okay, so let's pick up slide 18.

MR. SYDNOR: The new plan has essentially five program areas. And we are going to go through those essentially program by program. And the last one there is pretty much carry over that we will talk about. But in 3.1, 3.2., 3.3., 3.4, there is also some things that are ongoing from the current plan.

Did you want to say something?

MR. SANTOS: Yes, again I just want to clarify like you mentioned, even from the old plan, this classification, binning is more for convenience. But in reality a lot of these projects have dependency between them.

CHAIR APOSTOLAKIS: Sure.

MR. SANTOS: And we are trying to improve the way, how the values products input others and try to make this a more integrated generation of knowledge as we go through. So, even if it is convenient to look at bins, we recognize there is a lot of integration.

MR. HECHT: Christina sent out a handout, I think on August 13th or something like that. And the numbering of the topics there is not the same as the numbering here. Did I not understand something?

I have, for example, 3.1 through 3.7 as opposed to --

MS. HERRMANN: Status one.

MR. SYDNOR: Status one is the seven program areas in the '05 to the existing, '05 through '09 plan.

MR. HECHT: I see.

MR. SYDNOR: So that is a status one. We do have a separate tool, a mapping tool which mapped the whole plan to it.

MEMBER BLEY: It's an Excel.

MR. HECHT: Okay. All right, I see.

CHAIR APOSTOLAKIS: So we start with the safety aspects?

MR. SYDNOR: Right. We are going to start with safety aspects of digital systems and Paul

Rebstock is going to discuss the first project, which is a new project that we are proposing, a new research topic area.

MR. REBSTOCK: The issue that we are concerned about with this effort is that digital systems will permeate a new plant. There are already a lot of digital systems in existing plants and we expect more and more direct control and safety implications in future plants. And interconnections between that plant data systems and management systems and all kinds of interconnections.

We have done a fairly complete job so far of looking at individual systems and saying what the individual systems need to do and what do you need at the boundary between one system and another.

This plan is to step back and look at the plant from 10,000 feet and say what are all of the systems in the plant. How do they interact with each other? What functions should be performed where? How should these systems talk to one another?

Some of the issue has to do with communications, communications protocol, the very specific kind of communication process that is described in ISG-4. There are also kinds of communications that may be appropriate or maybe should be avoided. And that is what this plan is to look at.

The end product will be, or one of the end products will be what I and probably nobody else refers to is the abstract integrated model, which is intended to be a way of looking at the plant and defining areas of kinds of systems and the interrelationships among them.

CHAIR APOSTOLAKIS: So I guess that is not very clear to me. The final product and do what? Give advice to some reviewer as to what to look for?

MR. REBSTOCK: It would do that. It would also provide advice to us, to the industry, to create a framework for discussing this kind of system, these kinds of systems to recognize where interfaces are, how pathways, for example, from outside the plant --

CHAIR APOSTOLAKIS: Somebody is putting papers on the microphones. Can you move the microphone a little bit away? Thank you.

MR. REBSTOCK: So the intent is to look at the plant from, like I said, from 10,000 feet, to look at all of the systems in the plant and how they are all connected together. There is incentive to want to be able to get certain information out of the plant control system on the CEO's desk. You don't necessarily want it to run the other way. There is information that needs to be shared between the control system and the protection system. That should be a very highly restricted communications process. And we will address that particular communications process in ISG-4. There may be other communications that are necessary or appropriate. What this is to do is to try to get a handle on the entire picture of all of the digital systems in the plant and how they would relate to one another.

CHAIR APOSTOLAKIS: How they are related to one another or how they should?

MR. REBSTOCK: Yes.

CHAIR APOSTOLAKIS: It is both.

MR. REBSTOCK: Both, yes. Like I said, you need generation information on the CEO's desk but you don't want some kid on the internet to modify your protection settings.

CHAIR APOSTOLAKIS: Right.

MR. REBSTOCK: So, how does all of that fit together? Where are the boundaries, what should be done where?

MR. HECHT: That particular example that you gave seems to be an issue for security, cyber security, but it is not listed there as one of the issues. It is reliability, redundancy and independence.

MR. SYDNOR: Well the ultimate concern under this one, if I may speak for Paul is you know, the effect on safety and its effect on safety systems. And it is not purely a safety issue.

CHAIR APOSTOLAKIS: It's both.

MR. SYDNOR: It is a security issue as well.

MR. HECHT: But isn't the way you described the issue really one primarily of information flow and is that really worthy of a research topic?

MR. REBSTOCK: I'm not sure I understand the question.

MR. HECHT: Well okay. Basically what you have said is put a firewall to prevent or put in what is called a guard to prevent certain information from going out or going in to whatever it is. Your containment region or what is called in the security world, enclave. And the methods and technologies for doing that are pretty well defined. What is the innovation of the research questions that have to be asked here?

MR. REBSTOCK: What you have described is a solution for one particular kind of an interface.

What this project wants to do is to look and see what interfaces exist. What interfaces should there be. What information is needed in which system? Step back and look at the whole thing.

Your are right. A firewall might be an appropriate barrier between one kind of system and another kind of system. What we are talking about here is what are those systems? What kinds of systems are there? The question of how do you protect and whether you use a firewall or whether you use an ISG-4 style blackboard kind of shared memory kind of communication or whether you use some other kind of process is one of the things that would be a derivative of this.

MEMBER STETKAR: To as the question differently, the third bullet there is development of a generic model, plant-wide digital systems. What is the vision for that generic model? I mean, is it just a few little bubbles with arrows going back and forth among them or is this a fairly detailed model?

MR. REBSTOCK: The intent is to make that model sufficient abstract that it would accommodate the system designs in most plants. I don't know right now what it would look like, whether it would be a block diagram or whether it would be sort of a box with lines that separate it. But the point is that it is an abstract thing so that we can look at levels of security requirements and levels of interface.

MEMBER BROWN: Why wouldn't -- are you finished John?

MEMBER STETKAR: I am but I don't know enough about it. I guess I come back to what Myron asked is I am not sure why research wants to be able to do that.

MEMBER BROWN: Yes, my question is more fundamental. When I looked at the section 3.1 and then section 3.2, which was the security aspect of it. We are seeming to assume that all of these diverse methods of communication are welcome, wholesome, useful, and desirable.

MR. REBSTOCK: Absolutely not.

MEMBER BROWN: But yet I didn't see the evaluation or the analysis or an approach to an analysis. For instance, why would we have wireless, for instance? Do I really want my data being broadcast such that it can be picked up as opposed to going with wired systems?

And that seems to me that is a higher level topic than let's assume that people do it. Now here is all the methodologies or the methods to make sure we are protected on the cyber security or from interception or what have you.

And so that was, I am not necessarily disagreeing but that just seems to me that as soon as I saw wireless, I am starting to wonder why in the world do I want this stuff out in the airways, particularly if you are worried about somebody hacking in, which we now know that people can hack almost anything. And the only true barrier then, you don't have any barrier other than a bunch of algorithms and other types of things you have sitting down there in the systems that protect yourself from it as opposed to a mechanical barrier. I want the wire going someplace.

MR. REBSTOCK: Right. I'm not sure I get the connection.

MR. HECHT: Well my --

MR. REBSTOCK: The question of whether wireless communications are acceptable or not is a legitimate question and something that we should look at.

Personally, I am not so sure that it is a good idea. But to communicate what?

MR. HECHT: Well before I start doing that, before I start assessing techniques and methodologies for cyber security, why would I even work on this if I haven't made a decision whether I am going to do wireless or not do wireless for whatever basis I have?

That was my thought relative to -- I see the program. The fundamental in my own mind, it was do I have to go that way in order to make that research relevant. And if you decide that we don't want to do wireless, then why would I have a research program for assessing those applications?

I mean, if I am missing something --

MR. SYDNOR: Well specific to wireless, it exists.

MEMBER BROWN: Well we could use it.

MR. SYDNOR: Nuclear plants are using it. They have wireless communication networks in the plant. They are using it for several different applications. I worked at a plant that had wireless applications.

So it exists. Not for safety systems but we are concerned about the implications on safety systems.

MR. HECHT: But if you have guidance for -- there is not thought, I haven't seen anything listed that says hey, you wouldn't do it that way or the staff.

MR. SYDNOR: Well some of our research in that topic area is looking at that. There was a previous research done that looked at applications of wireless, and we do power plants and some, for lack of a better term, best practices that if you are going to do that. And now we are investigation the cyber security aspects because they already exist out there.

And so we need to be cognizant of the affect of those systems on safety systems because ultimately, the wireless systems do connect into plant intranet. That exists in plants currently operating.

MR. REBSTOCK: Right. But the point of the abstract integrated model isn't really to talk about this particular technology. It is to look at what systems there are in the plant and how they would interface. The wireless communication process or some other kind of a communication process would be a detail of all the different areas of the plant or the different areas of digital implementation would interact with one another. That is a separate issue.

This is to step back and say what is there?

MR. HECHT: So this is really data flow. It is not really -- you know, I guess one of the reasons why Charlie and maybe I have gotten hung up is that this is really a question of the flows of information, what is allowed and what is not allowed.

MR. REBSTOCK: I would rather say information than data, yes. At this level, see this is an abstract level.

MR. HECHT: So what you really need to do here is in your abstract plant representation, what you need to do is identify all of the sources of information and all the users of information and say which, whether it is bi-directional or uni-directional. Is that right?

MR. REBSTOCK: That general concept would be something that we would be looking at. The amount of detail that we go into I think will depend partially on what we find. I am not sure what the end product is going to be.

CHAIR APOSTOLAKIS: Is this a big project?

MR. REBSTOCK: I don't think so.

MR. SANTOS: No and totally internal.

CHAIR APOSTOLAKIS: So we are not talking about something major here.

MR. SANTOS: No.

MEMBER BROWN: I only read one where it would be beneficial to develop further regulatory guidance on communication processes that are appropriate for the exchange of information between plant sensors/actuators and the protection and control systems among safety channels. That was under the technical basis for --

CHAIR APOSTOLAKIS: Where are you reading from?

MEMBER BROWN: Well, I am looking in the research program, section 3.1.1.

CHAIR APOSTOLAKIS: Oh.

MEMBER BROWN: I am just reading the words of what you are doing. And we already have -- so from reading that, I am saying oh, okay, I have got these detectors down there that are going to be broadcasting the plant parameter data out to my reactor protection system or control system.

MR. REBSTOCK: I wouldn't presume that we are going to do that, at this point.

MEMBER BROWN: Well, I am just reading the words, okay, in terms of the research approach.

MR. SANTOS: If the words are bothering you Charlie, --

MEMBER BROWN: No, no, no, no. And I try to relate it back to the --

CHAIR APOSTOLAKIS: It is an issue of

communication.

(Laughter.)

MEMBER BROWN: I was trying to relate it back to ISG-4, which was issued to provide guidance on data communications between channels. Now is this related to data communications between channels? Or is this the -- I just couldn't get a picture of what the thrust was. That was my point.

MR. SANTOS: We will take the comment.

MEMBER BROWN: I don't know. So I don't want to get down in the weeds. It was just a matter of what are we talking about. I'm sorry.

CHAIR APOSTOLAKIS: Okay. Is everyone satisfied?

MR. WATERMAN: This is Mike Waterman, Office of Research. I just want to emphasize that the research plan really provides a framework within which we develop projects. So this particular project is, it sort of lays out a broad scope of things that we need to look at.

But one of products I would see out of that is sooner or later, somebody in the NRC is going to have to go out and look at a plant design and you are going want to know what to look at and what to expect when they look at that. Somebody has to approve these systems, as they come in.

And so what we are trying to do with all of these projects is to provide guidance to the people on the ground so that when they get a whole map layout of the plant, they understand what they have to look at, what they can ignore, and what kind of things they ought to be aware of as potential safety issues.

So that is the basis for all of the research. But what I am trying to do is just provide a framework within which we can start projects down specific roads.

CHAIR APOSTOLAKIS: And I think it is important to bear in mind even a comment that Myron made earlier, that the Office of Research here is charged with doing things that are not necessarily research in the academic sense.

MEMBER BROWN: No, I understand. I got that point.

CHAIR APOSTOLAKIS: You are giving advice to like Mike just said, where you are what to do and so on. I mean, in another environment, you might say well, this is not research. But the Office of Research does that for the Agency. So, I think it is useful to bear that in mind. Let's not look for innovative research results into everything here. I mean, developing guidance is part of their job.

MR. REBSTOCK: Yes, and it doesn't presume what the guidance is going to be.

Deliverable 2 here says that we are going to look into communications processes between sensors and actuators in the system. That doesn't mean --

MEMBER BROWN: Such as voting.

MR. REBSTOCK: I'm sorry?

MEMBER BROWN: Such as voting, --

MR. REBSTOCK: Okay.

MEMBER BROWN: -- which is also covered in TWG-4 very explicitly.

MR. REBSTOCK: Right. But it doesn't say how we are going to do that. And it doesn't say what we are going to accept.

MEMBER BROWN: Well the TWG-4 just says you can do anything you want to, as long as you prove to us it is okay.

MR. REBSTOCK: No, TWG-4 says --

MEMBER BROWN: I have got the words right here, if you would like me to read them to you.

MR. REBSTOCK: We can talk about that separately.

MEMBER BROWN: Okay.

MR. SANTOS: Okay, next up is, were barely touch on it but again the trend is the various life-cycle activities are becoming more --

CHAIR APOSTOLAKIS: Can you explain the title? Maybe it is obvious to everyone. "Tool Automated Processes."

MR. SANTOS: Right.

CHAIR APOSTOLAKIS: Safety Assessment of a Tool.

MR. SANTOS: Engineering activities are become more and more automated. The process for which people carry out their engineering activities are becoming automated. So we are trying to assess what was the impact of mistakes on the use of that automation that will lead to eventual failures.

MEMBER BROWN: There are V&V tools out there that people want to use to prove that their software is satisfactory and defect free.

CHAIR APOSTOLAKIS: Like fault injection.

MEMBER BROWN: Whatever. The point being is if somebody has to validate the tools, you have to have some idea of whether those tools are correct, whether they are going to give you a correct result.

And this is very difficult to do and everybody has their own tool. And it is like models in the thermal hydraulic world or whatever. You know, how do you validate the model? Well you never have an end result that you can validate that you really got the true result because the only answers you get are out of the model, I mean out of the tool.

CHAIR APOSTOLAKIS: So the problem is that --

MEMBER BROWN: I am not against looking. I think you obviously have to do it. I am just saying this is --

CHAIR APOSTOLAKIS: This is usually what happens when developers of the tool exaggerate it significantly.

MEMBER BROWN: Absolutely.

CHAIR APOSTOLAKIS: So you guys will come back and put them in their place.

MR. BIRLA: This is Sushil Birla from research. In the first bullet you see two examples listed and those are real examples. New applications are coming in with code generation tools. You have a function block diagram design. Typically, this is done in a homegrown tool. The code generator is also a homegrown tool. And then they have verification tools, which automatically generate the test cases, automatically test that generator program and want to make a claim that you don't need physical testing. So that is an example of a verification tool. Again, these are homegrown tools.

So this touches on your earlier question. When there are industry-wide well used, well-known tools like MATLAB, like the RHAPSODY, your question was, is the industry leveraging any of that? This industry is not. It has typically got its own style of function block diagrams and then therefore, it ends up with its own homegrown tools. And that becomes then an issue of concern.

MR. SANTOS: And you know, another issue is, like we said in the technical basis, before it was one guy made a mistake. Okay. Now, as you move upstream in the same process you are introducing more of a systemic problem. If your tool is at fault, the propagation is going to affect all of your downstream activities.

CHAIR APOSTOLAKIS: So is this research going to look at individual tools and provide guidance? I mean, your next slide says that there will be regulatory guidance. So can you do this in a generic way or do you have to look at each tool or what?

MEMBER BLEY: Somebody drew a parallel to verifying form hydraulic calculations. And what their staff is trying to do is build their own models to test the calculations, maybe not in as much thorough detail as the designers did, but to have a really independent look. Have you given thought to anything like that?

MEMBER BROWN: There is an experiment you could run in this area that gives you a set of data that you can benchmark. And they talked about benchmarking as one of their other sections in here.

So but you can run these other experiments, get a benchmark, run the model and tool against it and see if you get a result.

CHAIR APOSTOLAKIS: If you follow this part under the terms of hydraulics, I think this makes a good point. Should the staff have its own tool?

MEMBER BROWN: I am not objecting to this. I am just pointing out that that is what they are trying to do, from what I can see when I read this one.

CHAIR APOSTOLAKIS: It is for sure. What is the answer?

MR. BIRLA: Your specific question was is this specific tool a particular classification of tools or a bit more general. This cannot be specific to a particular set of tools. The research is going to be more general. However, the starting point in each piece of research is going to be close to what is the set of conditions that you are confronted with. So as examples, you will certainly take what we are seeing emerging in licensing applications but the result will be more general.

And we aren't the only ones facing this issue. Someone asked earlier about international, what are you gaining. So I am going to weave in part of the answer to that here.

European regulators are experiencing the same issue. And they are a little ahead of us in the curve. And they are in the middle of drafting some guidance for qualification of tools.

CHAIR APOSTOLAKIS: So then somebody will take that guidance and actually apply it to a specific tool. Is that what you are saying? I mean, ultimately it will have to have some advice as to how this specific tool can achieve certain things. Who is going to do that? NRR?

MR. BIRLA: The user of the guidance will be the licensing office, NRO or NRR.

CHAIR APOSTOLAKIS: And you will provide kind of a higher level guidance. And I am really, I guess I don't understand this very well. I mean, high level guidance, if it is too broad is not too useful. Is it?

MR. FREGONESE: Can I make an industry comment on this?

CHAIR APOSTOLAKIS: Identify --

MR. FREGONESE: My name is Vick Fregonese from AREVA. Mike mentioned I was here today.

This is a real life example for us in the U.S. We have a topical report that has been submitted to the NRC on our CVAT tool, which is our validation tool. It is used extensively in Europe on all of our applications and builds over there. And so that is something that is really germane to us in the near term. So one thing would be that the guidance that does get promulgated would be something that will be timely.

To answer the question about MATLAB, there are uses of MATLAB that generate test vectors for some of our automated testing that we do, depending on what kind of modules they are. So our European experience where we are building four or five EPRs then bringing that over to the U.S. makes extensive use of these type of tools. In some cases, the staff has already evaluated, for instances, our space tool, which is our code generation tool for TXS.

So this is something I think that is pertinent to us and I can see why the staff would need some guidance to help them through to review it. There are some IEC standards and IEEE standards that talk about tools and how they should be clarified. You know, any clarification of that to make it easier both on your side and the staff side will probably be something that will be valuable.

MR. SANTOS: And what are the right questions a reviewer should be asking are of the applicant to validate the claims I think will be a great outcome of this.

CHAIR APOSTOLAKIS: How about Dennis' suggestion? I mean, in other areas, this stuff has its own codes.

MR. SANTOS: I am getting to that in a future project. I will cover that.

CHAIR APOSTOLAKIS: Okay, fine. You answered it. Anything else on this topic?

MR. HECHT: Yes, I just wanted to point out in the aerospace -- not the aerospace industry, the commercial aviation industry, RTCA DO-178 does have some comments on that. And at the top level, it defines development tools in two areas. Those that generate code and those that are used for verification.

And the overall philosophy is that if the output of a tool cannot be manually verified, then the tool, the code generation tool has to be qualified to the same level as the code which is supposed to be produced.

For verification tools, the standards are relaxed. But particularly if manual verification can be done, then that is relied upon as the primary justification. And I imagine that with you folks -- I have looked at that.

MR. SANTOS: The answer is yes. And we are lucky enough to have Debra with us. She is an expert. She came from the FAA and she is an expert on that.

MR. BIRLA: This is Sushil Birla. That is an excellent example of looking outside the nuclear industry for available capabilities, state-of-the-art, state of practice. How others are addressing these issues. The qualification of tools is an issue everywhere.

MR. HECHT: Oh, so you didn't mention that before that you were looking at other industries.

MR. BIRLA: There is another section in the project plan and as opportunities and questions arise, we will try to weave in our answer there. This is one of areas.

So the committee in DO-178 is right now wrestling with the same issue, with inadequacies of their standard, what should be the additional requirements, and part of the project to be tracking such efforts.

MR. HECHT: Thank you.

MR. SANTOS: Our next topic is an ongoing project. I have Mike Waterman here. He is --

MEMBER BROWN: Let me back track. Sorry.

Why wouldn't a possible fallout of these tool assessments or research that you do, I'll spin a little bit off of Myron's comment, say that gee, we really don't like these tools. And probably the methodology we should be using would be manual code evaluation and/or a hookup of the software platform and its system configuration to a generic plant simulator where you can then run the plant through a set of transients, other types of, you know pressure/temperature increases, trying to see that everything performs in a manner as expected.

So those are a couple of ways that have been used, to validate this stuff. There was that track.

MR. BIRLA: This is Sushil Birla. Let me tackle that, Charlie.

First of all, the boundaries of the regulator. We cannot prescribe solutions.

MEMBER BROWN: I agree you cannot understand that. Let me finish.

MR. BIRLA: Okay.

MEMBER BROWN: I understand you can't. But you can say no to approaches to doing things if they don't provide a substance satisfactory for you to agree that it is okay.

MR. BIRLA: That is exactly what I was getting at.

MEMBER BROWN: That is my point. That is the only point of my comment.

MR. BIRLA: Yes, so part of the outcome might be that the state-of-the-art is not adequate to give you the degree of assurance you need and therefore, this is not acceptable, the technique at the moment.

MEMBER BROWN: Or much of that is driving you. You come to the conclusion that these tools are not adequate.

MR. BIRLA: But then we would have to at least establish the criteria.

MEMBER BROWN: You mean a criteria -- you have to prove that it is not okay?

MR. BIRLA: Say why it is not okay.

MEMBER BROWN: No. Why don't they have to prove that it is okay?

MR. BIRLA: Yes, so what are the criteria? Yes, I guess they would be evaluated.

MEMBER BROWN: I know how to do that.

MR. BIRLA: Yes, so we would have to document that and get an agreement, a broad consensus on that. That is part of the issue here.

MEMBER BROWN: Well you walk into a trap is all I am saying, when you do it that way. It is like we will allow you to use any methodology you come up and we have to prove it won't work as opposed to you proving it will work.

MR. SANTOS: Let's offer some clarification on that. Oh, sorry.

MR. RICHARDS: I am Stu Richards from the Office of Research.

You know, that is an interesting idea that we tell them what to do but we can't do that, as Sushil said.

MEMBER BROWN: No, I understand that.

MR. RICHARDS: All right. But what we do, the way we do business just with I&C, generically across the board, should satisfy your concern. Licensees can come forward with a proposal and say this is how we want to do I&C or pumps or valves or whatever. And then they have to satisfy us that what they are doing meets our standards for safety before we will approve it. So the burden is on the licensee to demonstrate what they are doing is acceptable.

On the other hand, part of the Agency's mission is to be clear and transparent on how we regulate. So I think what they are talking about here today is in trying to accomplish that part of our job is to work with the industry and other regulators throughout the world to come up with appropriate criteria on how to use tools.

You are suggesting maybe the criteria is tools are unacceptable.

MEMBER BROWN: I didn't say that.

MR. RICHARDS: You know, we have to do the work. We have to look at, you know, can we come up with criteria that will satisfy? You know, if you do all these things, we will be satisfied that the tool is acceptable. We owe the industry that criteria if we can produce it, rather than saying, kind of bring me a rock and we will look at it and tell you a yes or no. We need to be able to come up with some way to do business. And I think that is what we are trying to do. You know, the result might be ultimately down the road that we have got so many questions about these tools, maybe we really don't want to do it. But I don't think we are there yet. Right?

So the burden isn't on us. I just want to make that clear.

MEMBER BROWN: In a way, that is what you sounded like when you first started.

The problem here is that the licensees or the designers have to show that their methodologies for their approaches are satisfactory and meet your fundamental overarching criteria.

MR. RICHARDS: Yes, but we don't want to do business where everything is custom one-time only review. You know, we like to move to where we have standards and things so it is a much more efficient process.

MEMBER BROWN: I don't disagree with that.

MR. RICHARDS: Well that is where we are trying to go.

MEMBER BROWN: It is always a nice thing.

MR. RICHARDS: But believe me, our job is to say no. Our job is not to prove it is unsafe. Our job is to say you haven't proved to us it is safe and we are not going to approve it until you do.

MEMBER BROWN: Okay, well I will use one example, okay, just to show you. And this has been heard before. If you look at independence of I&C, go back in the old days in the analogue systems, there was one additional criteria. You had to have electrical isolation.

MR. RICHARDS: Channel-to-channel.

MEMBER BROWN: By default, you ended up with literally a channel of this and a channel of that. And they were independent. You almost could not get there. You had to work at not being independent.

With the advent of software-based systems, computer-based systems, now that electrical independence does not do it for you. You have to deal with data communication independence and how that is executed. And if you look at the methodologies that are used and you start pumping data from one computer to the other, now how do you prove that you are still independent? That is a very thorny issue which I am trying to deal with right now in the context of my time on this committee. I don't know how long I will live.

MR. RICHARDS: Well I think everybody here will agree with you that is a really good issue.

MEMBER BROWN: All I am trying to say, my point I am trying to get to is this is another area of the software validation process that brought some of that -- I mean you used to be able to look at the old systems and it was kind of obvious. You had an amplifier that did this and that. It is not that obvious anymore.

MR. RICHARDS: No.

MEMBER BROWN: And it is a far more difficult task to do. And the tools that people have been using and then advertised. The comment was very, they were homegrown. People are doing their own stuff and they want to tell you this is okay. I don't have to test anything. And it is difficult to step back and say how hard do they have to demonstrate that or if they yell loud enough, they will just well, okay. They say it is okay so it is okay.

That is kind of a struggle. It is an abstract thought process but that is the thought process.

MR. RICHARDS: You know, there is a lot of people I am sure with the staff that are probably more in agreement with you than you realize.

What we are doing is we are presenting the issues here. These are the things that we need to go off and learn more about. We don't know the answers yet. You know, we are just trying to tell you, her is the areas that we have to explore, we have to learn more about. We have to get that international experience. We have to work with industry so that we can grow in this.

We don't have the answers. And what we are looking for from you guys is, are we exploring the right questions. Are we going and looking at the right areas and is there things we have missed? We don't have all the answers.

MEMBER BROWN: I did not disagree with this particular. I wasn't disagreeing with this with my comments.

It is just that I am trying to make the point. You asked for committee comments or a member comment. I am not saying that the others agree with me, necessarily. Observations relative to what you are doing. I am just trying to put it in a context of the overall problem.

MR. RICHARDS: Yes, it is just difficult for us. I mean sometimes some of the comments I am hearing today are basically answers. They are saying you are looking at this issue. It is isn't the answer to this. You know, we haven't done the work yet. You know, we are working for the program offices. They have input into this, too. So it is hard for us to agree or disagree with you when you start talking about what the answer is.

MR. BIRLA: Thank you for the support, Stu.

(Laughter.)

MR. BIRLA: And Charlie, I understand the general theme that you are getting at.

MEMBER BROWN: Yes.

MR. BIRLA: If you take over the boundary, you can say for sure that this problem won't hit you. That theme ran in your wireless example. Why don't you just ban it? Same thing in the independence. If we have physical disconnection, then the problem won't be there. And you could take the same thing with tools.

And we used to. Now that boundary is being pushed. And this is where the regulator is between a hard rock and a -- what is that?

MEMBER BROWN: Yes, but I agree. I would say you are not between a rock and a hard place because you still have the job of assuring independence. And architecture is in the software world just as best setups for validating software in the testing world have certain boundaries or conditions that you know you have to meet.

And if it is fuzzy whether it is being met, you have to be careful about being too acceptable -- no that is the wrong word. The locator bit is gone. So that is the only point.

CHAIR APOSTOLAKIS: And we totally agree.

MEMBER BROWN: We can go on.

CHAIR APOSTOLAKIS: Heave we reached that point? Okay, okay. Next.

MR. SANTOS: I will speed up and stuff for you.

MEMBER BROWN: It is not over, George. It is not over.

MR. SANTOS: You had a question, sir? Oh, this is the UVA work where you had a previous question.

CHAIR APOSTOLAKIS: What is going on? Have I lost control here?

(Laughter.)

MEMBER BROWN: You just regained it, George.

CHAIR APOSTOLAKIS: Okay, what is next?

MR. SANTOS: It is an ongoing project. University of Virginia fault injection is developing a methodology so we say to fault injection. So there are basic methods basically to try to shake the system, once it is finished. Okay? To try to uncover faults that weren't found through the normal lifecycle --

CHAIR APOSTOLAKIS: I thought we objected to that second sub-bullet, that you cannot use those methods to say anything about probabilities. It was very clear, black and white.

MR. SANTOS: They still want to try.

CHAIR APOSTOLAKIS: Sometimes I get the feeling that the EPRI listens to us more than you guys.

MEMBER BROWN: You noticed that.

CHAIR APOSTOLAKIS: We said explicitly that this is not appropriate.

MR. WATERMAN: This is Mike Waterman, Research. The other outcome of this research is to develop a method whereby we could do the equivalent of exhaustive testing of a system to reach some measure, if you will, and objective measure of whether or not that system is of sufficient dependability, if you will, or reliability.

The project started out with the title Software Dependability, I believe and Dr. Johnson then in here discussing how you go about doing a coverage analysis of the system. And then using that coverage analysis in the Markov model, you can determine how many tests you need to do and where you need to do those fault injection tests to come up with some idea of just dependable is that software.

The idea being that if you could come up with some kind of idea of where your failure modes were in a particular system, you could then feed that into a PRA, along with some numbers that are developed out of that. And I think Jeanne Dion can provide even more detail.

CHAIR APOSTOLAKIS: I suppose if you find faults in the system, you fix them.

MR. WATERMAN: But the idea is that when a safety system is developed, well all the faults have been eliminated. Right?

CHAIR APOSTOLAKIS: They are two separate things.

MS. DION: This is Jeanne Dion.

CHAIR APOSTOLAKIS: Is it useful to have fault injection and increase your confidence if this thing is going to do its job?

MR. WATERMAN: Yes.

CHAIR APOSTOLAKIS: Yes. Is it reasonable to say that based on that I can say something about the probability of the thing not doing its job? No.

MS. DION: That was the point I was going to make. We did decide that the use of fault injection methodology to produce failure rates for PRA is not appropriate. However, the fault injection process could be used to verify failure modes or perhaps --

CHAIR APOSTOLAKIS: At some point -- does it say it? Unless PRA models, you mean also failure modes, which I am going to say you are going to say yes. Right? I agree with you.

MS. DION: For the development of PRA models.

MR. SANTOS: All I am trying to say here is that we are looking at PRA. We will discuss it later today in a more integrated manner. And this one of the projects that could help provide to their efforts.

CHAIR APOSTOLAKIS: But isn't it also true that if you identify your failure mode, you are not going to say, oh, there was a failure mode, I will give to BNL. No. You are going to say, I am going to go and fix it. Isn't that true? And that has been the problem from day one in the academy report and so on. These are not random failures that you say well, gee, I have to tolerate some of them.

In the software, you find the problem. I don't know, are you going to say it is okay? No, you are going to fix it. Right? And that makes a big difference in the calculation of probabilities. And then we get to publish to these idiotic papers that will assume there are so many faults remaining.

MEMBER BLEY: Well, no.

CHAIR APOSTOLAKIS: You know, that is good for giving you tenure but not doing real stuff.

MEMBER BLEY: I think one thing is, and I wasn't around when you guys talked about this before, of course you will fix the exact problems you find. But you might find classes of problems that are indicative of what else might be there, if you could test everything. And if I -- I don't want to dwell on the words on the slide, but if I learn something there about the failure modes or mechanisms that might help in structuring the problem, that will be useful. It wouldn't give me answers, probabilities, just like you said.

CHAIR APOSTOLAKIS: But they do have in

the presentation, we were actually presented with formulas that give you failure rate.

MEMBER BLEY: I suspect I wouldn't like that very much.

CHAIR APOSTOLAKIS: Okay.

MR. SANTOS: We agree with that. And I told you we are de-emphasizing that aspect of the work and putting more on the fault, you know, the invasive part. But we don't want to throw away everything that we have learned.

CHAIR APOSTOLAKIS: So let me understand how you are going to use this tool. AREVA comes with a new program to do something. Code. Are you going to start injecting faults and doing things? Are you going to have one of your contractors do that for you or are you going to ask AREVA to do it? I don't understand how this is going to be used.

MR. SANTOS: Right now, this is research. So we will develop a methodology. It is up to the licensing offices to determine how will they implement, whether they do independent contract or how they will roll it into the regulatory framework. That is up to the --

CHAIR APOSTOLAKIS: Let's do it for the why to see whether they can --

MR. SANTOS: If I give you answer, it would be my own opinion. But it is still --

MR. SYDNOR: Well, the answer is we haven't answered that question.

MR. SANTOS: Right.

MR. SYDNOR: I mean, that is part of this work is to determine viability and whether it can be used in that manner.

We have already, and that was what I was talking about earlier. We had the UVA come and present their preliminary results, which they obtained from testing the AREVA TELEPERM platform which we purchased a couple of years ago. And that is not a full RPS mockup. It is a channel, channel and a half of equipment. But there were some interesting results out of that and we also presented those to AREVA for their benefit.

CHAIR APOSTOLAKIS: So when is this going to close?

MR. SYDNOR: We are testing another platform. The Invensys Triconex platform. It has just been sent to the University of Virginia and we are going to test that to see what other plans we have.

That vendor is very interested in the

outcome because they believe they have a fault tolerance testing program that they have used successfully. So they are interested in the results.

CHAIR APOSTOLAKIS: So when I look at this --

MR. SYDNOR: But we are looking at the method. And I believe from what I have seen, just personal opinion, that UVA could commercialize this methodology and vendors could use it. Now, are we going to require that use as a part of a licensing submittal? That decision hasn't been made yet.

MR. HECHT: There are two, you mentioned two programs. You mentioned Triconex and you mentioned the AREVA TELEPERM platform. Triconex is basically a triple modular and redundant PLC. It is a platform on the TELEPERM system, I assume as a reactor protection system, which had the application integrated.

Testing of the Triconex system using fault injection would get significantly different information than testing of the TELEPERM.

MR. WATERMAN: This Mike Waterman, Research. The purpose of the research right now is not to test platforms and say this platform is good, that platform is bad.

The purpose of using platforms is so you can develop a systematic methodology, if you will, for testing systems in general, by applying a coverage process such that you can identify particular tests that would represent many fault injection tests that would come out with the same result.

The reason we use different platforms is simply to develop that methodology. And in the process of doing it, it is actually quite interesting to see some of the things that University of Virginia has developed to make that process more systematized, if you will. For example, the automatic generation of the test scripts and things like that and identifying which test.

So the idea is not well we are going to single out AREVA or we are going to single out Invensys in these tests. That is not the purpose of the test. It is to develop a methodology that we could perhaps apply in the future to help us reach reasonable assurance that a system is good enough to be used as a safety system.

MR. HECHT: It still comes back to the question of if you are testing the reactor trip system, there are a finite number of inputs. If you are testing the ability of the Triconex system to respond and recover and reconfigure, it is a completely different --

MR. WATERMAN: And is there a generic process you can use so that no matter what the system is, you can apply that process to the system to identify which faults to inject to give you reasonable assurance?

We also tested a feedwater system that was donated by Calvert Cliffs. Okay? So but the idea is to develop a method and not to say oh, you know, we are going to test Invensys. Yes, it is a different system but fundamentally it is a system. And where do you inject the faults? How do you determine how you inject those faults? Do you understand what I am saying? You have to develop a method to systematically prove it.

MS. DION: Can I just add something that would probably help clarify your question? You are right with the TELEPERM system being tested as a mock RPS system. There will be a similar application that we will set the Triconex up with and test it under a similar application. So, it is not just --

MEMBER BROWN: Protection system application.

MS. DION: Yes. Something representative

of a reactor protection system.

MR. HECHT: But is the Triconex system representing one channel or is it representing three channels?

MS. DION: Well, since we only have -- that is still yet to be determined. I think we only have two channels.

MEMBER BROWN: You have two separate platforms.

MS. DION: Yes, we have two. Two chassis.

MR. REBSTOCK: Well, there may be some confusion on the Invensys system. They call that three channels. That is three processors in one channel. It is a redundant system. Each individual channel has three processors in it that are all part of the same channel.

MR. HECHT: But presumably, the reason why you would use Triconex is to increase the reliability of even your single channel.

So, I guess we should speak about divisions.

MR. REBSTOCK: Well that is kind of a commercial issue. One division in one system and one division in the other system are the same definitions. One of them implemented with a single processor, one implements with triple processors. They have different ways of going about it.

MR. HECHT: But if you just --

MR. REBSTOCK: It is still just one division.

MR. SANTOS: I guess if you do have four channel Triconex, you end up with 12 processors. Right?

MEMBER BROWN: Yes. You have four divisions.

MR. SANTOS: Right.

MEMBER BROWN: Four divisions, right.

MR. SANTOS: I believe four separate chassis.

MR. HECHT: So what are you testing? Are you testing the ability of the Triconex platform to recover from failures internally or are you testing the ability of an application of your mock application?

MR. SANTOS: We are testing our methodology.

MR. WATERMAN: We are developing a methodology so that no matter what the application is, it can be fault injected and you come up with some idea is this system fairly bullet proof? What kind of assurance do I have that this system qualifies as a safety system?

You know, we are getting all hung up on the platforms and much to the chagrin of the vendors who have been kind enough to support us in this project, we are not testing the AREVA TELEPERM XS to say the XS is no good or the XS is good enough. We are trying to develop a methodology so that down the road, whatever application runs on whatever platform, we can apply this method to come up with some reasonable assurance using a systematic process that is predictable and is consistent from application to application.

The vendor has gotten just as upset about the idea of us testing their platform. What we needed was we needed hardware and we needed software running on the hardware. Where should we get it? Well, lets go out to the nuclear industry which maybe someday we will apply this to and use some of their stuff, which is what we did.

We bought an AREVA platform. Invensys donated theirs. I believe Calvert Cliffs donated some hardware and software of theirs so that we could start developing this methodology that we can use to consistently evaluate one system after the next, regardless of whether it was Invensys, TELEPERM, Westinghouse or whatever.

CHAIR APOSTOLAKIS: I think there is enough interest here so we should schedule maybe a series of Subcommittee meetings in the next year or so where we can go into more detail in these projects as the members of our consultant feel appropriate.

I don't think we can go into too much detail today. So, this is definitely a project where obviously there is interest. So maybe we can invite the University of Virginia to actually give a presentation. And you know, we can ask all these questions then and make comments and even write letters if we would feel that way.

MR. WATERMAN: It is a very good presentation. They spent about, I don't know, four to six hours down at AREVA presenting it. They came up here and gave us an abbreviated two-hour presentation. So it is pretty interesting stuff.

CHAIR APOSTOLAKIS: So you know, and I am sure there will be -- I mean, we have done it in the past. There is nothing new here.

MEMBER BROWN: I don't know. I haven't done it in the past, George. I am just listening, absorbing interesting information.

CHAIR APOSTOLAKIS: Good. As you should.

I think we have to get moving here and it is unfortunately --

MR. SANTOS: I will try to speed up.

CHAIR APOSTOLAKIS: Well, it is not only up to you.

(Laughter.)

MR. SANTOS: Okay. I will try anyway.

CHAIR APOSTOLAKIS: So let's see, you are going to move now onto a new project?

MR. SANTOS: Yes.

CHAIR APOSTOLAKIS: I think we should break here and maybe beat the crowds downstairs. So, we will be back at 1:00.

(Whereupon, at 11:51 a.m., a lunch recess was taken.)

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

(12:59 p.m.)

CHAIR APOSTOLAKIS: Okay.

MR. SANTOS: Okay, the next topic is one that sometimes people talk about Digital I&C is different from other disciplines. And you know, you walk the halls and you see people working at their models, whether it is thermal hydraulics or finite element models and what have you. And I am just like, where is our model?

So basically, we are trying to develop and the level of detail exact question that we will develop the answer as we go through developing the actual projects.

But in a high level, we want an integrated model of the digital system that will be integrated to some of the thermal hydraulics and physics models. So we have an integrated model of the overall plant so we can help, you know, validate responses to digital system failures, validate application algorithms, and basically assist their reviewers when they get a proposal for enhancing their functions.

CHAIR APOSTOLAKIS: So how do you envision that model? I mean, what would it be? Again, would it be a diagram?

MR. SANTOS: No this is not of the high level. This is of the details actually whether this will be --

MEMBER SIEBER: Software?

MR. SANTOS: -- software models. Okay?

MEMBER SIEBER: It's like a simulator model.

MR. SANTOS: A simulator model that is integrated with the simulator with TRACE, for example, RELAP. Okay? And the fidelity of that model will be a subject of the research itself. Okay? Because this could get very expensive in a heartbeat.

MEMBER SIEBER: Could you actually use a simulator model?

MR. SANTOS: Yes.

MEMBER SIEBER: I would think that would be a pretty good tool, provided you could benchmark it to something.

MR. SANTOS: That's right. And in other applications, I have seen such a concept work very well and be very helpful to reviewers accomplish their work.

So that is basically it.

MEMBER SIEBER: It gives you the opportunity to insert faults.

MR. SANTOS: Yes.

MEMBER SIEBER: System upsets, all kinds of things.

MR. SANTOS: Correct.

MR. HECHT: Is this with respect to safety systems or is this with respect to control systems?

MR. SANTOS: We will start with safety systems but that doesn't necessarily limit us there. Again, the scope, the detail, how far we take this, okay, it will be part of the research itself. But we will probably start small and grow from there.

MR. HECHT: Well, safety systems has been emphasized over the past couple of -- or yesterday. And basically just monitor and if a condition is met, then intervene. How much fidelity? What would you learn from such analyses or from such a simulator?

MR. SANTOS: Basically more of the functional dependencies that may exist between parameters. You could help discover racing conditions that you weren't aware of when you are trying to develop your trip calculations, for example.

MR. HECHT: But isn't that already addressed in great detail prior to, you know, in the reactor physics calculations, reactor kinetics calculations?

MR. SANTOS: Some of it is but basically you also want to see that the assumptions, the actual system, the sign doesn't violate your safety analysis that you have bounded. Okay? If you made a change to digital systems, you want to see how the time response and everything is bounded within your analysis also.

MEMBER SIEBER: Yes.

CHAIR APOSTOLAKIS: Okay.

MR. SANTOS: We will skip this because we have covered it in great detail. The next topic is operating experience analysis. I will turn to Russ.

MR. SYDNOR: I am going to talk about this topic. And obviously we have talked a lot about it in the last day and a half. And some of the things that we are going to be doing under this research topic have already been discussed. So I am going to try not to duplicate those discussions. I do want to touch base on some of the stuff that has been ongoing and the things we have done.

The COMPSIS has been mentioned a couple of times. And a number of years ago Bill Kemper started the U.S.'s participation in OECD NEA COMPSIS database and I have been continuing that. And some of the points about the usefulness of that database are well taken.

It is at a fairly high level. It doesn't get into any type of taxonomy that we have found useful down at the mechanism level. But what we have been hoping is to learn more about failures in other countries due to that because there are about ten nations participating in it. And we are trying to, via the steering committee we work on there, get them to enter more data because the representatives tell us they have more data but that they haven't entered more failure data. So, we are still trying to work that effort. Is it a useable tool at this time? No, it has got some interesting things in it and some people have even run analysis on the limited number of events that are in there. Limited in sites, I would say that you can get from that at this point.

MEMBER STETKAR: Russ, I don't really know what they are doing but is this, if you were to, in this forum, hazard a guess, do you expect any substantial participation in terms of the utilities in the other countries supplying that information in the near future? I am talking about two or three years. Or will this be a 20-year, German-type develop the amount of data o support the failure rate for a valve-type exercise?

MR. SYDNOR: I will just answer that. I

am disappointed in the participation level at this point in time. And you know, I haven't seen --

MEMBER STETKAR: I was just curious in terms of recommended level of our Agency's participation.

MR. SYDNOR: Well, I am trying to put more events in and maybe lead by example by putting more events in that we have from all of the LER events that have been discussed here.

MEMBER STETKAR: The LERs, that is a good seed, but the LERs in our country, I suspect are perhaps more detailed than the regulatory reports that are received in other countries, the underlying information is there. But if you can't have timely access to that through their organization, the question is --

MR. SYDNOR: Is it worth it?

MEMBER STETKAR: -- is it worth it.

MR. SYDNOR: That is certainly in the back of my mind. Like I say, we are trying to regenerate, foster interest in it via our participation. My personal opinion, I would say the prognosis is not good --

MEMBER STETKAR: Okay.

MR. SYDNOR: -- because I am just not

seeing it. And there is a couple of key countries that are not participating in that. The French don't participate. The Japanese don't participate. So I mean, you are missing a lot.

MEMBER STETKAR: You are missing the vast majority of the international experience.

MR. SYDNOR: Yes.

MR. SANTOS: Because of that prognosis, we don't want to solely rely on that. And the Agency has other --

MEMBER STETKAR: I was just getting a sense in terms of balance of resources and emphasis.

MR. SANTOS: Right.

MR. SYDNOR: So we are still supporting at this time. It is a collaborative effort that we have committed to.

MEMBER STETKAR: All right.

MR. SANTOS: The Agency has other vehicles already placed where we could emphasize the digital discipline aspects of it through some of the bilaterals that we haven't been doing as much.

MEMBER STETKAR: Do you think that might be more effective?

MR. SANTOS: My opinion, is probably.

MR. HECHT: In trying to deal with the

COMPSIS data, it is a very elaborate record structure and it probably takes a number of hours, maybe eight hours to translate an LER into that COMPSIS framework, assuming you know what the LER is.

So it sounds like I don't know, even the 322 reports that were spoken about earlier today would take more than a staff year of effort. Right?

MR. SYDNOR: Well not all of those would qualify for entry into it, the way they have the scope of it set up.

MR. HECHT: So I notice that in the 2005 to 2009 research plan there were three projects that dealt with the COMPSIS database. I guess the lesson learned from that experience is that it is a dying or a dead effort.

MR. SYDNOR: OECD is not, you know, whether they continue to support funding in it, I guess really depends on the member countries. I mean, it is fairly low cost and the problem really is --

MR. HECHT: Low cost or low budgeted?

MR. SYDNOR: The database is up and running. I mean, they have already committed. It is really just individual countries dedicating their resources to input data.

MR. HECHT: The server is up and running.

MR. SYDNOR: Yes.

MR. HECHT: That is not -- yes, okay. I guess you understand that that is not a great achievement. I mean, it is -- So, how many records are in COMPSIS at this point?

MR. SYDNOR: Oh, it is really only about probably about three dozen high level events. But again, remember the scope does not include things like turbine control or feedwater control. The computer system is important to safety.

MR. HECHT: And how many of those 3,000 records relate to digital system --

MR. SYDNOR: Three dozen.

MR. HECHT: Three dozen.

MR. SYDNOR: Thirty-six.

MR. HECHT: Thirty-six. Oh. Oh. I withdraw my question.

MR. SYDNOR: Thirty-six.

MR. HECHT: I withdraw my question.

MR. WATERMAN: This is Mike Waterman, Office of Research. The only thing about the COMPSIS database is when you tunnel down in there to find out what the level of granularity is, as I recall, it stopped at software failure. Which is not a lot of granularity. I mean, we have already identified several subcategories of that. And both us and EPRI has identified many different categories under software failure. And the COMPSIS database, the last time I looked at it, didn't go into that level of detail. So I don't know how useful it is going to be anyway.

MR. SYDNOR: Under this topic area, we have also, I think George mentioned yesterday, that will we ever get meaningful data from non-nuclear industries. We had explored that starting a couple of years ago and using Oak Ridge, we had done some efforts to go out and try to find digital fire data databases, any information we could from a number of nuclear industries.

I found some information usefulness was questionable. We did some assessments on that that were part of the ISG-2 effort to see if we could learn anything that influenced the guidance that was put out on diversity under ISG-2.

But part of that work also uncovered some other databases that we could potentially purchase. And so we went ahead and authorized Oak Ridge to proceed to see if we could find meaningful there. Not just from the data standpoint but, you know, from a taxonomy standpoint, could we learn some things that would help us as we structure the classification or taxonomy system going forward. And that is almost complete. But your prognosis from yesterday is probably right. We are probably not going to learn anything that gets down into the level of detail that we are going to be interested in.

But we have invested in that time. At least when we are asked have you looked we can answer yes, we have looked. And we have looked quite extensively.

CHAIR APOSTOLAKIS: It is okay, Dan. It is okay.

MR. SANTOS: I am not ready to make that conclusion. That is all I wanted to say.

And now an example I wanted to give is that the Agency also has a Memorandum of Understanding with NASA. And as part of that effort, we are trying to expand. It is already covered with the terms to look at data. JPL is an example, some of their V&V-centered efforts to try to derive some insights and knowledge on that.

So I don't know. I don't know if I can make that conclusion yet, given their vast experiences.

MR. HECHT: I know that the PRA work is

going to be covered separately by Alan. But there is, I think, a strong relationship between the operating experience work and the PRA work because the parameters, of course, would come from this. The question that was raised earlier yesterday was I think, and today, was actually phrased and I think the short hand is the denominator. And so is there going to be any attempt to get that total operating time or number of demands so that a rate or a probability of recovery from a failure is going to be gathered?

MR. SYDNOR: Well, I think the answer is we are going to explore is that achievable. You know, I can't say that we will be able to do that.

I have had discussions with people at INPO that have a similar interest in getting better failure data information.

CHAIR APOSTOLAKIS: The digital system is useful when you are talking about random failures, not when you are talking about designs.

MR. HECHT: And that is one of the issues. Let me ask you in follow-up to George's question, I am going to ask you another one. And that is that we have 322 nuggets that were discussed yesterday and I think that is going to be a major focus of the operation experience. But is there more information available elsewhere, particularly on annoying failures that may be recorded somewhere or could be recorded somewhere that aren't reported that might very well be random failures?

MR. SANTOS: I think the answer is yes. And you know, that is where we get into how far is the regulatory arm reaches. And that is why the MOU with EPRI will help us reach into some of their other members to get some of that additional information.

MR. HECHT: I didn't see that stated anywhere as an objective in this plan. I mean, do you think that it might help to understand the relative proportion of random versus systematic failures?

MR. SANTOS: Good comment.

MR. HECHT: I think that operating experience would be a key, I think figure of merit in determining how far one could push the PRA work.

With respect to JPL, one of the points that came up at the BNL conference which is relevant here is that two of the people who participated in that panel and they are one was from JPL and that was Allen Nikora. And then the other person was Kishor Trivedi of Duke University. They were working together on analyzing NASA operational data or JPL operational data. And they claim that more than half of the failures from operational experience were of the random nature.

MR. BIRLA: I followed up with both of them. Allen is very interested in going deeper into the data. If you recall, they classified in two broad categories, board bugs and window bugs. But that was just two cores. So, Dr. Allen Nikora is formally leading a project. And the purpose of the project is more refined analysis, finite granularity analysis. But what should be the framework of that analysis? So, he is very interested in collaborating with us. And if we can set up the structure, that would be useful to both. That could be one good outcome, even though that it by itself might not be just the structure of how you analyze the detail.

The trouble is that it pulls even greater on architectural and you have to use a lot of knowledge and intelligence in extracting meaning out of that. In the first case, Dr. Nikora himself read through 1800 such reports. Now it is time to scale himself up. But you can not scale up that level of competence, so he is trying to write an artificial intelligence program to do that. And that is where we think that we would probably have to invest economic manual labor and reading and interpreting and having a common understanding of how to interpret. We see some value in that.

MR. HECHT: So is that part of that, is that going to be part of this effort?

MR. BIRLA: We envision it is again something being explored under the MOU, again DRA, Division of Risk Analysis, the leader in the MOU with NASA and through the DRA coordinator we have reached out. There is interest on both sides to pursue further.

Technically, I had enough conversations with Dr. Nikora to know that technical people, himself, myself, we both want to work together. But the logistics of, you can't take a contractor and say now go read there. You can't get the same level, guarantee the same level of depth and knowledge.

And the second thing is the visibility of the data. JPL typically does not allow outsiders to look at the data. The contractor can. Their headquarters cannot. So we would have to work out some arrangement where even if we used a third party, a contracted party, it would be a party acceptable to JPL. And yet having the competence that we would like to see to analyze the data manually. That is still under exploration.

So you will see that there is another section in the research plan that talks about collaboration outside of our industry. In that broad category, this is one of the topics.

MR. HECHT: I see.

MR. SANTOS: And I go back to what I said in the beginning, these projects, all of them are integrated. So even though I am presenting this, it is really, there are other projects that fit in. There is tentacles everywhere.

Next, Sushil Birla.

MR. BIRLA: Okay, this project, as you see from the background sheet, the drivers are a number of elements here, some the ACRS itself is aware. There was a recommendation on taking inventory of all the DI&C systems currently in the plans and some kind of a classification of them.

And then there are several ACRS letters about focusing increasing effort on identifying failure modes and then there is an SRM that enforces that recommendation of the ACRS plus adds another one about exploring the feasibility of risk quantification in failure methods.

These came from the ACRS and the Commission. We integrated in this project some other requests, one that you all are familiar with in the PRA research project they needed parameter of the base, they needed offices' opinions. Enough of that. Is there some other approach we can take analytically? Yes. And similarly would be human factors research group.

Over and above that, from the licensing offices there was some interest, specifically from NRR as they were going through the review of Oconee, they began realizing that within the time available, they have to exercise some judgment. I am not really sure whether that is deep enough. And I have requested research to take a deeper dive into the three pre-approved platforms and the associated networks and the effect of having very highly integrated systems.

So it is really the issue, the new issue, the new kinds of failure modes that arise when you integrate functions that were hitherto independent, like RPS, ESFAS, non-safety, safety, service units, human interface units. A number of these kinds of elements are integrating into the system that are first including the complexity and secondly introducing unknown and uncertainties.

So this project was formulated to address all those needs. So include the technical basis for understanding failure modes the feasibility, risk quantification that the Commission asked us to investigate.

To do these kinds of studies without a context becomes too open-ended. So given that we got the NRR request for the three pre-approved platforms and their networks, we thought that we ought to use that as a nucleus to characterize the domain over which we would bound the scope of this activity.

There are right now seven or eight platforms that are in the picture, the three pre-approved ones plus a few more have surfaced in applications. So we would like to limit the scope of this work to the domain characterized by what we see in these emerging platforms. And of course, the application, the safety functions applications, RTS ESFAS.

So with that bounding, we would have some hope that we can come up with a cause-effect understanding, particularly introduced through the effect of interactions that come with this higher level of integration.

MR. HECHT: If I were to reparaphrase this project, is it to basically how to assess a DI&C system? Is that --

MR. BIRLA: Well, failure mode characterization, yesterday we had the discussion on effects and modes and mechanisms, depending on the level of indentation. So for this class of systems that you see for safety functions, what would that framework be that would be the major output?

Professor Apostolakis calls this a cause-effect chain, you might say contributing factor chain but limited to this domain of applications, RTS ESFAS and the seven or eight platforms that you see.

MR. HECHT: Are you looking at what regulatory agencies internationally have done with the advanced systems? For example, the use of safety case methods and what is being done in that area?

MR. BIRLA: Remember, this is the scope of this is failure mode characterization.

MR. HECHT: I see.

MR. BIRLA: Yes. Now the safety case idea relates to it but safety case method or such methods are not the scope of this project.

CHAIR APOSTOLAKIS: One of the problems at the beginning of this whole business of Digital I&C nuclear, which in fact I witnessed myself during the deliberations of the committee that wrote the Academy report in '97 was that people just didn't know. So the most popular example was the Arion failure.

So the poor guy here is talking about a simple digitalized system to start the pump and they would hit him with the Arion failure. You know, but you can't you do anything and all of that because look at what happened in France. And that was part of the motivation of this. You know, tell us what kind of systems we have in nuclear power. Are they actuation systems only, in which case talking about Arion is not appropriate? Are you talking about feedback and control systems, in which case now you are beginning to get closer? That was missing and I remember a member of the committee was from a major A&E and he was hit by some academics with Arion and the guy was frustrated. My systems are not that complicated. Why are you bringing up that damn example all the time?

So that is part of the motivation is that we have certain classes of systems. Some of them are very simple. So their operating experience that applies to them, you know, should be the appropriate one. Everybody had Arion up here. Arion, Arion.

MR. HECHT: Because it happened in 1996.

CHAIR APOSTOLAKIS: Yes, it is what Tversky and Kannerman said, you know, anchoring effect, I think it is. You remember the most recent occurrence and you always bring it up.

MR. HECHT: Yes.

CHAIR APOSTOLAKIS: Very good. Shall we move on?

MR. HECHT: What kind of output do you expect from this activity?

MR. BIRLA: A framework of cause-effect relationships that you would see in this application environment for this family of platforms.

MR. HECHT: So it is kind of like an FMEA.

CHAIR APOSTOLAKIS: Oh, absolutely. Yes.

MR. BIRLA: That would be going a little too far but a framework within which you can develop either an FMEA or a root cause analysis.

CHAIR APOSTOLAKIS: Don't pay much attention to me. I take that back.

Okay, where are we now? Diagnostics and prognostics. Nice Greek words you stole.

(Laughter.)

CHAIR APOSTOLAKIS: You stole them. They are almost unrecognizable but that is okay.

MR. REBSTOCK: This is a new effort. The work will be getting under way soon. It hasn't begun yet.

The issue is that there are a lot of

things out there that can examine plant equipment, digital equipment and mechanical equipment and tell us good stuff about what kind of condition it is in. But we don't have much experience with it and it has the potential for adding considerable amount of complexity to the systems that are doing the monitoring, plant computers that are doing the monitoring.

So what this project is supposed to do and I expect it will be a fairly simple project is to take a look and see what is out there, what kinds of things are available, how they work, how they should be implemented, where they should be implemented, for mechanical equipment and for digital systems as well. And it includes self-testing and digital systems and automatic calibration.

Online monitoring is a particular aspect that could be included under this but it has already been addressed in NUREG/CR-6895. It was issued a couple of years ago. So we will leave online monitoring out of here if it has already been addressed. This is looking more at things like vibration signatures and control valve actuators and mechanical equipment issues, using noise analysis to evaluate conditions of bearings and that kind of stuff, auto testing, calibration, and digital systems.

MEMBER BROWN: You are talking about real time calibration when you are talking about that?

MR. REBSTOCK: Potentially. I mean, the point of the project is to see what is there and what the implications of it are, not necessarily to approve it.

MR. SYDNOR: Okay, I am going to move on to essentially a new program area, the security of digital platforms. This is ongoing work. We began about a year and a half ago using Sandia National Labs to help us do some cyber-vulnerability assessments of digital platforms for several different projects. One was a collaborative effort with the utility who volunteered to let us use their Common Q equipment, which they had in a lab mockup type environment. And so we actually set up a collaborative research equipment with the utility and Sandia. And Sandia went to the utility site and performed some cyber assessments of their equipment. Again, it was a Westinghouse Common Q platform, which the utility was using in a safety-related plant application. Now we didn't actually do assessments on the plant equipment. This was in a laboratory mock-up environment and was a partial simulation of what was in the plant.

That work has been complete and we have

two reports from Sandia that documents their findings there. And they did find, again, this is not a fully integrated system so it is in a mock-up environment but they found that not surprisingly there are cyber vulnerabilities in a digital system depending on what type of access you give to that system.

And so these reports will help generate knowledge internally and help. And we are also working on some regulatory guidance. Not only the NUREG guide 5.71, which really deals more with programmatic and cyber security from a programmatic standpoint, but the licensing offices have also initiated an effort where they are looking at a potential new ISG looking at the technical, the safety-related system review aspects of cyber security, more under the NUREG guide 1.152 and criteria. And so this testing has some real life examples of what probabilities can exist. It is a good thing it did for the utility. They were interested in mitigations. You know, how could they protect against these vulnerabilities. And so Sandia gave recommendations, too.

As part of that work, the utility also asked that we actually do an assessment of their plant-specific plant data network, which was an interesting exercise because that is not something that the NRC would normally look at but we had Sandia do a cyber assessment there and they were able to give the utility advice on potential vulnerabilities on their plant data network, the firewall configuration, for example.

We are also at Sandia. We just completed and the documentation I think was just finalized for the report. Again, Invensys has been very supportive of a number of our efforts and they loaned us equipment, the Triconex equipment and we did some cyber-vulnerability assessment at Sandia in a lab environment and so we have some documentation of that.

And we are moving on, the next step there is Sandia is the AREVA TELEPERM equipment that was at University of Virginia has been moved to Sandia and they are going to take a look at that from a cyber-vulnerability standpoint. The reports that are coming out of this are, you know, fairly detailed and technical. They get down into things that these cyber assault specialists are actually getting in and playing with the code and changing things. And so they are fairly detailed reports. They are non-public documents but the generic outcomes of those we want to make sure that we are covering those aspects and our regulatory guidance that we are using not only on the security side but also the new ISG on the technical side.

So the lines that are coming out of this are going to help us improve our regulatory guidance and make sure it is adequate. And there is also some potential feedback on these vulnerabilities that the vendors may want to do something about.

Again, these aren't fully integrated systems in plants. They are partial markups and things like that. But we are learning some interesting things about the vulnerabilities.

MR. SANTOS: Expanding on that, I think the context is critical. I mean, this is an inside out look. We are not looking all the programmatic things, the licensees can implement to provide adequate protection of their systems. It is just looking at inside out from the platforms out.

An interesting follow-up question might be okay, once you identify your security mitigations. Well, what is the impact of that on your safety functions. So that to me is also a research question to ask because you might find out, oh, let's put all this encryption and all of this good stuff. Well, what are you doing to your safety function?

So, it will be very interesting.

MR. SYDNOR: Not all of the mitigations have to be designed into a system.

MR. SANTOS: Exactly.

MR. SYDNOR: The mitigations can be external.

MR. HECHT: Have you -- I mean well, let me put it this way. Does DHS have anything to offer this with their cyber security center?

MS. DION: Can I say something? This is Jeanne Dion in the Office of Research. Prior to coming to NRC, I was a Sandia employee and there is a number of different groups at Sandia that are involved with this project. The people who are doing the vulnerability assessments, they are a part of Department of Homeland Security. So they are the same people involved with the DOE projects.

MR. SYDNOR: But NRC does maintain liaison at DHS. It is the US search site and others that are security.

MR. SANTOS: NSIR is our lead.

MR. SYDNOR: Nuclear Security Incident Response office.

MR. SANTOS: And we are plugged in with them.

MR. HECHT: Okay. And are those links being used to direct or influence the results of this research or the results of the reg guide that are --

MR. SYDNOR: Yes, certainly for the reg guide. This research is pretty down in the details of these system-specific. And so --

MR. SANTOS: Actually, I got it the other way around. The DHS folks wanting for us to come talk to the critical assets groups.

MR. SYDNOR: The next network security topic here is what we are doing under this one is actually we have Sandia again looking at a generic networking issues in protection and control systems in nuclear power plants. What type of networks are likely to be used and what type of regulatory issues and cyber security issues do we need to be aware of because of those uses of networking.

And so we have got Sandia working that one. There was a little discussion previously on this wireless network security. And as a follow-on to some previous work, in previous years, Oak Ridge had done some exploratory anticipatory research for us looking at potential uses of wireless applications in nuclear power plants. And like I say, there are applications in use at nuclear power plants that are limited to maintenance and commercial applications at this point in time. They are not being used for -- I won't say no one is using them for a control system but they are certainly not being used for safety-related systems.

But the previous work looked at best practices for using wireless in a nuclear environment and things that people really need to be aware of so they don't misuse it or don't inadvertently affect other things.

The work we are doing now is then, you know, okay, given that you have some wireless networks in the plants, what type of cyber security issues do you need to be aware of for those type of things?

So these are not, you know, looking at physical. They are more looking at best practices and standards and making sure we understand what those are.

MR. HECHT: Is there a plan to consider, you know, wireless can sometimes buy you things, particularly in terms of less vulnerability to fire. I am out of my area of expertise, but is that a long-term plan or is that any part of this what benefits wireless could give you?

MR. SANTOS: There is an effort that NRC is also plugged in. LWR sustainability projects, life plus 60, life beyond 60 years. And as part of that, there is a Digital I&C group that is looking also at cable-replacing issues and things where wireless might play a role. So that is how we are looking at the long-term potential benefits.

MR. SYDNOR: That is not being --

MR. SANTOS: That is not the other. This project, that is all.

MR. SYDNOR: But there is an effort with DOE to look at long-term life extension.

MR. SANTOS: So we are monitoring that effort.

MEMBER STETKAR: The preliminary stuff from the fire people --

MEMBER BROWN: Do you really want me to start talking? I have already said all I need. I'm sorry, John. Go ahead.

MEMBER STETKAR: The preliminary stuff, the fire research folks have a program looking at fiber optic cable impacts from fires. And some of the preliminary stuff they have done looks pretty good. So in terms of putting off vulnerabilities, there may not be much to be gained in terms of fire risk benefit versus all the other detriments from the wireless technology. Although, the fire research people don't have conclusive information either.

MEMBER SIEBER: I don't want to get us off the track but is it true that fiber optics is better in fire scenarios than wire?

MEMBER STETKAR: That is certainly what they indicate, that it is, yes.

MEMBER SIEBER: It's made out of plastic.

MEMBER STETKAR: Well not only doesn't it short, but apparently it is pretty hard to actually burn the stuff to open it up.

MEMBER SIEBER: Well, yes, it is sheets. In sheets.

MEMBER STETKAR: Anyway, we are off the topic here.

MEMBER SIEBER: We converted all of our data systems not control systems to fiber optics. And that was part of the reason that we didn't have data --

MEMBER STETKAR: There is not a lot out there yet. The research folks, they have something in their budget for it. But DOE is working on it a little bit.

MEMBER SIEBER: It's good stuff. It is high speed.

MR. SYDNOR: I am going to move on to the last topic area in the security program is it is called security assessments of EM/RF vulnerabilities. But what this really is, it is an ongoing project. We are already substantially into it. In fact, we may be wrapping up this with the final report, soon. So it depends on maybe some policy-level decisions and whether this applies in the NRC's scope or role of regulatory oversight.

This is really revisiting a study that was done in the early 1980s looking at EMP affects on nuclear, potential EMP affects on high level nuclear detonation on nuclear power plants. And I am sure most of it where there has been a lot of new press out there, with the Commission on EMP as reported to Congress several times in the last couple of years on the potential affects on national critical infrastructure for such an event, potentially a new terrorist-type adversary delivering such a threat.

So the effort here is revisiting that. The early 1980s study concluded that nuclear plants at that time would trip, would shutdown but would survive, the equipment would survive the pulse because of some inherent protective features you get in the rugged construction of a nuclear power plant. And the analogue instrumentation control systems would survive and you would be able to achieve, say shutdown. What they did at that time, they did a detailed assessment of four different nuclear power plants.

MEMBER BROWN: Analog semiconductors. When we looked at that from the Navy standpoint, the analog stuff that was transistors and stuff were very vulnerable to EMPT.

MR. SYDNOR: I'm not saying that they weren't vulnerable.

MEMBER BROWN: You can go back to some Digital I&C.

MR. SYDNOR: This conclusion didn't say they weren't vulnerable. It is saying that they were protected by the plant structures.

MEMBER BROWN: Oh, plant structures. Yes, you put stuff inside a steel hull or a steel containment.

MR. SYDNOR: Or concrete walls with rebar.

MEMBER BROWN: It depends. Yes, I got you. I got your point.

MR. SYDNOR: The people that we are using at Sandia do this for a living both defensively and offensively. They know what we are talking about.

The current study was taking a fresh look at that. You know, the wave transmission and everything from an EMP pulse is still the same. They have some new techniques, analysis techniques they use now obviously much better than they did in the early '80s. And they are also considering the fact that we have digital equipment installed in these plants. And there is a potential new threat with portable high radio frequency, high level radio frequency of weapons.

And so they are drawing some conclusions about potential vulnerabilities from those and what are the -- Are there new impacts? Potentially yes, but again it gets into these are acts of war or whatever. Is it in NRC's regulatory role or scope and we have had some preliminary discussions with our office director and at the director-level in the Nuclear Security and Incident Response Office to talk about these.

Former chairman Klein had a specific interest in this. And one of the reasons we were doing this research was his interest in the subject and making sure that we had analyzed for affects on the plants themselves.

And so where we are at on this, we have gone out and looked at several nuclear power plants. We have preliminary reports from Sandia. We are going to be wrapping that up, presenting that information to the right management level at NRC and determining is it a threat potential that the NRC wants to, needs to take action.

There is the potential that preliminary conclusions from the EMP are probably going to agree with the conclusions of the earlier study. The plants will still be able to achieve safe shutdown for an EMP-type effect for high frequency. Perhaps not.

MR. REBSTOCK: They only give me the little projects. Advanced instrumentation and advanced controls I can talk about pretty much at the same time.

They are two separate projects. Their kickoff meeting on both of them is a week from tomorrow with Oak Ridge. What they are looking at is the milieu that we are working in for these is the next generation reactors, high temperature gas reactors. And the concern, as far as instrumentation is concerned, is that the operating conditions in these plants are very different from the operating conditions in conventional plants and most everything else.

There are some very high temperatures in there. There are some very severe challenges to certain measurements. And so the purpose of the instrumentation projection is to look at that, look at what the current DOE designs have, what direction they are going in, what sorts of solutions are they looking at to try to get a leg up on what may be coming in in a licensing request in the not too distant future for one of these plants, so that we know what it is that we need to look for and what it is that we need to be concerned about.

The controls is the same issue. There are, the plants operate differently from conventional plants. The control systems will be very different. There may be interest on the part of the designers for using control strategies and control logs that we haven't looked at in the past. So we are just trying to get a look over the horizon to see what is coming.

MEMBER STETKAR: Paul, the advanced reactor controls, is that -- you prefaced it by saying it is strictly for the new, next generation reactors. Is it the new reactors?

MR. REBSTOCK: The new reactors would be addressed in there, too. The controls would be.

MR. SANTOS: It includes some of the modular --

MEMBER STETKAR: Because I can see the

words that are in there about plant start up, shutdowns, mode changes and things, indeed our current technology that is being used.

MR. REBSTOCK: It could be.

MEMBER STETKAR: It is.

MR. REBSTOCK: Well, yes. Right. It is not used in our current domestic fleet.

MEMBER STETKAR: It is not used here but it is current technology in other operating reactors.

MR. REBSTOCK: Overseas and in other industries.

MEMBER STETKAR: In nuclear power plants, in terms of an automated shutdown.

MR. REBSTOCK: No, I said and in other industries.

MEMBER STETKAR: Oh, okay.

MR. REBSTOCK: Other industries. Yes, there are all kinds of wonderful things that you can do --

MEMBER STETKAR: I'm just curious.

MR. REBSTOCK: -- that are not done in current plants. And what we wanted to do is to get our arms around that whole story.

MR. SANTOS: It includes some of the proposed module reactors also.

MEMBER BROWN: Let me ask one question. When you talk about advanced sensors and whatever. Different mediums require different types of sensors.

MR. REBSTOCK: Right.

MEMBER BROWN: What would you be looking for relative to from the regulatory standpoint that you would need to look at. I mean, you have got fundamental guidelines in 10 C.F.R. 50 relative to the application. But in a short time, I haven't seen anything specific to details of types of instrumentation. If somebody wants to measure temperature with this doohickey or that doohickey, you get an output. It has got to meet certain other environments and other type qualifications.

And if people build a gas reactor, they are going to have to find something that is going to measure the parameters under which they are operating. You are fundamentally interested still in the overall -- I am not trying to tell you what you are interested in.

MR. REBSTOCK: No, I understand.

MEMBER BROWN: Please don't take that the wrong way.

MR. REBSTOCK: I understand what you are saying.

MEMBER BROWN: I mean, the idea is you are going to have sensors. You are going to have temperature pressures. You are going to have flows. All the standard stuff.

MR. REBSTOCK: But we want to have confidence that whatever it is that is proposed is going to work. Whatever it is that we approve.

MEMBER BROWN: Yes, but if you look at all the IEEE standards, etcetera, etcetera, there is tests, environmental qualification, those apply to the regime which you will have to define for their testing regimes before they come out.

I was just looking for an idea of what you mean you are looking for that it is different from the application and the qualification of the standards you already have in place.

MR. REBSTOCK: We would want to have an idea. If they say that they want to measure the discharge gas from a pebble bed reactor at a thousand degrees Celsius with a certain kind of temperature sensor, we want to have already some understanding as to how that sensor will behave under those circumstances and what sorts of things it might experience.

It may turn out to be a very simple issue and that everybody knows that a type whatever, thermocouple, will do the job and there is not an issue. In that case, this would be a very short project, as far as that particular cleansing is concerned.

On the other hand, that regime, considering the pressure, considering the corrosive nature of the gas, may turn out to be very difficult to find something to do that. So we want to know about another issue.

MEMBER BROWN: Yes, but -- go ahead.

MR. REBSTOCK: You need to know the flow through the core. You need to know the coolant flow. You have go very tight geometry. So ways of measuring, accurately measuring that coolant flow are very limited.

So, we want to get an idea of what it is that the researchers that are designing these things have in mind so that we can look ahead and get a feel for ourselves as to whether they are moving in the right director of if they go that way, what it is that we need to look at.

MR. SANTOS: And another example is the proposed solutions have techniques that infer the parameter for even directly measuring something. And therefore, you need some sort of different techniques for calculating accuracy or what have you. You want to be able to get a sense of what that will be, specifically for the dynamic pebble bed ones.

MR. REBSTOCK: Plus you need three dimensional flux map in the core.

MR. SANTOS: Right.

MR. REBSTOCK: You have to know that.

MEMBER BROWN: Yes, but are not going to use it if they don't demonstrate some way to do it. I mean if you can't design -- if you design a reactor with instrumentation, if you monitor it --

MEMBER SIEBER: You don't have a fixed geometry.

MEMBER BROWN: I understand that.

MEMBER SIEBER: So that is going to be tough.

MR. REBSTOCK: Those are the challenges.

MEMBER BROWN: But if you have got rocks?

MR. REBSTOCK: Our point is not to design the instrumentation.

MR. SANTOS: That's right.

MR. REBSTOCK: But it is not to solve their problem. It is to know what it is that they are --

MEMBER SIEBER: But other than core flux, core mapping, all of this other stuff is used in other industries. Steel mills, coal fired power plants, there is high temperatures, corrosive. So it not like it is, you know, 20 years of research.

MR. REBSTOCK: Correct.

MEMBER BROWN: But we built reactors in the early days without adding for protectors because we didn't have any. We had X core. And then we would --

(Laughter.)

MEMBER BROWN: It is nicer to use that stuff in the core.

MEMBER SIEBER: Safety feature is distance, then. You want to be miles away.

MR. SANTOS: Like I said, this might be --

MR. REBSTOCK: So the point, John?

MEMBER STETKAR: Well my question here was, it was interesting when I read this one. It was reactor instrumentation for advanced reactor application type stuff. And when I looked, my perception, rightly or wrongly is from the regulatory viewpoint. I am looking down. People propose a design. If they have a design that doesn't have instrumentation that works with the design and allows them to do this stuff, well, I am not out promoting that, that is up to the industry to determine what they are going to use, not the NRC.

So, if they are being aware, they are going to have to come through and tell you those kind of things.

CHAIR APOSTOLAKIS: So you don't think this is necessary.

MEMBER BROWN: I don't know. It just seemed, this one seemed marginal to me when I looked at it.

CHAIR APOSTOLAKIS: Okay.

MEMBER BROWN: It is not that I am against it. It just, if I looked at -- and he is right. You may go out there and look at it and this may be a five minute research project. Say well, okay, we are not going to spend any money on this right now because there is no place to go.

MR. REBSTOCK: The thing we don't want is for them to come along and say here is how we are going to do the instrumentation and it is something we have never seen before. And then we have got to go and run and figure out what it is.

MR. SANTOS: Right. And hold up that review for them because we don't know.

MR. REBSTOCK: Hard to imagine how they could do that.

MEMBER BROWN: Theoretically, if they want their project to go through, they should be feeding that information out before you ever get there. Otherwise, they are not very smart and you don't want to work with them in the first place.

MR. SANTOS: No comment.

MR. SYDNOR: It would be nice if it worked that way.

CHAIR APOSTOLAKIS: I think you made your point. Where are you now, survey?

MR. SANTOS: This is anticipatory research. It is ongoing. We do our reports every few years. We try to be ahead of the curve looking at their things. An example might be instrumentation technologies like Johnson Noise thermometry for high temperature applications.

MEMBER BROWN: What was that again?

MR. SANTOS: Johnson Noise thermometry.

MEMBER BROWN: Oh, okay.

MR. SANTOS: NIST is developing that. That is an example. You know, some people would say nanotechnology.

MEMBER BROWN: Sure.

MR. SANTOS: I mean, I am not saying we will see this but we are trying to be anticipatory, develop knowledge at a minimum, at the staff level.

CHAIR APOSTOLAKIS: Are you going to be also up-to-date with the state-of-the-art in software methods, in general?

MR. SANTOS: Yes.

CHAIR APOSTOLAKIS: Are you guys going to conferences? Are you reading the literature knowing what is going on?

MR. SANTOS: Yes.

CHAIR APOSTOLAKIS: When was the last time you went?

MR. SANTOS: Actually were you at the --

CHAIR APOSTOLAKIS: Don't tell me Brookhaven.

MR. SANTOS: No, no, I am bringing to mike.

CHAIR APOSTOLAKIS: Yes?

MS. HERRMANN: For NRC people in general.

CHAIR APOSTOLAKIS: What?

MS. HERRMANN: I said NRC people in general. I was there two weeks ago.

CHAIR APOSTOLAKIS: You were, two weeks ago? Where?

MS. HERRMANN: It was DHS and I forget which university was sponsoring it on cyber security.

CHAIR APOSTOLAKIS: But how about technical societies like the American Nuclear Society has a meeting every whatever year and the IEEE Society does.

MR. SANTOS: Yes, the staff is heavily involved. I mean, we have a lot of members of actual working groups of IEEE standards.

CHAIR APOSTOLAKIS: But these are groups. I am talking about --

MR. SANTOS: But also conferences.

CHAIR APOSTOLAKIS: -- the open meeting, here anybody can come and present something.

MR. SANTOS: That's right. I mean, the Agency supports the ANS meetings. I mean, we had the one in I&C in Knoxville back in April and we sent like 20 staff there, 20 plus staff to that meeting. And staff presented several papers. A lot of members share findings through their readings or their own personal research is also fostered and encouraged by management. So, I think we are in good shape in that arena.

MR. BIRLA: And to add to the examples that Dan gave, the National Security Agency holds a once a year not totally open, by invitation open forum of researchers that I got an invitation to and spent a whole week with the min the Baltimore area. And that was very educational to me on what other researchers are finding out about the difficulties of cyber security risk assessment.

So your point is that part of the research portfolio should be to learn about what others are doing in the area and that point is well taken.

CHAIR APOSTOLAKIS: Well, be up-to-date. I mean, that doesn't mean that you are going to apply everything that you read but you have to be up-to-date.

MR. BIRLA: And we agree.

CHAIR APOSTOLAKIS: Charlie, you are about to say something?

MEMBER BROWN: Well, this is emerging technologies.

CHAIR APOSTOLAKIS: Yes.

MEMBER BROWN: How can you argue against seeing working with them?

CHAIR APOSTOLAKIS: Collaborative and cooperative.

MR. SANTOS: We are undertaking several collaborative activities. We heard a lot of the MOU but that is not it. We also heard NASA. But we also have good collaboration with other federal agencies in relevant areas. Safety assessment and security are two of them.

The White House, through the Office of Science and Technology Policy, they have a NITRD program which comprised, Sushil help me out, what 18 federal agencies?

MR. BIRLA: Something like that.

MR. SANTOS: Official members but all the members are held where they actually meet and share the products of their research.

CHAIR APOSTOLAKIS: What does it stand for?

MR. BIRLA: Networking and Information Technology Research and Development. It is an interagency coordination effort. And they have coordination groups in cyber security in high confidence software and systems.

CHAIR APOSTOLAKIS: That is exchange of ideas or somebody actually says, let's do this?

MR. BIRLA: Well, each agency has its own program. So the first thing is just to be aware of what each other is doing so that we can piggyback on each other, exchange information, do not duplicate effort and waste all the resources. So that is the baseline.

MEMBER BLEY: How long has that been going on?

MR. BIRLA: This is probably seven or eight years ago about five agencies started. So the Department of Defense and Department of Commerce through NIST, National Security Agency, National Science Foundation, NASA, have been the prominent ones.

The FDA is there because they have medical devices that they regulate and they have had some difficulties in that area. The numbers have grown. Department of Homeland Security is there now.

The Nuclear Regulatory Commission got invited through a contact that Dan had at a workshop that he went to. So, he passed that contact on to me to be the representative and then Stu and I had a discussion. Stu agreed that we should participate in the interagency coordination effort. The NRC is not an official member of the group but --

CHAIR APOSTOLAKIS: Too small?

MR. BIRLA: I beg your pardon?

CHAIR APOSTOLAKIS: We are too small or what?

MR. BIRLA: Well, it is just a matter of going through the formalities. For all practical purposes, any information that is available anywhere in any federal agency is accessible to us. The main thing is that we are getting to know who the researchers are. Who the program managers are, what are their ideas, whether we have similar issues. And we do.

How do other regulators approach the same issues? A little bit learning about that is going on.

MEMBER BLEY: Did you find you had been going to the same people for the researchers supporting or is it a different community?

MR. BIRLA: It is a different community.

MR. SANTOS: Yes and different networks of natural expertise.

MR. BIRLA: So we get a little bit of an inside track on the agenda of the National Science Foundation because before the program announcement they give an opportunity the coordination group members. Here is the program announcement. Does it address the needs of the federal agencies represented in the NITRD program? If not, what would you like to see added in that.

MR. SANTOS: Two points I want to make.

CHAIR APOSTOLAKIS: Even NSF is becoming a user need agency?

MR. SANTOS: Two points I want to make. Although you heard Sushil mention that each program executes their project, this program coordinates cross-cutting issues and proposed budget to the OPM, you know, to the budget cycle, funding for programs that will satisfy all the members.

So if one agency doesn't have enough budget, it could leverage the team to get cross-cutting issues resolved. And we are finding in the areas of safety assessment, there is a lot of similar issues that we are tackling with.

So one of the proposed ideas are still being discussed is to create a subgroup out of the regulators, the FDAs --

MR. BIRLA: So informally we have an agreement that from the regulatory perspective, what should be the research? Nobody is looking at that. All the economics and the developers all out there look at it from the developer's perspective.

So, yes, the FDA representatives said they have an interest. The FAA representative isn't there but NASA is doing some work that would be applicable for future aircraft. We said yes, we would like to be a part of that discussion group. So on an informal basis, we have begun to share ideas on what our issues on which we need to get some more spotlight, or more funding or whatever, or make sure that we formulate our individual projects a little better with your input or reviewers on.

MR. SANTOS: COMPSIS we talked about. Halden Reactor Project, I had the opportunity to visit and work with some of their engineers. Although they are a small shop, they do have some very good ideas they are trying to work and be ahead of the curve. So we get a leverage where a member participates and provide them feedback on the direction of their program. So, I think we can do more with them and we should. So that is something, I hope, moving forward we can do with them.

The MOU again is kind of new but talking to EPRI, I expect the more meaningful meetings starting next month, as schedules allow. These are some of the topics that we are going to collaborate on. Clearly a starting point could be the reconciliation of our finding on the -- go ahead, sir.

MEMBER STETKAR: I was going to ask Sushil. It is really interesting the interagency stuff. Have you found that any other agencies are as quantitatively oriented as we are?

MR. BIRLA: There is a group in NASA and Alan has already had them here for a day and there is ongoing collaboration going on there. But there are other groups in NASA who think differently.

MEMBER STETKAR: Okay. But NASA.

MR. BIRLA: Yes. Other than that, I am not aware of any.

MEMBER STETKAR: Thanks. I was just curious.

MR. BIRLA: Yes. Alan, are you aware of any other federal agency where there is that kind of an enthusiasm on quantification?

MR. KURITZKY: Alan Kuritzky, Office of Research. No. NASA, as Sushil mentioned, we have been trying to work with them. We have a memorandum of understanding with them and we are working in that area. But that is the only one so far that we have identified.

MEMBER STETKAR: FAA, FDA have.

MR. KURITZKY: I mean, they may have something. I am not aware of it.

MR. SANTOS: Another are of the MOU I am excited about if it comes to bear is that we know Halden is helping us in human reliability analysis, trying to put real operators through simulators. But then the question of cultural differences and all that, well, can we do it here with our own operators in our own simulators. And you know, maybe leveraging EPRI's access under members to help us generate the data that we need is something that I found.

CHAIR APOSTOLAKIS: What data? Human operations?

MR. SANTOS: Human, yes.

CHAIR APOSTOLAKIS: Why is that your business?

MR. SANTOS: I'm sorry?

CHAIR APOSTOLAKIS: It is not your business, is it? Human reliability?

MR. SANTOS: Of course it is. I mean, PRA, Digital I&C, human reliability on these systems are becoming more and more integrated.

MEMBER SIEBER: Who is at the handle at the endpoint of a system? It is the human.

MR. SANTOS: It is the guy, yes.

CHAIR APOSTOLAKIS: Something that breathes.

MEMBER SIEBER: Yes. You read it and turn it.

MR. SANTOS: But the MOU, what I am trying to say is not only Digital I&C but also it covers some human factors elements.

CHAIR APOSTOLAKIS: Oh, sure, yes, we know that. We have known that for a long time.

MR. SANTOS: But that is an aspect I hope we can leverage.

CHAIR APOSTOLAKIS: Swedish operators on Norwegian reactors. It tells you a lot about Texas.

MR. BIRLA: This continues in the same theme of working outside the organization and exchange of ideas.

In the international arena as you already will know, there are a set of I&C standards that set up a different regulatory framework, an assessment framework for users and suppliers outside the U.S. And then there is the NRC framework. So there has been an interest within the NRC in a long-range goal of harmonization across international standards because suppliers are international. The same companies are putting in plants and digital systems and different environments.

There are some fundamental differences, due to which this is not going to be an easy task but this is part of the scope of this project. So it is taking off through many different directions. One is a traditional participation in the standardizing organizations. The NRC has mostly been the IEEE, working groups, and there is a nuclear industry-specific body which plays an active role. But it has been many years since the NRC has been in any IEC working group. It has pretty much abandoned presence there.

The bright spot in the whole dark spectrum is that there is a memorandum of understanding between the IEEE and IEC now that in this are, Digital Instrumentation and Controls, if there is any new standard in the future, they will joint logo it. That means they will work together.

There is also an understanding in principal that if there is a revision to an existing standard that overlaps each other's territory, they will work together to see if they can harmonize but they have not made a commitment to.

So, I have talked across the program offices and everyone recognizes that it is something that needs to be undertaken but it is also going to take a lot of effort. It is a long-range, 10 to 15 year horizon activity.

Through NRO's leadership, there is

participation in the MDEP program which has a couple of working groups that address this area. And some work has been done to compare different standards to see what are the deltas. But where it goes, it is part of this project is to add some resources and investigate, at least on a thorough comparison basis, where we are aligned, where we are different, what needs to be done to overcome the differences. And then item by item pursue which difference we eliminate.

And through each of the societies are working organizations, IEC and IEEE, make sure that when standard comes up for revision or something new is proposed in the area, have a presence there.

So in principle, we have an agreement. We have not yet estimated the resource requirements and not represented to management what resources it will take but in concept and principle, there is good support from both program offices, NRR and NRO.

MR. HECHT: I would just point out that getting to know a standard, a serious standard is something which takes years.

MR. SANTOS: You will probably see this in the next three plants.

MR. BIRLA: Yes, it is something we are

undertaking, that is true.

MR. HECHT: That is one standard.

MR. BIRLA: Yes. There is a small effort in the direction, the NRC, as I mentioned earlier through NRO, is participating in several MDEP working groups. And in NRR, there is an initiative to start meeting with a task force of safety-critical software that includes seven West European regulators. And they put together a position, common position, with their knowledge of the prevalent standards in Europe of what is not covered well enough in those standards that should be to make regulation more effective. So the NRC has been invited by the task force to join it and to work with it.

So to gain an understanding of the standards, the issues, this is another avenue.

MR. FREGONESE: Can I make a comment about the MDEP really, really quickly?

This is Vick Fregonese from AREVA. The one thing I have noticed about the MDEP is that there seems to be a lack of transparency with those proceedings. With the NRC's interacting with the other regulators, those are not open meetings. And the one thing I would like you to consider as you go forward because we are very interested in this international regulation because we are building plants all over the world, there is misalignment between the safety classes. As you know, there is F1a and F1b in Europe, here we have Class 1E, and STUK has the Safety Class II. And so as we try to draw lines to line these safety classes up, we are very interested in what you all are talking about.

And it seems as if when you are discussing some of these issues which involve all of these designs with the international community, it would be great if we could somehow participate in that. So, I don't know if you can influence that. But when the NRC is involved with the other regulators, I know it is kind of their meeting but you know, my kind of outsider view is that we are really interested and we actually have some information we could probably share to help those conversations.

So that is just something that I put out. If it is really a research project, I just wanted to make that clear.

MR. SANTOS: I would like to --

CHAIR APOSTOLAKIS: Go ahead, Debra.

MS. HERRMANN: Yes. Since the MDEP's is an NRO initiative, I will be glad to take your suggestion forward.

MR. FREGONESE: I appreciate that. Thank you.

MR. WATERMAN: Perhaps the industry will reciprocate with its meetings.

(Laughter.)

MR. FREGONESE: Yes, I think -- sure, if we have a meeting. One of these forums you have talked about are meetings.

CHAIR APOSTOLAKIS: I have participated in meetings of foreign committees, semi-regulators, and it is really a very different environment. We just close the door and start talking. Nobody can come in to the room unless invited. So you should appreciate what is happening here.

MR. FREGONESE: I do and that is why I made the comment. Thank you.

CHAIR APOSTOLAKIS: Okay, that is a simple diagram there.

MR. SANTOS: It is self-explanatory.

CHAIR APOSTOLAKIS: And I have no problem with that. Charlie, do you?

MR. SANTOS: It is self-explanatory so let's move on.

CHAIR APOSTOLAKIS: It is self-explanatory.

MEMBER BROWN: Are we going to the next page? Do you agree with that?

MEMBER SIEBER: I have no idea.

CHAIR APOSTOLAKIS: Well, it is regulatory guides and the standards they approve, or they endorse with exceptions.

MEMBER SIEBER: That's right.

CHAIR APOSTOLAKIS: Okay.

MR. SYDNOR: The last program area has three research projects and quite frankly we will admit this is kind of a catch-all area. These were carry-over projects from the '05 through '09 programs, some of which we tried to work and didn't finish and then a couple that were never started.

This first one we really are maintaining it primarily because of a request from EPRI and the industry to. There is still an issue with our regulatory guidance where we have some potentially overly conservative criteria for conducted susceptibility testing in one certain area. And that criteria was based on some in-plant testing that was done a number of years ago that may have been interpreted wrong. And so we have been asked to visit that. So we are maintaining this project in the research plant and take a look at that.

As part of exploring that, we thought that was primarily the only issue. But really, you know, meeting with the EPRI and industry working group for EMI, they have a new what is it called, Ray, a technical report or a topical report, your TR?

MR. TOROK: Yes, that was a topical report.

MR. SYDNOR: There is an EPRI report, a new report out and industry has a lot of valid claim to update to the latest standards here, both U.S. standards and IEC standards. And so we are going to maintain this in the research and try to devote some effort to it maybe perhaps as part of the MOU again because there is a potential if we have to do some testing, which is debatable whether we need testing. But if we do, it is perhaps some collaboration between NRC and EPRI would be the best way to achieve it.

This was a carry over project. It was in the '05 through '09 plan but no work was started in this area and it was really just a prioritization or need that was not an identified issue or need that drove this. But in our process for updating the plan, we were requested by NRR to retain this project and to try to devote some resources to it.

It is certainly a valid technical issue

and is worth exploring to see if there are implications that perhaps we are not using our regulatory guidance adequately to make sure that we are protecting these systems from power supply issues. Are we doing that adequately? We certainly have good guidance on 1E power supply systems.

MEMBER BROWN: Now is this a consideration that you don't understand what the level, in other words, you have inadequately or not properly characterized the fluctuation of a power input power to a bunch of the power supplies? I mean, you do have over-voltage spike-type tests in place right now. So presumably, those were developed with some knowledge of the switching transients and other type things that can be on -- I can see Jack shaking his head.

That is what we did on naval plants is we ran tests and found out that there was some ranges that we had to cover and there were some ranges that we would never be able to cover, so we ignored those and just started with fry stuff.

MEMBER SIEBER: The issue is the grid is changing from time to time. Load distribution is changing. And so a major blackout introduces a lot of transients to the electrical grid.

If you look over the last ten years, the most significant national risk event was that blackout. Fortunately, everything worked at nuclear power plants but when we get to my operating experience report, you will see from the risk standpoint, that is the dominant event from the last ten years and we ought to pay attention to it.

MEMBER BROWN: Yes. I guess my question is if you are looking at what -- is this the grid? I mean, this is looking at what is coming off the grid that you have to protect against and assessing it against your present standards?

MR. SYDNOR: No matter what is driving the power supply --

MEMBER BROWN: Whatever.

MR. SYDNOR: -- fluctuation, certainly the grid and the grade of grid are issues that industry has spent a lot of time and a lot of redesign on those issues and in many cases, installed new backup diesels and station blackout diesels. There has been a lot of work done in the industry to protect against the grade of grid and loss.

But with the implementation of new digital systems, plant-specific configurations of power supplies that power the networks and the digital systems, I think NRR's concern here is, you know, do we fully understand all of the implications of that?

We haven't started this. We haven't scoped it. It was requested to be retained and so we will be working with NRR as move forward on it. It is a legitimate issue. We all recognize that.

MEMBER SIEBER: There were not a lot of I&C failures induced to my knowledge out of the last one. On the other hand, the potential was there. And every blackout with a lot of switching transients, is not going to produce the same thing. So the more know, the better off you are. All of it is important.

MR. SYDNOR: One of my first learnings involving digital systems back in the '90s, I think it was, installing a digital feed system at the plant, we didn't get the power supply configuration correct as far as redundancy. And we continued to have events, not because the digital system wasn't working but because we would have power supply issues.

And so we learned some painful lessons about going back in the design.

MEMBER SIEBER: And simple things like CPUs can reset, if there is a momentary interruption. It is really beyond the capability of the EMI resistance.

MR. SYDNOR: And this last topic here is

again another one where there has been some very early exploratory research done on this. I think it is part of the '01 to '04 plan. But there hasn't been an active licensing on this so we have not devoted resources to it. But again, we were asked to retain this one.

I think there is still some discomfort level. Do we understand the basic operating systems that are being used in the platforms that are being proposed and you know, what are some implications of that from a regulatory review standpoint that we might need to know. It could be more educational type of research than anything else.

MR. HECHT: Can I ask some questions about that? Because this also relates to the other topics of operational experience and PRAs. If the operating system fails, then obviously you lose that processor.

What operating systems are currently being used in safety systems?

MR. SANTOS: How many?

MEMBER BROWN: I thought they were custom.

MR. SANTOS: Home-grown.

MR. HECHT: So basically it was the kernel that came along with the architectures that we were considering. Is that changing in the advance plant?

Can you address that?

MR. FREGONESE: The operating systems in the existing fleet versus the advanced plants?

MR. HECHT: In up-coming I&C systems. And maybe you ought to identify yourself again.

MR. FREGONESE: This is Vick Fregonese from AREVA.

Globally, the systems that we are going to be installing in the U.S. are an evolution of systems that we have had in operation in Europe and Asia for many years.

MR. HECHT: Do they have operating systems?

MR. FREGONESE: Excuse me?

MR. HECHT: Do they have operating systems?

MR. FREGONESE: Yes, they do. So, and I know the NRC has extensively reviewed the platform. You know, Mike was involved extensively in that review. The existing fleet, I spent 15 years in the existing fleet. There is a lot of discreet digital devices, EPROMs, PROMs, small custom systems and there are some systems that are used on the commercial side for digital feedwater turbine controls.

There have been some events that we saw on the EPRI research that the digital systems do have some power supply of vulnerabilities in terms of their monitoring because one of the digital monitoring techniques is to put the system at a known safe state when you reach a certain instability in the power supply. So they have a different failure mode. And I think if you look at the operating experience, it needs to be considered.

So normally, we have an uninterruptible power supply or a reliable source of power that supplies these digital systems. In a new plant design, that is our approach to avoid perturbations, especially from the grid. You shouldn't see grid-induced perturbations work their way down to affect the digital systems, at least in our design.

MR. SANTOS: I don't think I --

MR. FREGONESE: Oh, operating systems, okay.

MR. SANTOS: Yes, I have got --

MR. FREGONESE: You have got slides of it. Okay.

MR. HECHT: Not operating systems, operating systems.

MR. FREGONESE: Operating systems.

MR. HECHT: Like VX.

MR. SANTOS: Yes, the architectures.

MR. FREGONESE: So we do use an operating system on our computer system?

MR. SANTOS: Yes, like Windows.

MR. FREGONESE: It is not like Window. Asynchronous, deterministic, --

MR. SANTOS: An example.

MR. FREGONESE: -- operating system. It is a stupid computer running dumb software for safety applications. That is kind of the approach we take.

MEMBER BROWN: Is it a custom --

MR. SANTOS: Yes, it is custom.

MR. FREGONESE: Yes, yes, it is.

MEMBER BROWN: -- design main operating system.

MR. FREGONESE: Yes, that is right. And the other DCS's you will see around the world will use, do use windows in some cases for the HMI. There is various vendors that use versions of Windows. I forget what that version is called.

MR. SANTOS: What I have seen is, you know, bought super package, operating system in the application and they tend to be home-grown.

MR. HECHT: So nothing like VX Works or VERTEX or --

MR. SANTOS: No, I haven't seen stuff like that.

MR. FREGONESE: UNIX for some of the DCS's.

MR. HECHT: Well for the DCS's. You have a controller for the DCS's --

MR. FREGONESE: Yes.

MR. HECHT: -- doing the HMI.

MEMBER BROWN: What is a DCS?

MR. FREGONESE: Distributor Control System.

MEMBER BROWN: You mean managing the LAN?

MR. FREGONESE: The human machine interface which would be a flat screen that you would use to interface with the automation system.

MR. HECHT: But Vince was saying that they are actually also using them for control.

MR. FREGONESE: The distributor control system for sure. They are using those for control.

MR. HECHT: UNIX.

MR. FREGONESE: In the one instance I know of, they are using it for the HMI only.

MEMBER BROWN: Well, make sure you define your terms. Are you thinking control in terms of it is used to control a turbine generator speed or are you talking about -- I think he is talking about control in terms of it is the way the information is presented to the operator.

MR. FREGONESE: Right. The automation system has a different operating system then the human machine interface.

MEMBER BROWN: Okay, I wasn't clear.

MR. FREGONESE: I'm sorry.

MEMBER BROWN: All right.

CHAIR APOSTOLAKIS: Whatever.

MR. HECHT: So what operating systems are we talking about which would, I guess my initial interpretation of this topic was are there some generic operating systems that might be used across platforms, as opposed to AREVA or Common Q or, you know, there is another one that might be used.

MR. SANTOS: It is vendor-specific. And I go back to link their relationship of projects. Sushil talked about the three pre-approved up to seven platforms for which we have the information. We will start focusing on those.

I have a proposal to make. I would like for you to consider starting the PRA topic at 3:00, so finishing up the research plan by 2:45 at most or earlier and then going into the PRA topic at 3:00 p.m.

or 3:15 instead of 4:00.

CHAIR APOSTOLAKIS: Good proposal.

(Laughter.)

CHAIR APOSTOLAKIS: Well, I was wondering about that. You need --

MR. SANTOS: I really would like --

CHAIR APOSTOLAKIS: -- to go through the slides --

MR. SANTOS: There is no need really. The rest is for completeness, schedule, priorities. Unless you have any questions on the slides, this is more of the process, I would rather stay focused on the topics themselves.

CHAIR APOSTOLAKIS: You want to go to the summary, then?

MR. SANTOS: Sure.

CHAIR APOSTOLAKIS: I think, you know, I don't know what we can say about setting priorities. I mean, that is your business.

MR. SANTOS: Yes, we just put it for completeness, unless you have any questions.

CHAIR APOSTOLAKIS: Well, that is it.

MEMBER BROWN: There is no summary.

CHAIR APOSTOLAKIS: We don't get involved in that. So, you have a nice picture here from the web someplace?

MR. SANTOS: This is an internal web page.

CHAIR APOSTOLAKIS: So summary. Unless somebody objects, we go to the summary.

NRC Digital System Research Plan is a flexible -- keep going. Keep going.

MEMBER BROWN: I think we are done.

MR. SANTOS: Basically, I would like to repeat this morning's --

CHAIR APOSTOLAKIS: This is, yes, this is something that is expected.

MR. SANTOS: This morning's objective, I go back to that. That is the summary within our objectives.

CHAIR APOSTOLAKIS: Your objective is to help the Agency.

MEMBER BROWN: Page three?

MR. SANTOS: Page three. Let's go over there.

CHAIR APOSTOLAKIS: Purpose and objectives. Oh, that is your objective, to get a letter from the ACRS?

MR. SANTOS: That is my summary right there. Are we missing something?

CHAIR APOSTOLAKIS: I don't know.

MEMBER BROWN: Questions?

CHAIR APOSTOLAKIS: Well, you guys are going to give me input after we hear the PRA folks. Right? But you have a comment right now.

MEMBER BROWN: No, I just had made some notes, a couple of notes. And this is based, and my thought process here on what you are all doing is just relative to what I perceive is the hardest problems we face today and that is how do you ensure you have got satisfactory software for these programs.

CHAIR APOSTOLAKIS: That's right.

MEMBER BROWN: And I guess I didn't really see the focus of a particular effort. It may well be there. I mean, you talked about V & V but not in the manner in which I would have thought about it. And you talked about their tools for whatever. And as I have listened to how we try to streamline the regulatory process so that these guys aren't jumping every -- you don't have to learn something new with every new design iteration. I noticed in a bunch of the standard guidance that you issued, you say hey if you do it this way, we are kind of happy with that. And if you do this, this, and this. And it is amazing how they like to do it that way because they know you will agree with it and it won't take as much time.

So when I looked at software methods or quality assurance methods, they are normally program-type methods. You know, you will have a program to do this. You will have a program to do this. You will validate data. But there is no details. There is not a methodology that yields, that you all have determined. You are letting people feed that to you. And I would have thought that we would try to develop what methods appear to provide the best software. I don't know on what basis you make that conclusion but that is what I would be looking for.

I know what we tried to do in our program 30 years ago, but that is not really relevant from a resource standpoint to the regulatory regime in which you all operate. So that was the first item. In other words, not programs but a specific QA software method. You know, whether you adapt somebody's or whatever, that is what I would have thought would have been a good thrust.

The second item was, if you look at the way the systems are being implemented with shared data going from -- you can argue whether I like that or not, okay, as the boss over here so capably tried to tell me that I wasn't allowed to say no. Although I disagree with that, we will work on that later.

The point being is you are faced with this and that is another vulnerability that you have to deal with. And Paul and I had probably a half an hour discussion which delayed my lunch, but that was beside the point. I wouldn't waste away.

In terms of shared data and error detection correction codes and stuff like that. And so it would really behoove you, I would think, to have some idea of the types of algorithms, of data evaluation algorithms or what have you if this stuff is being traded from channel to channel. But you would say okay, look, we have gone and we scoped this. We have researched it. We have run thousands of tests in this particular algorithm for assessing data coming from other. That says we are going to get non-corrupt data when we go from division to division.

And the same thing with error detection codes. Some would argue, and Paul stated, he says, oh no, once you do this error, it always comes out right. There ought to be something. You are now putting the protection for bad data at the processor, at the division level at the processors, once you start allowing data to go back and forth. Therefore, you have to have more robust means for evaluating that information if it is going to be there.

Those are the three areas I would have expected maybe a little bit more emphasis or elaboration. I don't know which section you put this under but it is probably the one up in the beginning under 3.1 or something like that.

So anyway, that was my input. I don't know whether that is --

MR. SANTOS: I think they are good comments. We will take them into consideration.

MEMBER BROWN: You never tell us we have bad comments, until later.

MR. SANTOS: Until later.

MEMBER BROWN: I'm just kidding. All right, I am done.

MR. SANTOS: We will probably have to take it and formulate it in appropriate activities and then get it through the process.

MEMBER BROWN: It is just an observation of what I consider you all's biggest vulnerability, at least from what I have seen to date. And that is why I tossed it on the table.

CHAIR APOSTOLAKIS: Jack?

MEMBER SIEBER: Well I think the staff has to respond to what hinders what applicants come in with. And I think this plan is pretty versatile from the standpoint of touching the bases, so to speak.

On the other hand, I don't see anything specific enough in there that would allow full knowledge sufficient for the review of any type of system that I know about now. And so this is going to be an ongoing project for some time. But overall, I find it pretty good.

CHAIR APOSTOLAKIS: Well, since we are going around, Dennis? Are you prepared to say something?

MEMBER BLEY: I agree with John. I think it is broad. It has got good coverage. The devil is in where it heads and what we begin to see. From my own little corner of the world what I really want to see is the collaboration exercise and where that is headed on the things we were talking about this morning.

I think the rest of it is pretty well formed and that is the place I am at.

CHAIR APOSTOLAKIS: John, do you agree with what you heard or you are just no comment?

MEMBER STETKAR: I have no comment.

CHAIR APOSTOLAKIS: No comment. Not from them. I mean from what you heard from Dennis and Jack.

MEMBER STETKAR: I understand that. I have no comment.

CHAIR APOSTOLAKIS: Okay.

MR. HECHT: There were, I think, several areas that required further, I guess, looking at. You have already spoken about the fact that you are going to be providing us with more detail on the work that UVA has been doing under that test he called benchmark reliability data.

Then with respect to operating experience analysis, you have, if you have the budget, you are certainly in a position to get data that could be much more useful than, I would say, the small data set that you have with the 322 failure reports that EPRI has. And that comes from a variety of sources. Like, I will be feeding comments to a chairman who may or may not pass them on to you in that regard.

With respect to the analytical assessments, I found that vague and I didn't quite understand what was coming forward. And maybe what some additional definition that will become clear, or it might be that it is unnecessary or may not address what is needed. I don't know.

And finally, the communications task, it was unclear. On the one hand, Charlie, I think, raised his concerns, which I would call fault containment or fault containment regions. It is called partitioning in the aviation world.

And then on the other we were talking about data flows which sounded to me like it was a known problem. But once again, I guess you will be getting comments, the validation of those concerns through the subcommittee chairman.

Thank you.

CHAIR APOSTOLAKIS: Okay. So we will recess until 3:00. Yes?

MR. BIRLA: Would you entertain comments from the staff?

CHAIR APOSTOLAKIS: On?

MR. BIRLA: On the day.

CHAIR APOSTOLAKIS: On what?

MR. BIRLA: I would like to convey a few words of appreciation.

CHAIR APOSTOLAKIS: Yes.

MR. BIRLA: Well first of all, yesterday you pointed out, cautioned us against looking at data on the outside, outside the nuclear industry. And you gave us an example of connections with software reliability papers were publish and the value is minus 2.5 percent. We appreciate that feedback. And we assure you we will not go there.

CHAIR APOSTOLAKIS: Don't take it literally.

MEMBER BROWN: You have got to be careful, George.

CHAIR APOSTOLAKIS: Why?

MEMBER BROWN: They are liable to remember what you said.

MR. BIRLA: And we heard from several other members that there was value in looking at data outside and we appreciate that, too. We would like to get some specific tips on where to go so that the effort is well spent.

When Charlie was vocal, life was interesting. Later on in the afternoon, he got silent. And when again he was talking, it got a little dull. So we would appreciate more, and more, and more engagement. We thank you all very much for the active involvement and criticism.

MEMBER BROWN: Are they saying I didn't talk enough?

CHAIR APOSTOLAKIS: Yes.

(Laughter.)

MEMBER BROWN: I have never, ever heard that comment before.

MR. BIRLA: And we look forward to more fueling of that sort from all of you.

So any detail that you didn't see today because the plan was flexible at the beginning and you would like to see more substance or more detail or have more specific discussions, I think it was a very healthy process to call us back on the specific areas of interest and give us more time.

CHAIR APOSTOLAKIS: We will probably have subcommittee meetings on specific matters.

MR. BIRLA: Okay.

CHAIR APOSTOLAKIS: Or areas. So, we will get much more detailed information so that Mr. Brown will speak up more.

Well, thank you very much. This is not done yet. We have to look at the PRA part.

(Whereupon, the foregoing meeting went off the record at 2:43 p.m. and resumed at 3:05 p.m.)

CHAIR APOSTOLAKIS: Back in session with PRA and I&C. Mr. Kuritzky.

MR. KURITZKY: Thank you. I am Alan Kuritzky with the Office of Research and we are here to talk to you today about Digital I&C PRA. With me is Louis Chu from Brookhaven National Laboratory. He is the principle investigator for the work that BNL is doing for the Division of Risk of Analysis in the Digital I&C PRA area. It is a very complicated area. It covers a lot of disciplines. There are a number of other individuals at Brookhaven that are supporting us in this work. Gerardo Martinez-Guirdi who has previously briefed this subcommittee has been heavily involved as Dr. Meng Yue, also an electrical engineer with a lot of experience in Digital I&C systems, has been involved as well as some other support staff at BNL.

We last briefed this subcommittee in April of 2008 and followed along with a full committee briefing in May of last year. And what I really wanted to do was come here today to just give you an overview of some of the activities that have gone on in the last 14 months or so. As you are well aware, we do not supply any documents for your review this time. So therefore, it is not going to be as in-depth as in the past.

CHAIR APOSTOLAKIS: What happened when you draft NUREG that we reviewed at that time, did you ever --

MR. KURITZKY: Yes.

CHAIR APOSTOLAKIS: -- finish it?

MR. KURITZKY: Yes, that document was published in October of last year. We also have a draft NUREG, a second in the series, which was sent out for public comment in November of last year and we are just getting ready to finalize that document. It is going through the final phase of getting ready to get published.

Again, because we haven't supplied any documents at this time, my intention here was just to give a brief overview of what we have done over the last 14 months if it has been quite a while since we have talked to the subcommittee, my intention and hope is to be able to come back to the subcommittee early next year for a much more detailed briefing, at which point we will have several documents to give you to look at and we can get into a much more detailed technical discussion.

CHAIR APOSTOLAKIS: January, February, is that what you mean?

MR. KURITZKY: I'm thinking February. Again, it depends on what the availability of the subcommittee is, the schedule which I haven't checked into as well as of course just the fluctuations in our project schedule. But right now, February looks like a pretty good time, if it works.

MEMBER BLEY: Are you going to tell us what has happened to that old Appendix C? Is that still living and moving somewhere?

MR. KURITZKY: You know, that isn't part of the presentation but I can tell you kind of what has happened to that. That appendix doesn't exist as a formal document anywhere. Some parts of it were, I'm kind of jumping the gun but some parts were, involved in a software PRA workshop that we held up at Brookhaven, recently. Some of it also is going to be involved in some of the work that we are doing right now that Brookhaven is doing for us in software. And the document as a whole has been given to the Division of Engineering and it is going to be considered as part of some of the projects that we are doing that you heard about earlier today in failure mode application etcetera.

So, it is kind of living on in various different arenas. But as a whole document, it is not actually in the process of being published.

Okay, so let me just go ahead and get into the brief overview that we have. I am just going to spend a few seconds --

CHAIR APOSTOLAKIS: Is Louis having a second set of slides?

MR. KURITZKY: No.

CHAIR APOSTOLAKIS: Oh!

MR. KURITZKY: No. No, Louis is here -- I will tell you why Louis is here.

CHAIR APOSTOLAKIS: For support.

MR. KURITZKY: I wanted one hour just to give you a heads up on what we have been doing in the last 14 months and to let you know we are going to come back in a more detailed presentation. But since you requested two hours, I immediately got on the phone and told Louis that he had to come down here. I don't want to handle that next hour by myself.

(Laughter.)

MR. KURITZKY: So that is why Louis is here.

CHAIR APOSTOLAKIS: You need less than two hours? Did we do that?

MS. ANTONESCU: Yes, we did.

MR. KURITZKY: So in any case, so Louis does not have a presentation.

CHAIR APOSTOLAKIS: Let's finish in an hour.

MR. KURITZKY: Yes, that works. That works for me. Sorry Louis.

(Laughter.)

MR. KURITZKY: Even in the one hour or half an hour, if you have any tough questions, he will still earn his pay.

Okay, so quickly, I am just going to go quickly over the background just to remind people the objective. The previous research I am going to go over. Mostly we will focus on what was in the most recent NUREG CR that we are currently finishing up.

I am going to just give you a brief overview of an international meeting we held, a technical meeting on Digital I&C of PRA last year, as well as go over our plans and recap the software PRA workshop we had in Brookhaven a few months ago, and then talk about the future interactions.

Okay, we all know that the current licensing process for digital systems is based on deterministic criteria. However, the commission in it 1995 period policy statement has encouraged the staff to use PRA in the regulatory arena, wherever, supported by the state-of-the-art. However, unfortunately right now we know that for digital systems, the capabilities in the PRA area are not up to snuff or a robust risk-informed applications.

I don't want to pass judgment on the work you heard about yesterday from yesterday. I don't view that as really Digital I&C PRA application because that was a black box which released a general PRA application. And that can be decided by others, as they see fit.

But inside that black box, with the digital system itself, there are a number of gaps that exist, which we have identified, we have to work and we are not really in the position to do much with it at the present time.

Okay, the objective of this work, the ultimate objective is actually to come up with tools and methods, and regulatory guidance for making risk-informed decisions related to digital systems and for getting digital system models into plant PRAs. That is the goal.

Some of the previous research that we have done over the last few years, the subcommittee has been briefed on this. We have identified a set of desirable characteristics for doing digital system PRA models. We have applied various methods to a benchmark system. An example, a system, digital feedwater control system, using both traditional and dynamic methods.

Just to remind the subcommittee, I know you don't particularly like the terminology traditional and dynamic but it is an artifact of our programmatic breakdown, so we keep it in dynamic for the purpose of this research is really those methods which explicitly account for the interactions between the digital system being modeled and the plant physical processes and the timing of those interactions.

So in other words, you are linked to essentially a plant dynamics model so that you can get real-time integration there. With the traditional methods, we don't. We have some boundary conditions that are input at the beginning of, you know, for the model and we just work on those set conditions.

This research has been documented in a number of reports over the last few years. The work Brookhaven has done for the division of risk analysis on the traditional methods was documented in NUREG/CR-6962 was the first report, which was the one that the subcommittee reviewed last spring. That one was published final in October of last year. We also are now working on the final publication of NUREG/CR-6997. That one discusses the application of the traditional methods to the digital feedwater control system. That report, like I said, should be published in a couple of months. And both of those reports, we feel reflect the comments that we received from the subcommittee back in April. Because if you recall, back in April, besides providing you with the draft of NUREG/CR-6962, we also had already completed a lot of the technical work for the second NUREG and we gave you preliminary insights on that. And so you gave us comments back there when we tried to account for those in the second NUREG.

CHAIR APOSTOLAKIS: Is the work that Brookhaven is doing incorporate, does that work incorporate any of the findings of Ohio State and ASCA and Virginia, or is it just something we did and we will forget about it?

MR. KURITZKY: Well, the work that I am talking about right here that was done over the past few years that is documented with NUREG/CRs, that is when we had the two separate groups.

CHAIR APOSTOLAKIS: I understand that.

MR. KURITZKY: So there was some interaction but not a lot. So that NUREG 6997 does not incorporate the general work that was done by OSU or its subcontractors.

CHAIR APOSTOLAKIS: Okay. But the work, I understand Brookhaven is continuing the work.

MR. KURITZKY: In the software reliability area?

CHAIR APOSTOLAKIS: Yes.

MR. KURITZKY: Okay in that work, yes. In that work, actually NUREG/CR, and again, I am kind of jumping the gun but we are going to discuss the work that BNL is currently doing on quantitative software reliability methods. And that builds on work that BNL did previously in that area some years ago. It is expanding it to look at other methods, more recent methods, and it also is looking at some of the methods that are identified in NUREG/CR-6901, it was the original NUREG/CR produced by Ohio State University and company and they identified a number of dynamic modeling methods, some of which those are broader methods for modeling a digital system, doing a reliability model. But again, we are focusing on quantifying the software reliability failure right now but some of those methods are in fact, or parts of those methods are ones you want to consider for quantifying software. So there is some of that being looked at.

MR. HECHT: Alan, isn't it true and perhaps, Dr. Chu, you could comment on this as well but in the model that you did on the digital feedwater control system, in that report, that you considered both the hardware and the software? I mean, I don't understand how one can consider software in isolation. Software, I mean, the most reliable software there is is a software which doesn't run and doesn't execute and has a success probability of one.

MR. KURITZKY: Right.

MR. HECHT: Once it starts executing, that is when you have failures and didn't the DFWCS also include channel failures in general and reconfigurations in general?

MR. KURITZKY: I can answer. The report that we did or the study that we did with the digital feedwater control system, we did consider software. We considered software in the sense of the successive software, how it normally operates. And that was heavily involved in the identification of the various hardware failure modes and understanding the operation of the system.

In fact, the simulation tool which we had to develop to identify the failure sequences, the component level failure pads, was based on a source code of the software for the system. As far as failure, software failures, we had only placeholder events, recognizing that of course, software can fail and it can lead to system failure. But because that was one of the areas identified as needing additional work.

Again, the study that we did was to establish where the state-of-the-art stood at the point we were looking at it, not necessarily to advance the state-of-the-art. So, we went there to fill the holes. We just wanted to see how far we could model the system with the current state of knowledge.

So one of the big holes that we identified was the fact that we could not quantify or even model software failure at that point. So, we had placeholder events in there.

Now, the additional work that is being done, including the software workshop PRA, the workshop that you attended, is to start having this head down the road of seeing how we can incorporate software failure into the models.

MR. HECHT: Well, those placeholder events, as you called them, based on my maybe inadequate understanding of the model, consisted of states, did they not? And so the real question whether to transition rates into and out of those states.

MR. KURITZKY: That directly goes to the

quantitative -- that is putting a probability value or failure rate on those events. But even so, those are two events that we stuck in there.

I jumped back for a minute to the discussion we had yesterday with EPRI and of course with the staff this morning about failure modes, failure mechanisms. Okay, in the PRA, we were worried about the failure modes. And again as we saw, you know, if you take a component level, the failure modes at the component level or the failure causes of the system level, the failure, you know, it works its way up.

So the failure modes that we have in there are again just some high level. I think we have one that it hangs or something or it doesn't provide the right output. But others might say that there could be other failure modes you need to consider. We think it is a fairly limited set at that level but nonetheless, we were not attempting to try and be exact or complete in modeling software in that DFWCS proof of constant study. We just had some placeholder events, recognizing that we are going to need to do more work in that area. And that if you were going to theoretically use that model for something, you would have to come back and do a better job at monitoring the software.

MR. HECHT: All right. I have to be very careful because I am sitting next to the person who taught me Markov modeling 35 years ago. But is it not true that if you were to consider other failure modes, it would just be a matter of adding additional states and that just, you know, if you had the proportion of failure modes and the overall failure rate, or you had a failure rate or a transition rate, let me call it that, into each one of those failure modes, you could do that?

MR. KURITZKY: I think that our belief, Brookhaven's and my belief right now, well I don't know if it is our belief, but we think that it is possibly or probably a way we can go about it. That is a discussion that is still open. I mean, there are a lot of people out there who some people feel that we can do it. It is essentially looking at it discreet from the hardware almost, you have these software events. Others may say no, you can't. You need some type of integrated approach with the hardware, software, or somehow combined together.

Some people just use a beta factor to account for software. You know, a beta factor on top of their hardware to account for software failure. So

I mean, there are different approaches and I don't think we were at the point where we can say definitively what the proper approach should be. That is why we are doing the research into the software reliability area.

But the way we are kind of by default going along, is just like you have said. Well, we would have failure modes in there. Maybe we have to add a couple of more. The biggest issue is quantify. You know, coming up with a value to stick on those events. But I just have to caution, even the concepts of just sticking those different events in there isn't universally accepted.

Does that answer the question?

MR. HECHT: It is certainly not universally accepted. And -- but -- It kind of does. Yes, thank you.

MR. KURITZKY: Okay. All right. So, --

CHAIR APOSTOLAKIS: Slide number six.

MR. KURITZKY: Okay. This just I wanted to quickly just go over a couple of the findings that are documented in NUREG/CR-6997.

CHAIR APOSTOLAKIS: Which is the Brookhaven report.

MR. KURITZKY: It is the Brookhaven report that is going to be published shortly. It is the second one. It is the one that we actually applied the traditional methods to the digital feedwater control system.

These findings are essentially the same as the ones that we presented back in April of 2008. So, I don't want to, I don't intend to spend a lot of time on them.

Again, if you recall, we modeled the system at a relatively low level of detail. Probably lower than most other models that are out there right now. We call it a major component of the module level. And that is down to like microprocessors, analogue digital converters, multiplexers, ram, bios. It is a fairly low-level component model for the digital feedwater control system.

We used that level of detail because that is where we had some publicly available data to stick in. Granted, not very good data and we had a big discussion about that last year, but also allowed us to model certain design features of the system, which we felt were important to understanding and correctly modeling how the system operated. And that is where again, there may be some different discussions. I think some of the other models out there, maybe some of the vendor models that are out there for the new reactors don't go to that level of detail. And that is two things.

I mean, the level of detail obviously in a PRA model is driven by a couple of things. Where you have data available -- I mean, you don't want to go down to lower levels if you don't have to because it just makes it a lot more complicated. So you go down to as far as you need to get data and to find out where you have system interactions. And so, you know, those are the two main ideas.

A third one, kind of a bonus, almost, is that as you will see from the fourth bullet, is that by going to that lower level of detail, you can sometimes identify things about the design or operation of the system that maybe other people in the design and implementation process haven't caught.

And particularly in our case, Louis and company identified a couple of scenarios, failure scenarios that were not picked up in the plant hazards analysis, the plant who the system is based on. One of them involved single delay times, where there is fault corrective, fault tolerant features in the system. They are supposed to pick up a certain failure, failure over to the backup CPU if there is some problem with the main CPU. And there is also a manual control station which you can fail over to, too, in certain situations.

In this one particular scenario that was picked up that the plant did not identify was you actually want to fail over to the back up CPU so you keep automatic control going but the signal times were such that the failure over to the manual control station occurred before the signal for failure over to the back up. So, you end up losing --

MEMBER BLEY: And then you are there.

MR. KURITZKY: I'm sorry?

MEMBER BLEY: I said and then you are there.

MR. KURITZKY: Right. And so that was one issue.

CHAIR APOSTOLAKIS: And this was picked up by the simulation.

MR. KURITZKY: Well, this was picked up, in reality, what BNL did, was they went through and manually did a very detailed FMEA of the system. Okay, and then when we went to try and model it and come up with their failure paths, and by we, of course, I mean BNL, but when they went to look at the failure paths and realized that certainly when it came to combinations of failures, you couldn't just do it mentally. You had to have some type of systematic method for finding out what impact on the system was of these various combinations of component failure modes.

And in fact, even some individual component failure modes it wasn't very easy to tell what the impact on the system was going to be. So that is when they developed the deterministic simulation model that was based on the source code.

Now, I think these two events, correct me if I am wrong, were picked up when you were doing the manual FMEA.

MR. CHU: I think the first one, the one associated with time delay was picked up during the manual FMEA. The other one was during the running of the simulation to basically, by doing the manual FMEA, we have certain expectation, you know, how failure mode would affect the system. But then when we run the simulation too, we get the outcome of the failure mode and we compare with the manual FMEA.

Sometimes there are disagreement and then we try to resolve the difference. So in doing that, we recognize the other situation that, you know, it appears that you know, the design, it becomes a question of the design. Maybe the design could be changed so that that kind of failure mode could be avoided or will not cause loss of control.

CHAIR APOSTOLAKIS: What do you do if manual FMEA in a computer code? What do you do? You start assuming faults?

MR. KURITZKY: Excuse me. We didn't do the manual FMEA on the computer code. The manual FMEA was done on the hardware system.

CHAIR APOSTOLAKIS: Oh.

MR. KURITZKY: The software --

MEMBER STETKAR: You assumed the software would respond --

MR. KURITZKY: Right.

MEMBER STETKAR: -- the way the software was designed to designed to respond --

MEMBER BLEY: When you did that part.

MR. KURITZKY: When we did the model, the simulation model.

MEMBER STETKAR: -- in response to that fault.

MR. KURITZKY: Right, exactly. It was the source code of the system that was used to come up with that simulation model, so we could process through actual hardware failures.

CHAIR APOSTOLAKIS: Did you bring the possibility of software faults anywhere in this evaluation?

MR. KURITZKY: Again, just going back to what Myron had mentioned before, when I was responding to Myron's question, we have a couple of placeholder events for software failure.

CHAIR APOSTOLAKIS: Okay but these two failure modes --

MR. KURITZKY: Hardware.

CHAIR APOSTOLAKIS: The search for these did not include software faults, did they?

MR. HECHT: No. This is purely on hardware.

CHAIR APOSTOLAKIS: This is only first.

MR. KURITZKY: Exactly.

MR. HECHT: But what happened was that that simulation was actually a form of V&V or was a verification of the code. It wasn't a stochastic.

CHAIR APOSTOLAKIS: It was partial unification.

MR. HECHT: Yes.

CHAIR APOSTOLAKIS: I'm sorry again. Okay.

MR. KURITZKY: Yes and Louis would love to have anybody who wants to have their codes V&V'd using a similar process, he would be happy to do it for them.

CHAIR APOSTOLAKIS: So you -- I'm sorry. Jack, you were looking at the control system over feedwater system.

MR. KURITZKY: Yes.

CHAIR APOSTOLAKIS: You found those two failure modes. Did you fix them?

MR. KURITZKY: Did we fix them? No.

CHAIR APOSTOLAKIS: So when you say later that you did something with the reliability, what, you assumed that these existed?

MR. KURITZKY: When we did something -- oh, yes in the calculation. Yes, when we calculate and again, only for proof of concept purposes, when we calculate the failure rate, potentially we are doing it, initiating to that frequency, but failure rate for the systems, those are essentially cut sets, yes. Those are point-level failure pads that are included in the quantification.

CHAIR APOSTOLAKIS: Well that is what I am a little fuzzy how that can be done. But --

MR. KURITZKY: Well there are different states in the Markov model. We stuck in values for each of them.

CHAIR APOSTOLAKIS: Let's put in the numbers.

MR. KURITZKY: Again, remember the values are being stuck in for proof of concept purposes only.

CHAIR APOSTOLAKIS: But the states in a Markov model assume that you have transitions occurring at constant rates and so on. And this is of a different nature, it seems to me.

MR. KURITZKY: Well it was still based on, these each involved like some hardware failure causes this condition to occur.

CHAIR APOSTOLAKIS: So the randomness counts for the random failure of that hardware component.

MR. KURITZKY: Exactly. Exactly. It is just the way the system responds to that hardware. I mean, better design --

CHAIR APOSTOLAKIS: Yes from a hardware point of view, I don't think we ever had any major objection to what you have done. It is when you bring in software faults in, the disagreements begin to grow.

MR. KURITZKY: Right.

CHAIR APOSTOLAKIS: But as far as hardware is -- yes, sure.

MR. KURITZKY: And to short-circuit that discussion, let's go right -- the areas of potential additional research, which are very similar to the ones we had in NUREG/CR-6962, we didn't learn a lot of new stuff in going to the second NUREG that we didn't identify in the first NUREG. Essentially the areas where we need work are coming up with a means for incorporating software failure into the models.

CHAIR APOSTOLAKIS: So all the work that we discussed yesterday with EPRI this morning would have stopped. Really it is irrelevant to what Brookhaven has already done. It will be useful in later tasks.

MR. KURITZKY: That is right. You kept trying to say multiple times, can I stick that number in the PRA. And there were no numbers that you saw yesterday that can be stuck in the PRA.

CHAIR APOSTOLAKIS: I understand that.

MR. KURITZKY: Right.

CHAIR APOSTOLAKIS: But they are not even giving insides to the Brookhaven group because these are software related and you are focusing on hardware.

MR. KURITZKY: That's right. Now, when I go to talk about the work that BNL is doing now and that we are planning to have them continue doing, then it is going to be a different story. Then that information is something that you can use.

CHAIR APOSTOLAKIS: Absolutely, yes.

MR. KURITZKY: Yes, right now, it is hardware models so it is different.

CHAIR APOSTOLAKIS: And you mentioned that in your introduction in your apps.

MR. KURITZKY: We have it mentioned in so many places, don't worry about it.

CHAIR APOSTOLAKIS: In bold-face letters?

MR. KURITZKY: And how much the data is of no value, we have that mentioned a thousand times.

CHAIR APOSTOLAKIS: Thank you, Alan. Thank you. You are a good person.

MEMBER BLEY: Alan?

MR. KURITZKY: Yes.

MEMBER BLEY: My memory needs a little help.

MR. KURITZKY: Yes.

MEMBER BLEY: Everything you have talked about so far sounds like what we saw last time around.

MR. KURITZKY: Exactly.

MEMBER BLEY: Is that true?

MR. KURITZKY: Yes.

MEMBER BLEY: Okay.

MR. KURITZKY: Yes, this is just a quick recap.

MEMBER BLEY: That is what I thought. I was afraid I am missing something here.

MR. KURITZKY: The point being that is has been 14 months since we have talked to you. And really we --

CHAIR APOSTOLAKIS: We are older men, we forget.

MR. KURITZKY: We are all older.

CHAIR APOSTOLAKIS: Thank you.

MR. KURITZKY: But really, we haven't advanced the technical work that much in these areas. You are documenting and preparing reports and whatnot. But essentially --

CHAIR APOSTOLAKIS: I don't remember. Did you have the failure modes the last time we met? I don't remember.

MEMBER BLEY: Yes and there is one that is simulation, tells you how to the fault here interacts if it hits at the wrong time.

CHAIR APOSTOLAKIS: Oh, yes. How tedious was it to do the FMEA?

MR. CHU: Okay, we started with reading.

We had three guys sitting in a conference room reading plant documents, including hazard analysis. This way, we educate ourself to learn how the system work. And look at the hazard analysis, see if we are agreed with what is said there.

And we probably spent six months doing that kind of work.

CHAIR APOSTOLAKIS: So it was six man-months?

MR. CHU: Yes.

CHAIR APOSTOLAKIS: Is that what you are saying?

MR. CHU: Yes, and doing that, the difficulty was the information is scattered here and there. There is some description in regular document that give you some information and then you need to get another piece of it from different documents.

Somehow, when you put together the two pieces of information you found they seem to be disagreeing. So there is that kind of a problem. And very often we run into the situation that we say where to read the software, see if the software will tell us exactly how the system would respond in this situation.

So you have situation where you actually took the source code and read it, try to figure out. Eventually we recognized we cannot do this manually or it is going to take forever. So we think of developing the automated system.

CHAIR APOSTOLAKIS: I would be curious to see one instance, once case of this, how it was done. But I also would like to be the one picking it. So, I don't know how to do that.

I mean, if you come prepared, you are going to give me a stylized thing. Anyway, I am very curious how this was done. The way it was described, what Louis just described. I mean, I don't know. I have to think about it.

MEMBER STETKAR: Louis, was that -- you started telling the story that you had. Was it actually six man-months to produce the FMEA or six man-months to understand the system or systems.

MR. CHU: Including understanding --

MEMBER STETKAR: Okay, but at the end of that six man-months, you had the FMEA as well as the --

MR. CHU: The actual developing of the simulation to and, you know, generating of all the sequences to what longer time --

MEMBER STETKAR: Oh, but in terms of the -

- oh. You said you did a manual --

MR. KURITZKY: First pass at the FMEA.

MEMBER STETKAR: -- first pass FMEA. And that was a six man-month level of effort.

MR. CHU: And then you know, we get to the point of formulating the approach for developing --

MEMBER STETKAR: The simulation tool from there.

MR. CHU: Right. Developing simulation tool itself, you know, kind of once the idea is formed, doing it took longer. We got a graduate student into the programming. Maybe it took another sox month of calendar time to do.

MEMBER STETKAR: Well, in perspective George, this is for a three-element feedwater control. Although it is a digital system, this is a pretty doggone simple device, in the grand scheme of the world of control systems.

CHAIR APOSTOLAKIS: Right.

MEMBER STETKAR: So just think in terms of --

CHAIR APOSTOLAKIS: I understand.

MEMBER STETKAR: -- level of EPRI, if you are talking about something really interesting.

CHAIR APOSTOLAKIS: I'm sorry. Jack?

MEMBER SIEBER: It is three parameters, complex control or one up or what?

MEMBER STETKAR: That's right. With some automatic transfers and things like that.

CHAIR APOSTOLAKIS: At the end of the six months, had you done any analysis that said this little thing is down and this is what happens or you were ready to start doing that? This is -- when did the graduate student come in to actually do the simulation? At the end of the three months.

MR. CHU: At the end of the two months, that is after we set him up in the conference room reading reports, trying to do the manual FMEA.

CHAIR APOSTOLAKIS: Yes. Manually you did what? That is what I don't know.

MR. CHU: Manual FMEA. Effectively, we had the hazard analysis, which caused component failure modes and described its effect on the system.

CHAIR APOSTOLAKIS: Including the software? Including the output? What happens to the output? Because you said then that you start some simulation. I am trying to understand what you did before that and what you did after.

MR. KURITZKY: Louis, let me, if I can. In the NUREG/CR-6962 that gave you draft of last time, there was an appendix in there where it had the FMEA table for the main CPU. In the new report, we have the FMEA tables for all the controllers and modules that were evaluated. But even for the last report, you had it for the main CPU and you see all the different component failures that were considered. You are really looking at signals, various component signals coming and signals going out. And the third mode really involved whether the signal comes out correctly, etcetera.

And if you look in there it has the calm of the effect and you can see exactly, you have got a good idea of what they were considering when they were looking at the various failures.

Now what that doesn't show you is that after having done that, actually the new report will show you a column that says did they have to stimulate this one. Many of them they could tell just by looking at it as Louis was saying by looking at various plant documents, whether or not a particular component failure led to a system failure.

For some it was too hard to tell so they went and ran it through the simulation model. All of the combinations, they also put through the simulation model because the FMEA table is giving you a single failure and always looking at one of them.

CHAIR APOSTOLAKIS: So these two failure modes were identified after those two months?

MR. CHU: The first one --

CHAIR APOSTOLAKIS: And you said you -- I'm sorry I forgot that. Okay.

MR. CHU: And the fact that we used the simulation tool, the fact that we are running the actual control software. So there are detail features n the software that is automatically captured. Like the ability to detect all the range kind of visions, deviations, and act accordingly.

CHAIR APOSTOLAKIS: But I, at some point in the future, I think it will be very useful for the subcommittee -- I am going a little away now from this -- to understand what features say of the Ohio State simulation your approach does not have and they do. And maybe what you have and they don't.

I really would not want this to proceed and say we did this and the rest of the world can go do whatever they want. I mean, they are paying a price in the sense that they are spending, I think, much more time simulating the system. That is my understanding. Usually, along with that, you have some extra benefits that other methods that are perhaps simpler don't have.

So, I would like to understand that. The same thing with DFM that Sergio has developed. What is it that he is doing and what information is he getting out of it that perhaps you are not getting out and vice-versa? Okay? That will be, I think, a very useful thing before we settle on a method. Because if we do that, then perhaps we can do also what Alan said earlier that maybe we can borrow from here, put it in our method or whatever and come up with a hybrid that will have all the good aspects and features of everything.

MR. CHU: Let me suggest something. In the latest NUREG/CR-6997, we have a chapter in which we try to compare our model with the dynamic model. We recognize, you know, the studies have very different assumptions. We analyze different situations but that dynamic model consider a power transition going from certain level to another level and consider time period of 24 hours.

Well, our folks had to calculate something like initiating event frequency, loss of feedwater due to failure of the feedwater control system. So there are many different assumptions made in the two different studies.

And another difficulty in comparing the two studies is that, you know, the detail of amount of documentation and the amount of time we spend on trying to compare it is another factor. Therefore, I will say to go to a good comparison, we need to have kind of the two team of people, each spending some time looking at other people's model. And they will sit down in a conference and argue, debate, and I would say how did you model this, how did you model that. And we may end up saying well, you didn't do this right and they may tell us we didn't do certain things right.

So, going through this process we can know better and make better comparison.

CHAIR APOSTOLAKIS: Why don't you?

MR. KURITZKY: Someone has to pay for it.

CHAIR APOSTOLAKIS: You.

MR. KURITZKY: I left my wallet in my other --

CHAIR APOSTOLAKIS: I think it would be a big mistake saying this is our method. We recognize our other methods but tough. No. I mean, we are trying to build the best model we can. Maybe you can play that role. Put some extra effort on the stand where the other guy is doing. They did a feedwater system, didn't they?

MR. KURITZKY: Yes.

CHAIR APOSTOLAKIS: Look at the assumptions. I mean, you can figure it out. And then compare. You don't have to bring them in.

MR. KURITZKY: Let me, if I can, as Louis mentioned, in the new NUREG 6997, there is a chapter where we try and compare between the two models. And as Louis mentioned, there is some substantial differences in the boundary conditions for those two cases. So there is a limit to what they can compare.

However, when we come back to brief you in more detail on this report, you will see that there were some failure modes that we had difficulty modeling with our approach. And we suspect, though don't know, that it might be easier or we may be more capable of modeling these particular failure modes, if we had a dynamic model of the system, as was used in the OSU, etcetera work. So, there may be some benefit to that.

One of the questions that we have, if you look at the very last bullet on this page, determining if and when a dynamic model of the plant is necessary for including the digital system PRA model. That is an open issue. But you talk about, Professor

Apostolakis, is whether or not there are pieces from that one that we can use, whether we should consider together what one has and one doesn't have.

We looked at a control system, a feedwater control system. The reason we looked at a feedwater control system, in fact going back to how we briefed you a year ago, we were going to look at -- both approaches we are going to look at two different benchmark systems, a feedwater control system and a protection system.

However, and we started looking at the protection system. This is the one of most interest. But because we were unable to procure the actual system, the protection system, we were forced to switch and do the feedwater control system first.

As it turned out, after many years and millions of dollars of doing the benchmark systems, we decide okay, maybe right now we know enough, we have identified enough holes that need to be filled that maybe we should be looking at, and we have got feedback from the committee on some of these holes, then maybe we should start looking at some of these known gaps right now and not jump in with all the money and time to do a second benchmark. We can learn additional things from that second benchmark but maybe the debt isn't sufficient for the cost right now when we have other things we can use that money for.

So therefore, we have focused on a control system. With a control system, the dynamic model might become more important, having a plant model. However, when we go to protection systems, which are really the biggest concern for plant PRAs because in reality, in a plant PRA, we are not going to model the digital feedwater control system with a fault tree. You are going to have an issue of that frequency data in there that is going to stick in. So we don't need this model. It is really just an exercise and prove the concept of being able to model a digital system.

For a protection system, which is an on-demand system, maybe the need for a dynamic model plant is not that great. We don't know for a fact. We haven't done it yet. But as you will see, the discussions in our international trip back in October, as well as some of the other stuff that we have come up with from our work says you know, we are not so sure that that is necessary and it is a big expense. You say that you get certain value for that expense. Yes, you do, we are not sure yet now whether that value is worth it. And it may be worth it in some cases and not in other cases. So that is something we need to look at.

CHAIR APOSTOLAKIS: This is the idea behind the request for you to develop categories of software and applications, you know, to come up with methods that are appropriate for each class. And Yes, I agree that for actuation systems, you may not need something very sophisticated. So there is nothing new there. I am not saying do it for everything.

But coming back to Louis' comment, when you say different assumptions, what exactly do you mean? Different assumptions as to how the system works or different assumptions in order to develop a model.

MR. CHU: I guess maybe the way Alan described it is more accurate. Different boundary conditions. As I described it, we looked at it, we tried to develop model to estimate how the control system will fail causing a loss of feedwater control and then we can calculate the frequency of this event. A factor is the frequency of initiating event or the loss of feedwater.

But the dynamic model considered a change in power level in going from, I don't remember numbers, say from 50 percent to 80 percent and stay there for eight hours and come back to 50 percent. So the scenario that they model is like that. And then there are a level of detail of modeling, I am sure. Our model in terms of how the figure is more detailed than the dynamic model.

CHAIR APOSTOLAKIS: Well and then the question is, is there a need to worry about such a scenario? Sure there was a reason why they did it. And if there is a need, could you do it with your method? You know, these are the kinds of, as you say, different assumptions. But you can evaluate those assumptions and say why did they make this assumption and does it make sense to make this assumption?

MR. HECHT: It sounds like they were different, they were models for different purposes.

MR. KURITZKY: That is how it turned out. I mean, I think if it was coordinated better in the beginning, we wouldn't have that situation.

MR. HECHT: They were answering different questions.

CHAIR APOSTOLAKIS: All right.

MEMBER STETKAR: The bad state in either model was no feedwater. I mean, what was -- I understand the bad state in your model. It is no feedwater.

MR. KURITZKY: Right.

MEMBER STETKAR: What was the bad state in their model?

MR. KURITZKY: I think the bad state in their model was like Louis mentioned, they were transitioning from power to I think 70 percent.

MEMBER STETKAR: I understand the boundary conditions. What was the --

MR. KURITZKY: Well, I will assume loss of feedwater.

MEMBER STETKAR: Loss of feedwater?

MR. CHU: And so they have two bad states. One is high level in the generator and one is low water.

MEMBER STETKAR: Okay, so theirs was improper control.

MR. CHU: Right. So currently, we are able to demonstrate the benefit of their modeling of the control process. They can actually physically calculate the level, dropping to low level or high level point. So that is the apparent, you know, benefit of being that kind of model.

MEMBER STETKAR: You mentioned we haven't seen the NUREG. But you are saying that the comparison that you did make, there seemed to be some benefits of their process compared to yours and perhaps some benefit of your model compared to theirs.

Since they looked at a ramp up, apparently a ramp up, and a reasonable steady state, and a ramp down. Is the benefit of their model on the ramp processes?

MR. KURITZKY: Well, again --

MEMBER STETKAR: Or did their model actually show some benefits in that steady state?

MR. KURITZKY: Well, I think where we have identified a potential benefit is really there was certain failure modes and again, this is a little more detailed than I was planning to talk about but there were certain fire modes that we had a trouble modeling, a signal drift. Okay? We assumed in our model that if a signal drifted, that it ultimately would drift out of range high or out of range low.

Okay, and it was easier to model once you had out of range out of range low, you could monitor it fairly easily. And the reality of it is that you typically pick up that. If you had out of range indication, it would pick that up.

But really the worse situation would be it drifts but it stays in that range. So it is out of range enough to cause you a problem but not enough that you pick it up. But that was a condition that we couldn't really model very well.

MEMBER STETKAR: So you get a --

MR. KURITZKY: Right. So in fact we modeled it, we really modeled it non-conservatively because we assumed it would go out of range and that is really not conservative. How much non-conservative, I don't know. But so we felt that if you had an actual model of the plant, you would be tracking it and you would see if it gets to the point where it actually causes a problem or not.

Okay, but there are also other factors that that other model might not have even been able to give us the right to fully correct the answer either.

But I think the point is, it is not a competition between the two methods and it is not like a race to be first in space, etcetera. We have two different projects that we did and we learned many things from doing both projects. And it is not that we are discarding one and only moving forward with another. We have done the two essentially hardware projects, dynamic and traditional. We recognize that there are other aspects and digital system monitoring that need to be addressed and we are putting more of an emphasis right now on some of those other aspects, software reliability, failure mode identification.

Once we get a better handle on those and assuming we move enough that we feel we can forward, then we start to look back at the total models again and then we may decide okay now that we are going to try and put a whole model together, do we want to use something that is more of a static model? Do we need to have a plant dynamic model? It is going to be case-by-case because some systems may need it, some software platforms may need it. And again, that last fold is really just a little bullet stuck at the bottom of the slide but it is a pretty power packed, potentially resource-packed bullet. I mean, that is a question that we need to answer.

So I think a lot of your questions and recommendations right now really apply to the point when we get back to that bullet and look at integrating the system.

MEMBER SIEBER: If you assume that the controller does not fail and it is in proportionately being reset with a bias on it and your level is the bias, the only parameter that makes it a permanent offset is an error from the bias signal. Right? Which is the level signal.

MR. KURITZKY: Talk to Louis about that.

MEMBER SIEBER: Whereas, if I have an

error in steam flow or feed flow, sooner or later, somewhere out there, the bias will correct it. Now the question is, does it hunt in between? Does it trip? Does it starve the steam generator? Do you overfill? And it is a dynamic setting where the controller is set which tells you which way it is going to go an how far an how fast. Right? And do you model all of that?

MEMBER STETKAR: They didn't. I'm sure they didn't.

MEMBER SIEBER: Okay well that tells you whether it fails or not.

MR. KURITZKY: And again, that goes to what we were saying. We just assumed that it would eventually, if it was going off normal, it was going to eventually fail high or low. In the dynamic model, they can do it --

MEMBER SIEBER: The output, which is the out portion.

MR. KURITZKY: Yes, right.

MEMBER STETKAR: In other words, they would have taken the level bias and just failed at high or low, rather than just a gradual offset.

MEMBER SIEBER: Well, regardless of analogue or digital, it doesn't happen that way.

MR. KURITZKY: Right but in a PRA, there are a lot of things that don't happen the way you have them in the PRA.

MEMBER SIEBER: I just have to move to another land --

MR. KURITZKY: Exactly.

MEMBER SIEBER: -- where things happen --

MR. KURITZKY: Never Neverland.

MR. HECHT: But the point is there a state in which things are acceptable and then there is a state in which things are not acceptable and that is the failure state. That is basically the abstraction or the simplification of that.

MEMBER SIEBER: I look at it from the operator's viewpoint. Unless he has an instrument that tracks each of the three parameters, he may not know. He may not see the transient, except he may get an alarm somewhere in there.

MR. KURITZKY: In fact, if you look at the failure modes and effects tables --

MR. HECHT: Well, no, that is not moving.

MEMBER SIEBER: If you review your board like you are supposed to, you will pick it up.

MR. KURITZKY: Again, if you look at the failure modes and effects tables, which we have in the new report, and I am not sure if they are the same detail level in NUREG 6962 but we talk about what signals, when the failures occur, besides whether or not it was also a loss of the automatic control. Also whether or not there is some indication to the operators that something has gone out.

MEMBER SIEBER: Yes, a smart controller would probably flip the main somewhere in the process. That would give them the warning.

MR. KURITZKY: Environmental failure. Yes.

CHAIR APOSTOLAKIS: It seems to me that Mr. Sieber just gave you what happens in real life.

MR. KURITZKY: Right.

CHAIR APOSTOLAKIS: And somehow, you have to model that. You can't just say --

MEMBER SIEBER: This doesn't model real life, as I see it.

MR. KURITZKY: Well again, it is a level -- I only use it -- This is the first time I heard the term level of abstraction. But they said level of abstraction in the sense that, you know, we are modeling it at a certain level. You are not going to go into a PRA model and model the individual exact perturbations of the entire plant in all situations.

Okay? It is an approximation of what is going on at the plant.

CHAIR APOSTOLAKIS: But you have to convince people like Mr. Sieber that your approximation approximates what he says is going to happen.

MR. KURITZKY: Yes. Exactly correct.

MEMBER SIEBER: Right now, I would say whatever you want to do but this is sort of B.S.

CHAIR APOSTOLAKIS: Well that is --

MEMBER SIEBER: I think you can reach conclusions from what you are doing about reliability and risk. But it really doesn't model the plant the way the plant runs.

CHAIR APOSTOLAKIS: Well that is a decision made --

MEMBER SIEBER: You may get harsher results. You may get harsher results than you would out of actual operation at the plant from the model.

MR. KURITZKY: And again, I would stress that from a PRA point of view, in a PRA, we are not going to model a control system like this, with a detailed fault tree. We are going to use operational data, which for purposes of the PRA is sufficient. So we don't need to know the exact operation. If we are going to model a protection system and the same issue or something similar exists, then we have to worry about it.

MEMBER SIEBER: Well, but you are setting the framework now for how you are going to model a lot of things in the future. And I think you are going to have to grade modeling to meet the importance of the system, in order to come up with a real risk number, I think.

MR. KURITZKY: And that would be the benefit if doing that second bench. Doing a benchmark for protection system would allow us to see whether those same types of issues are going to be --

MEMBER SIEBER: I would be interested in thinking that one through.

CHAIR APOSTOLAKIS: Well, we do need the subcommittee meeting I think to understand that a little better. Because I am really disturbed when I hear we are not modeling the actual situation. I get very uncomfortable when I hear that.

Now you may be on your way. I can grant you that. But so far you haven't done it.

MEMBER STETKAR: George, in deference, you know, to people who really do risk assessment, there are very few things in risk assessment that model plant response in the way that you and Jack are perceiving the level of detail at which things should be modeled. There is essentially nothing. It is all a discrete abstraction of a dynamic process. It is all.

CHAIR APOSTOLAKIS: But it is incumbent upon you to convince people who understand the plan that what you are doing approximates --

MEMBER STETKAR: A risk assessment is not a dynamic simulator.

CHAIR APOSTOLAKIS: I know that.

MEMBER STETKAR: And it never has been.

CHAIR APOSTOLAKIS: But it approximates behavior. I mean the time --

MEMBER STETKAR: It approximates discrete behavior. Two states, success or failed --

CHAIR APOSTOLAKIS: Right.

MEMBER STETKAR: -- with some likelihood that you are in either of those states.

MEMBER SIEBER: The problem though is there is a third state and that state is impaired, not failed.

MEMBER STETKAR: For a risk assessment, impaired doesn't make any difference.

MEMBER SIEBER: I understand that but the risk numbers end up when you count them that way, risk numbers add up greater than they actually are in reality because of the way it fails.

MEMBER STETKAR: That has been a problem in the past when people have tried to develop, in some cases, very, very --

MEMBER SIEBER: It is hard to do.

MEMBER STETKAR: -- simplifications of very, very sophisticated models. I mean, this was done 30 years ago when people first started to try to evaluate reactor protection systems and determine that, you know, plants would fail to trip one in five times that they were challenged, which was a simplification of a very, very difficult process that was obviously wrong. But it was a very, very complex model.

MR. KURITZKY: And just, if you look at the insights that are in NUREG/CR-6997, I specifically didn't include it here because I don't want to get to this level of discussion. That was the exact issue that I avoided. But it is probably the longest written up insight in the report because it is an area that we recognize we are not doing a very good job on.

And again, I go down this last bullet that says well, do we need to or not, for protection system. And that we have to go through and see. But the point is extremely valid. We do talk about that in the insight section of the report.

MEMBER SIEBER: Yes, the only thing that bothers me is I don't hear anybody say that we are going to improve it. I mean, that is the state-of-the-art and there you are. And so you get a number and march off.

MR. KURITZKY: Well we actually talk about some ways at a very high level, saying here are some possible ways to go about approving it. The dynamic modeling was one that we speculate might be able to shed more light on it. But again, we also speculated on some of the limitations there, too. So, it is very complex.

CHAIR APOSTOLAKIS: It seems to me that John is right but that is not a license to do whatever you like.

MR. KURITZKY: No.

CHAIR APOSTOLAKIS: Okay. So there are many situations in PRA that a dynamic model would be perhaps more accurate. And we approximate with discrete states. But somebody takes the trouble to show that the discrete approximation is meaningful, it may not be exactly accurate but for certain purposes it is good enough.

For example, you lose off-site power, there is the competition you know, of restoring it. If you go to an event tree, it says was it restore three hours, in six hours, and assign certain probabilities that came from someplace and that is good enough for our purposes. You know, if it is the same situation here, more power to you. But just to say, now what we did was right because of discrete approximation, I mean, I think you have to convince people like Jack that it is an approximation. Then it is okay.

MR. KURITZKY: But we agree with you. We are not saying that it is right. In fact, our report says that that scenario is not done right and that it needs to be looked at in more detail.

CHAIR APOSTOLAKIS: Okay.

MEMBER SIEBER: I got to the first part, which is I agree it is an approximation. I didn't get to the second part yet which is, and it is right.

MR. KURITZKY: Yes.

MEMBER SIEBER: Okay, I didn't get there.

MEMBER STETKAR: One of the things that I caution and you have perhaps thought about it, or maybe not, is that you are, this feedwater system model you have developed, regardless of which of the two approaches you take, is modeling a dynamic control system. It is a constantly operating dynamic control system. And obviously those have some very, very distinct challenges to model. You know, can you actually simulate it or model it or develop reliability parameters or whatever.

You flipped and you said well, in a protection system, those complications don't exit.

MR. KURITZKY: May. We don't know.

MEMBER STETKAR: Okay, may. But when people think of protection systems, people immediately think of trip the reactor, given something out of bounds. I would throw in the fact that perhaps some digital integrated protection ESFAS actuation systems which are now not so clearly distinct between trip the reactor and get things stated, are indeed a hybrid of a dynamic control system and a digital on and off, pass/fail-type protection system because there are certain systems out there operating right now that do have a dynamic behavior.

If level is decreasing at a certain rate and temperature is doing this, then perhaps inhibit a certain depressurization function, for example. That is more of the nature of a dynamic control system. But it is in a safety related, safeguards application type function. So, a lot of the stuff that you are doing just because it is feedwater and it is non-1E and yadda, yadda, yadda, may in fact be very, very relevant.

Well, don't toss it out and just say well okay, we have determined that all of this dynamic stuff may not be relevant for the protection thing.

MR. KURITZKY: Right.

MEMBER SIEBER: Well, if you get into some little more complex system like PWR and flow versus power, you know, that is a FERV, that is a dynamic situation. You have to evaluate it in a more complex way than an on and off switch, as far as protection.

I think the combustion core power calculator is similar to that. Naval reactors had it made. You know, if it reaches a set point, it trips. And there is no dynamics or no calculator functions or anything other than set backs. Right? You can't tell me that.

MEMBER BROWN: I can only tell you you are wrong. I can tell you that the reactors of 50 years ago.

MEMBER BLEY: At one time. You have to

say at one time.

MEMBER SIEBER: Reactors of 50 years ago were that way.

MEMBER BROWN: But I will give you -- you are talking about a point protection system, which is what these plants have from a reactor protection. Even your commercial plants are all point protection systems.

MEMBER SIEBER: Yes, okay.

MEMBER BROWN: The power goes up, the pressure goes down, the temperature hits a point, you drop, you do something.

MEMBER SIEBER: That's right.

MEMBER BROWN: It is a point protection system. An integrated protection system models the protection analysis in the actual performance of the algorithms that you do it. So you decide what you want to do. They are very complex. You don't need to do that in these plants. There is no reason to go to that -- there may be some circumstances.

MEMBER STETKAR: There maybe some smarter type safeguard systems out there.

MEMBER BROWN: I agree there are a couple of that I have learned based on listening to what it going on. But in general, these are static plants.

Base load, you have got a certain place you want to be and therefore, your set points are fixed.

MEMBER SIEBER: And you can treat these in a relatively simple fashion, but the dynamic systems, I think you have to go a little further. I think.

MEMBER BLEY: I think what has got to happen here is that they have got to do what they are doing. They have got to go in more detail. And when you first start doing this, you have to look, as Jack says, a lot further. After you have done that a few times, you might be able to generate simplified models that you can use elsewhere. That is where it is going to end up. But right now, you have to go into more detail to understand how it is all working and generate the simplifications.

CHAIR APOSTOLAKIS: This discussion does not have the benefit of really knowing what you actually did. So, I think it is time to move on.

MR. KURITZKY: Okay.

CHAIR APOSTOLAKIS: I think you got the message.

MR. KURITZKY: Okay.

CHAIR APOSTOLAKIS: And maybe at the next subcommittee meeting when we have more details, you have an idea now what kind of questions you are going to get.

MEMBER BROWN: I would make -- can I make one observation?

CHAIR APOSTOLAKIS: Sure.

MEMBER BROWN: Okay, because I am not -- how you model analogue vice digital type systems is the only point that -- and this is just an experience thing and it is general. So don't take it as all truth. But in general, when we started putting digital systems in service, you knew when they broke they had discrete responses. If something didn't respond, it popped up here. It popped up there. It quit. Analogue systems, sometimes you weren't sure whether it was working or not. It seemed to be going with the flow and you couldn't -- they just, unless you had something that really failed low, you know, like a detector signal or something like that or a busted amplifier that zoomed up, --

MEMBER SIEBER: Or a broken wire.

MEMBER BROWN: -- or a broken wire, that is right. Other than that, you drift around, you would think well everything is happy. But it really wasn't. It wasn't responding right. It's response wasn't right, what have you. It was ambiguous.

And whereas the digital systems, man, you are looking at it all of the sudden the meter, instead of reading 200 is reading 700. It is not 210, 700. A control function, if it broke, bang. It slammed it up. It slammed it down. Just because dip flips or other software failures created large dislocations in terms of the information being processed.

Now, is that an absolute? No. But in general that is kind of what we saw. It is kind of an interesting thing.

I had to tell my bosses, generally, you will know when the digital systems are broken. It will be totally obvious. It is not so obvious with the analogue ones. So don't -- you have got to be careful how you model. That is the only point of the long dissertation. That was somewhat incoherent.

MR. KURITZKY: No, I understand.

MEMBER SIEBER: Now let's move on.

MEMBER BROWN: Pardon?

MEMBER SIEBER: Now let's move on, --

MEMBER BROWN: Yes, thank you.

MEMBER SIEBER: -- as George suggested.

MR. KURITZKY: Okay. So that is all we wanted to say about that NUREG right now. Like you said, we will come back another time and go into it in more detail and address those issues.

Okay, back in 2007, here is an acronym, the Organization of Economic Co-operation and Development Nuclear Energy Agency/Committee For Safety of Nuclear Installations/Working Group on Risk Assessment was encouraged to undertake an activity looking at digital I&C PRA. Since that was right in line with the work we were doing, the NRC volunteered to take the lead on that effort. So, with the help of BNL, we took the lead on that. The objectives of that activity were to identify and recommend current methods and data for including digital systems in PRA and to identify any short or long-term research advancements that were necessary.

The meeting, we actually held a planning meeting in October of 2007 here across the street at the Marriott. We had about five international colleagues participating in that planning meeting. The focal point of the activity was decided to be a technical meeting open to the entire WGRisk membership, where everybody would discuss their various experiences and models that they have been working on or methods that they have been pursuing.

And that meeting was originally scheduled to take place on Long Island in May of 2008. However for various reasons, our international colleagues, whether they balked at going to Long Island or whether they didn't like the date, I don't know but we ended up having to postpone the meeting and it was held, instead last October in Paris. The meeting was well attended.

(Laughter.)

MR. KURITZKY: In any case, the meeting was well attended. We had participated in --

CHAIR APOSTOLAKIS: You can say that again.

MR. KURITZKY: As Louis always mentions, there is great fishing on Long Island Sound and you have all of the fancy --

CHAIR APOSTOLAKIS: Wait a minute. The meeting was in Paris, you said.

MR. KURITZKY: Right in defense of Long Island.

CHAIR APOSTOLAKIS: Oh, the fishing is good?

MR. KURITZKY: In any case, back to Paris. In Paris.

CHAIR APOSTOLAKIS: Did anyone say, why didn't we go to Paris?

MR. KURITZKY: So, back to Paris in 2008, we had participants coming from over 20 organizations from 11 different countries. It was actually a fairly productive meeting. There was a summer report on that meeting that Brookhaven put together. It just recently got the approval from CSNI to publish it. There was just a few comments that they want the WGRisk Secretary to clean up and so we hope to have that report out publicly before the end of the year.

And at that meeting, there was a wide spectrum of modeling methods and ideas put forth. Very few people agreed on any particular aspect. We were pretty much all over the map as far as what people have done, what people think should be done, what they are planning to do. It was very useful to be able to share those experiences and learn about the other things that people are doing. We did actually find a couple of countries that were doing things more in line with what we are doing.

But in general, the consensus or the agreement among the participants was pretty much just focused on things, their high level topics, like the need to include software into PRA, the fact that data is pretty weak and that we need better hardware data, and that we should need to continue to address many of the issues that we identify really in the NRC work that we have done previously.

MEMBER STETKAR: Alan, we can read the report when it comes out. Just quick curiosity. Were there feedback from people who would actually tackle the real modeling problems of real systems?

MR. KURITZKY: Yes, but on the other hand, almost no one had to address software.

MEMBER STETKAR: Okay, but they had at least --

MR. KURITZKY: The Koreans have put models together. The Japanese have some very rudimentary models that are fairly old. The French have a method for addressing, which is a fairly simplified method.

MEMBER STETKAR: Not a method, a real analysis.

MR. KURITZKY: Okay, sorry. Others are considering that but these are actually models. The French have a model. The Japanese have a model. The Greens have a model. I don't Louis, there may have been others. Those are the main ones that I remember that actually have models.

MEMBER STETKAR: Thanks.

MR. KURITZKY: So in any case, I would say that the meeting was relatively successful in the fact that we got to exchange this information. Did we come out with concrete actionable recommendations that will help close all the gaps? No, not really.

The report does include some recommendations. They are broken down into three basic areas, method development, data collection and analysis and international cooperation. Again, they are very similar to the types of things we identified in the NRC research work that we had done around the same time.

One item that they did recommend was developing a taxonomy of digital component failure modes. This is also something that EPRI had talked about a little bit in their meeting today but more in the public meeting they had August 5th where they mentioned that was one of the things I think that they are considering for doing in their next fiscal year or whatever, something along those lines.

The other ones are the same standard holes that we know about. You know, methods for including software, quantifying software failure probability, getting data, dealing with fault tolerant features. You know, modeling them and quantifying them.

Again, the need and approaches for addressing dynamic interactions is the same issue. Do we need these dynamic models to come up with an adequate model of the system?

Data collection, the same things. You know, we need both independent and common cause hardware failure. We need better data. Looking at the operating experience to try and find out how software can fail. It is the same thing.

MEMBER STETKAR: Let me ask you because you have a little bit different perspective or experience. This morning, I got a relatively discouraging perspective on the prospects of being able to glean real operating experience from international partners. What is your take?

MR. KURITZKY: Well, and you will appreciate my take. I divided it into two categories. There is looking at the operational experience, to learn from the events. In that regard, I personally think data from non-1E systems, other industries, I don't care where it comes from, you looked at it and you see whether it teaches you something and whether it is something that you may want to consider.

You were mentioning before, you have to go through the data, one of you mentioned it.

MEMBER STETKAR: It was --

MR. KURITZKY: Dennis is being too quiet.

MEMBER STETKAR: It was the real Dennis of the two Dennises.

MR. KURITZKY: And you have to determine whether this stuff applies or not because in different cases, it may apply and it may not. Even whenever someone mentioned 50 rule data, may apply. Dr. Apostolakis said data from the Middle Ages may apply. You have to see. So I think --

CHAIR APOSTOLAKIS: No, no, I didn't say Middle Ages.

MR. KURITZKY: Medieval? I thought --

CHAIR APOSTOLAKIS: No, that was classic Apostolakis. 500 B.C.

MR. KURITZKY: In any case. But that is learning about the learning about the experience and getting insights from it. When it comes to plugging numbers in the PRA, you need the denominator. That was discussed earlier, too.

CHAIR APOSTOLAKIS: No, no. I think this discussion is too high level, guys. I mean, can we go on? Make your point.

MEMBER STETKAR: I am just trying to get a feel for, he said he had a meeting with very, very good participation and people from more than 20 countries and some people who were really doing things and everyone agrees that we need to take better advantage of operating experience.

CHAIR APOSTOLAKIS: Sure.

MEMBER STETKAR: This morning when I asked what is Research's experience on being able to actually -- if everyone agrees that we need it and it is really important, what is the prognosis for actually getting said operating experience in real time. Do you have the same sense?

MR. KURITZKY: I will probably yield to Louis to give you more detail.

I mean, my feeling was to have some plants or some organizations actually have models. And they --

MEMBER STETKAR: Not models. Real operating experience.

MR. KURITZKY: No, I am saying they have quantified those models. So they have data they have used to quantify those models. Now that data, a) very likely proprietary; but b) is it stuff that is applicable? Again, depending on what level you are putting the data in, determines whether the data from this system can be used for this other model.

So you know, I didn't get the feeling that there was a lot of readily usable data just sitting out there for us to sign a bilateral agreement and get a hold of.

MR. CHU: Yes, but my impression is the same as yours, you know, Alan talk about, there are occurrences that can be shared among different countries but when it comes to estimating parameters, you need a denominator or this is not clear.

MEMBER STETKAR: I am not really talking about the denominator. I am just talking about if I am operating a nuclear power plant in country East Slabovia and --

MR. KURITZKY: I don't think they are doing that.

MEMBER STETKAR: Not yet. And I have a large number of digital control systems in my plant and I have been operating said plant for ten years, I must have some operating experience from my plant that I could share with a greater international community so that we could all learn about this.

CHAIR APOSTOLAKIS: Independently of models.

MEMBER STETKAR: Independently of models. Independently of denominators. At the same level that EPRI was discussing.

MR. KURITZKY: Right. The operational experience.

MEMBER STETKAR: The operational experience.

MR. KURITZKY: Now the thing to keep in mind is that the majority of the people at the meeting were from regulatory agencies or the laboratories and organizations that support them. So they don't really have --

MEMBER STETKAR: Okay, thanks.

MR. KURITZKY: -- that access.

MEMBER STETKAR: Okay.

MR. KURITZKY: And I think it would be difficult to get the other people to cough it up, if they haven't.

MR. KURITZKY: Okay, again, a number of recommendations.

CHAIR APOSTOLAKIS: The Koreans, as you probably know, have been publishing many, many papers on software, various aspects. What kind of models are they using? I mean, are they drastically different from that we have been doing here or are they addressing different questions or what?

MR. KURITZKY: Well, it is a very timely question because Louis and I were discussing this earlier. Right now, the Korean models don't really address software. They are mostly hardware models also. But the Koreans are very interested in pursuing software modeling. And when we had our software PRA workshop, which I am going to talk about next, we had a gentleman from KAERI who was there. He was also someone who has been involved with some of our other work. He was at the meeting in Paris. And they are very anxious to pursue. They have I think a plan within the next three years to come up with software, failure probabilities to stick in their PRAs. So he is anxious to go do that work. They haven't really done, I don't think too much yet.

Louis, in fact, has been communicating email by them but they are interested in doing some type of cooperation. We haven't figured out exactly what.

CHAIR APOSTOLAKIS: Can you do that? Can the Agency --

MR. KURITZKY: It just showed up. We talked about it at lunch today. So we have to go back and see what is it they were thinking about doing. Whether or not we need to have a signed, bilateral agreement. I think there are certain agreements we have with Korea already. But again, to the extent of what we are going to do --

CHAIR APOSTOLAKIS: Because that would be, I think, a good step forward, to bring another group into this.

MR. KURITZKY: I mentioned early on that there were at least a couple of countries there that seemed to be doing things that were more in line. And Korea was the one that we identified as being our most comparing, similar to what we are doing. So it is an opportunity that we are going to look into.

CHAIR APOSTOLAKIS: Okay.

MR. KURITZKY: Okay, so the last thing that I wanted to talk about was the software PRA workshop that we held in Brookhaven in May. You saw reference to this earlier. In '97, the NRC asked the National Research Council to do a study on the use of Digital I&C systems in nuclear plants.

One part of that study looked at reliability and safety assessment. Two of the recommendations from that section were one, that yes, you should put software failures into your PRA models and two, you should be able to at least come up with bounding estimates for those events, using test data and expert judgment.

Okay, so taking that, as well as the fact that at this very subcommittee last year, it was recommended that the staff, when they do digital system, they integrate hardware and software. Software needs to be part of the picture, as well as the fact that we should go ahead and actually try and establish the philosophical basis for modeling software probabilistically.

Given that feedback, taking to heart, we did go ahead and have a workshop at Brookhaven back in May, gather experts to in fact some up with a philosophical basis for modeling software probabilistically.

What we did was, the objective of the workshop, the primary objective of the workshop was to come up with that basis. Since we are paying to bring together this August body of experts, we also felt that we would try and milk them for whatever we could on just how you go about modeling software and how you would quantify it.

And so we held that meeting in May. We had to decide who was going to get invited to that meeting. At first our inclination was to get people -- historically there has been some long running arguments between whether you can or cannot model software failure probabilistically. And we thought we would get a few people one side and a few people from the other side and stick them in the room and let them battle and see what the final answer is.

We later, on second thought, thought well, you know, those are long-standing arguments that have existed forever and if we bring them into a room for a day and a half, we are going to walk out with nothing further solved. And we are not really going to have anything of value for our time and effort.

So we decided instead, let's get a bunch of experts who are very experienced in the fundamental principles and the application of software reliability engineering and let them hopefully come up and establish a philosophical basis for modeling software failure probabilistically. We fed them many of the arguments that are in the literature why you are not able to do such a thing, so they could chew on those also. And in doing so, we ended up coming up with a core panel of seven researchers and professors from renowned institutions with experience in software reliability or software engineering. People have published books in this area and/or published extensively in journals and conferences and we brought them together.

We also decided to capture the perspectives and the experiences of the NRC. As well a the nuclear industry, to include a member from each of those organizations. And so these nine people were brought together to debate the issue of modeling software probabilistically and to hopefully establish a philosophical basis. Louis was the moderator for the discussions. ACRS was hosting, Myron Hecht was there. A number of other BNL, NRC observers such as myself were there to observe the discussions.

And as hoped for, they were able to come up with the philosophical basis for modeling software failures probabilistically.

Again, we are going to come back to you with the report. You can dig into it. You can give us your opinions on it and argue back and forth. I just want to give you just a quick overview. Today, since that report is not complete yet but basically, as everyone recognizes, software failure is a deterministic process. However, due to a lack of knowledge of exactly how the software fails or lack of knowledge as to the number and types of residual faults that may be in the software, the number and occurrence of triggering events, we are not able to fully account for all the aspects of the process for software failure.

So therefore, we choose to model it probabilistically. This is essentially the same basis that is used for many other probabilistic processes. The quintessential example of the random event is the flipping of a coin. Okay, we assume okay, you flip it 50-50, whatever it could come up. Could it come up heads, could it come up tails?

In fact, if you were able to totally control --

CHAIR APOSTOLAKIS: This is not the disagreement. I fully agree with the first bullet. The question is how you do it. Can you assign a failure rate or do you need to do something else?

The methodological issues are actually estimating whatever you want to estimate. I debate it. I fully agree that, you know, if you don't have a complete state of knowledge you have to have some probability some place. The question is how do you get that.

MR. KURITZKY: Right.

CHAIR APOSTOLAKIS: Does it make sense to assume failure rates for so few of our thoughts? That is where people disagree.

MR. KURITZKY: Right. Well, actually --

CHAIR APOSTOLAKIS: The other difference is that yes, I look at the record. I have so many tests and five pump failures. Fine. Then I do my song and dance and get a failure rate. The difference here is that I find one fault and I fix the damn thing. Now what do I do?

MEMBER SIEBER: You can't deduce anything.

CHAIR APOSTOLAKIS: Exactly. It is supposedly not there anymore. This is the heart of the problem, not the coin.

MR. KURITZKY: Right.

CHAIR APOSTOLAKIS: It is kind of what I expected when I saw the list of names. We need to be taught that we can do probabilistic. I mean, that is childish.

MR. KURITZKY: Okay, so --

CHAIR APOSTOLAKIS: It is not your fault, Alan. It is not your fault.

MR. KURITZKY: But nonetheless, I was taught.

CHAIR APOSTOLAKIS: Continue.

MR. KURITZKY: As far as whether or not it can be modeled probabilistically, you fix a fault but yet we have not --

CHAIR APOSTOLAKIS: You have uncertainty but the problem is you don't have a database now. What kind of database do you have?

MR. KURITZKY: Right.

CHAIR APOSTOLAKIS: You might argue that the fixing it might introduce other faults. Thank you very much. Yes, I know people have argued those things. But how do you actually do it in the real environment with a real regulatory agency that has the health and safety of real people in its hands? That is where the problem is. What do you do?

MR. KURITZKY: So we are in agreement.

CHAIR APOSTOLAKIS: Maybe they go to defense in that. I don't know. Maybe you deterministic guys knew it all along.

MEMBER BROWN: Yes. Independence and defense in-depth.

CHAIR APOSTOLAKIS: There you are.

MEMBER BROWN: And redundancy.

CHAIR APOSTOLAKIS: And diversity. Don't forget that.

MEMBER BROWN: Where you need it.

CHAIR APOSTOLAKIS: Where you need it.

MR. KURITZKY: So we are in agreement that you can probabilistically model that it makes sense to probabilistically model software --

CHAIR APOSTOLAKIS: Makes sense.

MR. KURITZKY: It is how can you come up with the value.

CHAIR APOSTOLAKIS: That is right.

MR. KURITZKY: Okay.

CHAIR APOSTOLAKIS: What is the evidence?

MR. KURITZKY: All right. So we have that first point taken care of.

So now how are we going to come up with the value? And that is --

CHAIR APOSTOLAKIS: Or the model. Or the model. But yes, I understand what you are saying.

MR. KURITZKY: So and we had some discussions in the meeting of that because once we got the coin toss out of the way, we focused on how we can go about coming up with failure probabilities and failure rates. And as expected with nine different experts, we have many different ideas. And many of your --

CHAIR APOSTOLAKIS: Two to the ninth.

MR. KURITZKY: And many of these articles that you were so enamored of earlier in the day.

So nonetheless, so we have some ideas about how to proceed. Again like you mentioned, you find the failure, you fix it. So it is very difficult to go on historical data to try and come up with the data like we do for many hardware components in a PRA.

That doesn't necessarily mean that we have no possibility of coming up with a value. It means that we may have to rely very heavily on expert judgment. We have to rely on other types of quantitative methods. It may have to be something where you qualitatively look at pictures of the system and somehow correlate them to some value.

Okay, there is no easy answer. That is why we are doing the research. We are going to pursue whether or not there are ways we can do it. In fact, in the next slide, I will talk about what our near-term work is and what our longer term work is going to address. And the question is at the end of the day, we may determine, we can come up with a value. I mean, I could around this room and ask everybody to give me their best estimate and divide it by seven. I mean, we can come up with a value.

The question is, does the value we come up with, is the level of certainty on that value sufficiently constrained where we can actually use that value for something. Can we use that result for something?

CHAIR APOSTOLAKIS: Well also, is it meaningful? Is it meaningful?

MR. KURITZKY: That is what -- if it is not meaningful, we can't use it.

CHAIR APOSTOLAKIS: I don't see that your role is one of being an advocate of a particular point of view. In the past meetings, the comments that at least I made was this is a different beast from other things that we have done in the past in the probabilistic area.

In the sense that the moment somebody says this is the failure rate, you have to question what exactly that means. Whereas, if you talk about pumps and valves and so on, we don't. We have all agreed and we do certain things.

So the difference here is that there is a fundamental question as to whether a concept like a failure rate is meaningful. That is all I said. You may come back an say, no, it is not. We are not going to do it that way for such and a such a reason. Fine, then you have a point of view.

But to say, you know, failure rate because of a do it in Hong Kong or somewhere else -- and again, their knowledge is design errors even in hardware. I do I model that? I don't know. Does anybody know?

MR. KURITZKY: It is in the data.

CHAIR APOSTOLAKIS: Some of it is. Some of it is. But if you go to the serious stuff that they found that would be realized only when you had a strong earthquake, you have a big problem there because you never had that earthquake and what if it is there.

You know, so these kinds of things, I am not sure. You have to ask these more fundamental questions. Like now we are talking about new reactors, like sodium-cooled reactors. We are going to have, the guys who will do the PRA there will have to do something that we don't do routinely for LWRs. Namely, they all have to rethink the set of initiating events. Whereas, now for LWRs we have pretty good list, you know. A lot of groups have done it. You may want to add something that is plant-specific. But by and large, I can go to two or three PRAs and look at the initiating events I have 95 percent of what I need to do.

You go to a sodium reactor or something even more exhaustive like lead-bismuth, you have to start rethinking from the beginning now. You know, what can go wrong and all that stuff.

MEMBER SIEBER: And how do you come up with failure rates for equipment that you never built?

CHAIR APOSTOLAKIS: Yes, that is right or passive systems and so on. So these create new questions.

And all we were saying at the subcommittee meeting saying that if you should take that attitude then you have to question something that appears to be routinely used somewhere else.

MR. KURITZKY: And we did. And the question is whether or not software failure rates are meaningful, software failure probabilities are meaningful was a question we put to the panel. And they believe, I think pretty much to a man, that yes, indeed, they are meaningful.

Now, that leads to the next question. If they are meaningful, how are you going to come up with them? Okay, and that is again, as I was mentioning, where we are trying to go forward with our research to try and see how we can come up with them.

CHAIR APOSTOLAKIS: And why they are meaningful.

MR. KURITZKY: Well, and that was part of --

CHAIR APOSTOLAKIS: By failure rate, the definition is minus DF over DP, or something like that, which means that something happens in time and then in the next delta T something may happen. And then I look at this guide and it tells me there is a fault due to specification requirements.

So now I am trying to make the connection. In the next delta T there will be another specification fault? Come on. You know, so that is the question. What does it mean?

MR. KURITZKY: Right. And unfortunately, you don't have the benefit of the report because it hasn't been published yet. But in the report, we go over the expert's discussion of these very issues. So we raised those exact issues with the experts. We actually sent them questionnaires prior to the meeting to get them on the right page, to have them start thinking.

And some of these exact issues were put on the questionnaire. We got detailed responses from them. Those were further elaborated on during the meeting in the discussions. The report that we will be publishing, hopefully within the next couple of months, will detail the results of those discussions.

Now, just because we got the --

CHAIR APOSTOLAKIS: So if there is failure rate, I can work backwards and find a cumulative distribution function. Right? I can always work backwards, which means that the software, if I wait long enough, will fail. Is that good? Is that reasonable, you guys could develop software?

If I sit back and wait, eventually the probability is one.

MR. HECHT: Just like any other component to the system.

CHAIR APOSTOLAKIS: Really?

MR. HECHT: Yes.

CHAIR APOSTOLAKIS: Well that is news to me.

MR. HECHT: That program eventually is going to fail. If I run the plant for a thousand years, --

CHAIR APOSTOLAKIS: The program? Why would the program fail?

MR. HECHT: Why would the program fail?

CHAIR APOSTOLAKIS: Random things?

MR. HECHT: Because eventually the environment in which the program runs, will encounter a set of inputs that would --

CHAIR APOSTOLAKIS: I don't' know about that.

MEMBER SIEBER: The interesting thing, the software question is analogue controllers, to my knowledge have been in the business 50 years. I have never seen one fail. And so when you go from analogue to digital, you are introducing a failure rate that is greater than the analogue failure rate. And ask yourself why are you doing it. It is either for cost, higher power output for a given size plant, lower fuel costs, greater maneuverability. And so here is the tradeoff, except some probably minuscule higher failure rate to obtain more flexibility, more efficiency, what have you. And that is what really ought to be weighed.

MEMBER BROWN: You never had an analogue controller failure?

MEMBER SIEBER: I can't remember any.

MEMBER STETKAR: I can.

MEMBER BROWN: That was a maintenance issue.

CHAIR APOSTOLAKIS: So the report you are about to publish will have all of this stuff in it?

MR. KURITZKY: Yes.

CHAIR APOSTOLAKIS: We are going to review it and do whatever.

MR. KURITZKY: Right.

CHAIR APOSTOLAKIS: So maybe it is not worthwhile spending too much time today.

MR. KURITZKY: I agree with that.

CHAIR APOSTOLAKIS: Because we haven't

seen it.

MR. KURITZKY: Exactly. That's right. Exactly.

New topic but really a follow-on to that topic because given the fact that coming out of that workshop, we felt that there was a consensus among the participants that it did make sense to model software failures probabilistically, you know, come up with failure probabilities and failure rates. And they had some ideas about how you might do it but they were failure scattered.

Our next piece of work is to go ahead and look at how we can take that next step. So, BNL is pursuing a review of quantitative software reliability methods. We mentioned this earlier the presentation. They are basing it on stuff they had done previously, adding in some other stuff has been done recently, as well as some done by OSU, etcetera. And they were going to try and identify one or two technically sound approaches for modeling and quantifying software failures. And again, it is debatable whether or not this will be successful. When you get a chance to see the report, you will have the opportunity to give us feedback on what you feel the extra panel came up with, what you think about it.

But based on the outcome of that meeting, we feel confident that we are ready to take the next step. And so we will move forward in that manner. And if we are able to come up with one or two technically defensible approaches or technically sound approaches, the next step would be to apply those in a proof of concept study similar to the benchmark studies for the hardware models that we did. We would take a protection system and see if we can, you know, take the software from the protection system and see if we can use those methods or approaches to come up with a failure probability.

MEMBER BROWN: Why would we want to do that? Are we trying to figure out how we can reduce a four-channel protection system to one-channel because we do a PRA on the one channel and determine that it is going to have a failure probability of one times ten to the minus seven? Is that it? Is that a cost reduction? Is that goal?

MR. KURITZKY: No. This is the goal. The goal is to be able to make risk-informed decisions on digital systems because the Commission wants us to. And the other goal is to be able to include those models into those systems into plant PRAs because plant PRAs need to reflect the as-built, as-operated plant. And if those are going to be system in that plant, they need to be in that PRA.

MEMBER BROWN: Did the Commission actually say do this with Digital I&C systems or did they say that they wanted PRAs used extensively by the state-of-the-art for risk-informed decisions and --

MR. KURITZKY: They directly said the latter. And if you look at some of the SRMs, you will see that they infer the first. They say they want us to look into risk modeling of digital systems.

MEMBER BROWN: I still, it doesn't tell me what do I use that for? What is my end product? The only thing I can see is I want to --

MEMBER SIEBER: Overall risk for the plant.

MEMBER BROWN: What?

MEMBER SIEBER: Overall risk of the plant.

MEMBER BROWN: You know, am I going to reduce the number of systems I have? That is the only relevant reasons to do it. Am I going to -- I mean, we determined years ago. We went from one out of two protection systems to two out of three to two out of four for good reason. For online reliability and for the enhancement in terms of your ability to shut the reactor down or, when it needs to, yes, or execute an

ECCS system when it needs to.

MR. HECHT: Charlie, can I suggest one reason?

MEMBER BROWN: Absolutely. That is why I asked the question.

MEMBER STETKAR: Charlie, if you were a regulator and had limited resources and you wanted to do an inspection program, do you allocate 100 percent o your available resources to inspect every last bit of piece of equipment in the plant equally because it is all equally important or do you, for example, use some risk insights to look at stuff that might be more significant?

MEMBER SIEBER: Or do you need to --

MEMBER BROWN: No. That is why I put in four systems. I mean, I don't understand.

MEMBER STETKAR: No, no, no. You put in four systems because that is the way you used to work. You can't do that when you have got a bazillion different systems and three inspectors. My tax dollars don't pay for the amount of people you had to look at your forces.

MEMBER SIEBER: When we conclude the Commissioners said it is our policy to risk-inform. We want a new safety clause.

MR. HECHT: I could suggest another reason, with your permission, Jack.

MEMBER SIEBER: Okay.

MR. HECHT: And that is, is that let's assume that we have some method to infer the failure probability of the software, based on observation, either tests or operating experience. And we can assign an upper and lower confidence limit to that.

If we assume that and I think that is ultimately if this research is successful, the more resources we spend, the narrower that confidence limit. But it costs money, and it takes time, and it may mean that some things don't get done. A risk-informed approach would tell you at what level you are willing to accept some digital technology, some software-based item, and at what point you need to stop.

MEMBER BROWN: You mean, what point you wouldn't use digital-based technology?

MR. HECHT: No. At what point something that you don't know about that you don't have enough insight into becomes acceptable. Because you have somehow or other gotten more observations. You have put more resources into valuating it so that you can understand it better and the failure probability or the overall risk goes down.

MEMBER SIEBER: It is the same argument as the maintenance rule. The same argument that John put forth a few minutes ago.

CHAIR APOSTOLAKIS: So the basic regulatory guide, 1174 requires for any change, --

MEMBER SIEBER: It is policy.

CHAIR APOSTOLAKIS: -- you have to have the basic risk of the plan.

MEMBER SIEBER: Right. It is policy.

CHAIR APOSTOLAKIS: Right now, they assume that software doesn't fail, digital software doesn't fail.

MEMBER BROWN: Who does that?

CHAIR APOSTOLAKIS: Oh, yes. Go and look.

MEMBER BROWN: Well who designs based on software will fail? That is why you have your design rules.

CHAIR APOSTOLAKIS: And then when you apply those rules, they say that is it now. Now failure.

MEMBER BROWN: No. Let's assume the software does fail. That was the whole basis of all the designs we did. We assumed the software would fail.

CHAIR APOSTOLAKIS: It is like other systems, if you look at the ESBWR PRA, it says they don't fail. Those days, it is a law of nature. Are you questioning them?

MEMBER BROWN: USAPWR?

CHAIR APOSTOLAKIS: ESBWR. Yes, there was a clear sentence there, which I cannot find again.

MEMBER BROWN: Well, I missed that sentence.

CHAIR APOSTOLAKIS: I am looking for it. We assume that passive systems do not fail, period.

MEMBER BROWN: Hold it. A protection system is not a passive system.

CHAIR APOSTOLAKIS: No, but I am telling you, there are certain things we cannot do. Yet, the regulations require the complete risk from the plant. And for those two items, the assumption there in the risk assessment is that they don't fail or they fail with ten to the minus a hundred.

MEMBER SIEBER: But that may not accomplish your purpose.

MEMBER BROWN: But the protection is not a passive system.

MEMBER SIEBER: Well, we are arguing about it.

CHAIR APOSTOLAKIS: I am just saying that there are these two areas, passive and digital, two separate things. We don't know how to do it. They never fail.

MEMBER BROWN: Moving on. I know you know they say if you look at the software failure but you design the overall systems and how you do it and the number you have, the redundancies and independents, so that when they do fail, you won't have so many of them fail that you can't shut down the plant. That is the point.

CHAIR APOSTOLAKIS: Maybe that is what I mean.

MEMBER BROWN: That is the point.

CHAIR APOSTOLAKIS: Maybe that is what I mean, that is my contribution.

MEMBER BROWN: You make an assumption. I mean a fundamental assumption, I mean, I have got these on every ship in the Navy and our fundamental assumption is the software will fail.

So for critical systems, ECCS, where we wanted to do it, protection systems, that is what we did. On a turbine-generator set, we didn't do that. Recently it failed. But we designed the hell out of it so hopefully it wouldn't so we can keep power going and the prop can continue to go around.

But that assumption that software will not fail is to me, just that is somebody has got their head -- I'm sorry. I won't go there.

CHAIR APOSTOLAKIS: Well but this is the situation we want.

MEMBER SIEBER: You can always go and trip the breaker.

MEMBER BROWN: Too late, maybe.

CHAIR APOSTOLAKIS: Okay. Are you done?

MR. KURITZKY: Just one point I want to make. I alluded to it in part earlier and I want to make it more completely now is that while we expect we will be able to come up in some way, shape or form with a digital system model, including software, the bigger issue or issues are going to be, as we mentioned before, is it something useful. Is the model that we are going to come up with something that can be used? Is the data that is used for the grammar or the input to that model going to have sufficient constrained uncertainty that this actually give you a useful answer. And B, even if you can come up a useful answer, is the level of effort that it requires to come up with that answer, to develop that model, is it practical? Is it something that you can have some PRA engineer or licensees go ahead and put together this model.

So just the fact whether you can do it, doesn't mean that it is necessarily something that we would ultimately want to do or would necessarily get done on a routine basis. It has to end up being useful and it has to be practical. And those two questions remain to be seen.

Last point. We alluded to many of these milestones earlier. But the NUREG/CR-6997 should be published n the next couple of months. The letter report on the software PRA workshops should also come out in the next couple of months.

The QSRM review that BNL was currently undertaking, we should have a draft letter report out for peer review at the beginning of next year and issue the final report later in the year.

So that comes down to where would be the best time to come back and give the subcommittee a more detailed briefing on the work that we have bee doing. And I felt there is a possibly a target of somewhere around February 2010 because at that point in time, we will have the software PRA workshop letter report that we can give to you. We will have the draft letter report that BNL has done and look at the quantity of software reliability methods, as well as probably some better update on the plans for our work going forward.

So I think that is the kind of time frame that I think would be beneficial to come back to the subcommittee and let you see what went on at that workshop, let you see what our thoughts are on quantitative software liability methods. And then you can give us your feedback as to whether or not you think we are on the right path, whether there are things we should be looking at or whether we were totally off the wall or whatever.

But I think that is probably the time that kind of balances getting our feedback to us in a timely manner but also have the opportunity to get you some products to sink your teeth into.

CHAIR APOSTOLAKIS: Well, first of all, do the members want to go around again to comment just on this? Because we are commenting on the plan. I think a lot of the details were discussed the last couple of hours probably should be postponed, --

MEMBER SIEBER: I agree.

CHAIR APOSTOLAKIS: -- until we know really, until we have a document from you and we know exactly what you are saying.

So from the plan's perspective, there is an item there that says we are continuing the work on PRA. We will probably say okay. Right? Because we cannot go into the details of what they are doing now, unless somebody has an objection to that. So we are really commenting on the plan and you gave it some feedback a little earlier. And tomorrow we are going to look at the two ISGs. And I guess it will be one letter. Right?

MS. ANTONESCU: Two letters.

CHAIR APOSTOLAKIS: No, excuse me. Two letters. Only one of the ISGs?

MS. ANTONESCU: We had plans for one letter for the Digital Research I&C plan and the second one for the ISG on fuel facility.

CHAIR APOSTOLAKIS: So I have three letters?

MEMBER BROWN: No, no.

CHAIR APOSTOLAKIS: I was told two.

MEMBER BROWN: You were going to do one letter on both ISGs, weren't you?

MS. ANTONESCU: Yes one letter on that.

MEMBER BROWN: So one letter on that and one letter on the R&D plan.

CHAIR APOSTOLAKIS: And why can't we

combine them and have one letter for everything?

MEMBER BROWN: Depending on the outcome of the ISGs, peoples conclusions from reading and seeing what they consist of, if we have general agreement with where they are going, you probably could, unless there is something that we consider that ought be re-looked at.

CHAIR APOSTOLAKIS: Well anyway, whether we have two letters or one letter is not that important.

MEMBER BLEY: It would be essentially, if it is one letter it would be the two pieces stuck together.

CHAIR APOSTOLAKIS: Yes, that could be.

MEMBER BLEY: So, it could be two as easily. It just seems that the plan ought to have its own letter separate from the ISG.

CHAIR APOSTOLAKIS: If that is what you want.

MR. HECHT: Among other things, it comes earlier so you don't have to do it twice.

MEMBER BROWN: No, the plan letter is for September. Oh, that is --

CHAIR APOSTOLAKIS: All critical support letters.

MEMBER BROWN: No, that is not what she told me earlier.

MS. ANTONESCU: It is for September.

CHAIR APOSTOLAKIS: Which one is for September?

MS. ANTONESCU: The plan.

CHAIR APOSTOLAKIS: How about the ISGs?

MS. ANTONESCU: October.

MEMBER BROWN: October.

MR. HECHT: So let's make it two letters.

MEMBER BROWN: It is two letters.

CHAIR APOSTOLAKIS: Oh, I thought it was for this time.

MS. ANTONESCU: No.

MEMBER BROWN: If you look at the agenda.

CHAIR APOSTOLAKIS: Why do we?

MS. ANTONESCU: Because we planned to talk about all these things for this upcoming.

MEMBER BROWN: It is a convenient location. You agreed to that.

CHAIR APOSTOLAKIS: Oh, okay.

MS. ANTONESCU: It was the best time for everybody.

CHAIR APOSTOLAKIS: I thought we were commenting on both.

MEMBER BROWN: Yes, we will, eventually.

MEMBER BLEY: I don't think we had a day in September to get together to go over the second one.

CHAIR APOSTOLAKIS: Okay, so it is only the plan.

MEMBER BROWN: Yes, for September. I won't be here in October.

MS. ANTONESCU: What?

MEMBER BROWN: I'm going to Tokyo --

MS. ANTONESCU: Oh, yes.

MEMBER BROWN: -- under duress.

MEMBER BLEY: I thought you did something wrong.

MR. HECHT: Alan, can I ask you a question?

MR. KURITZKY: Yes.

MR. HECHT: With respect to the quantitative, the QSRMs, we have heard that term before, there are I think two parameters that you need, at least for the state-based models that I am used to. One is the failure rate and the other one is the recovery probability or its converse failure probability upon demand.

In other words, one is a rate over time

and I guess you might call it a failure intensity function but it might not be a constant value. It might have a certain upward or downward trend. And the other one would be the probability of failure on demand. Or like I say, its compliment, the probability of successful operation upon demand.

Which do you plan to address or do you plan to address both?

MR. KURITZKY: I will have Louis answer it.

MR. CHU: I think we tried to address both because both are needed in the PRA model.

MR. HECHT: Thank you.

CHAIR APOSTOLAKIS: The question now is what should the staff present to the full committee in September? Is it the plan only?

MS. ANTONESCU: We cannot schedule the ISGs. We don't have time now for the ISGs in September.

CHAIR APOSTOLAKIS: We have an hour and a half for the plan.

MS. ANTONESCU: About an hour and a half.

CHAIR APOSTOLAKIS: Is that where we are? I mean, the members agree?

MEMBER BROWN: It just came out for the

meeting in September. I don't remember how much time was in it.

CHAIR APOSTOLAKIS: It seems only an hour and a half.

MEMBER BLEY: Well we lost that other session.

CHAIR APOSTOLAKIS: Well they rearrange things but they never do more than an hour and a half on a particular topic.

MS. ANTONESCU: An hour and a half.

CHAIR APOSTOLAKIS: So it is always an hour and a half.

MS. ANTONESCU: Do you know about the plan, how much time we got?

MR. DIAS: It is probably an hour and a half. I can check it.

CHAIR APOSTOLAKIS: So you guys will present, repeat what you did here? I mean, here you had a few hours.

MR. SANTOS: Yes, I think I can say probably do it in less than an hour and a half.

CHAIR APOSTOLAKIS: So you will take out some of the stuff you presented to us?

MR. SANTOS: Some where I said better.

MEMBER BROWN: Pick out some of the stuff.

MR. SANTOS: Right.

CHAIR APOSTOLAKIS: That is what I am saying. You will take out some of the stuff.

MEMBER BROWN: Some of it was boilerplate.

MR. SANTOS: Yes.

MEMBER BLEY: Don't take out the part on the interagency cooperation.

MR. SANTOS: Okay.

MEMBER BLEY: I think that will be very interesting to the full committee.

CHAIR APOSTOLAKIS: I remember this one that got stuck at the beginning there somewhere. What was it about? Further communication.

MEMBER BROWN: Yes, that one. Don't mess with that one.

CHAIR APOSTOLAKIS: Remember, there are seven other members or whatever. They are not shy. Well okay, then, if you feel you know what you want to do. Is there anything else we want to bring up today?

(No response.)

CHAIR APOSTOLAKIS: Well, with that, thank you very much. I thank the members. I guess the industry is gone so anyway I thank them, too. And I will see you tomorrow at 8:30.

(Whereupon, the meeting was adjourned, to reconvene on Friday, August 21, 2009 at 8:30 a.m.)

NRC Response to EPRI DAS and CCF OE Reports

Advisory Committee On Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee Meeting

August 19, 2009

Debra S. Herrmann, Senior Level Advisor for Digital I&C
Division of Engineering
Office of New Reactors

Topics

- Background
- General Comments on CCF OE Report # 1016731, final, dated 12/2008
- Results of NRC staff independent review of LER data
- General Comments on DAS Report #1016721, final, dated 12/2008
- Recommendations

Background

- NRC policy in this area, and how it was developed, is summarized in the letter from J. Grobe to NEI, dated 11/03/2008
- NRC policy has not changed
- Today we are providing our observations on the technical content of the EPRI reports

General Comments on CCF OE Report

- Fundamental concepts, definitions, and assertions:
  "Software not a significant source of CCFs"
  - This question does not address the problem of a lack of understanding of digital system failure modes, particularly as related to the nuclear industry
  - A primary concern when migrating to digital technology is that a new source of failure may be introduced: software CCFs
  - Other sources of CCFs (human error, hardware, etc.) remain essentially the same.
  - The question licensees, applicants, and NRC need answered is the prevalence of software CCFs in digital systems, so that the appropriate prevention, mitigation, and verification activities can be taken during the system engineering lifecycle
  - Determining the percentage of software CCFs out of the total CCFs experienced plant-wide is not as useful to a digital system engineer.

General Comments on CCF OE Report

- Fundamental concepts, definitions, and assertions:
  "Separation of 1E and non-1E events"
  - EPRI classified 1E software events separately from non-1E software events. EPRI then characterized the quality of non-1E systems as not being representative of the quality of 1E systems.
  - This classification assumption was questioned by the ACRS* and the NRC as being unrealistic compared to using a software integrity level categorization, which more realistically considers the effect of consequences on business operations as being nearly equivalent to consequences affecting safety.
    - *March 2008 Digital I&C Subcommittee Meeting, transcript pp. 216-285

General Comments on CCF OE Report

- Fundamental concepts, definitions, and assertions: "Separation of 1E and non-1E events"
  - EPRI: 49 events are related to 1E systems, such as reactor protection (RPS), engineered safety features actuation (ESFAS), diesel load sequencer, post accident monitoring (PAM), etc.
  - NRC Response: There is a low number of safety-related digital systems in current operating reactors
    - There are relatively simple digital implementations of parts of protection systems (i.e. core protection calculator systems, engineered safety systems)
    - Eagle 21 is not a complete digital system (DSPs)

General Comments on CCF OE Report

- Fundamental concepts, definitions, and assertions:
  "Failure mechanism v. failure mode"
  - The distinction between failure modes and failure mechanisms is an artificial boundary related to the level of abstraction
  - A digital system engineer should focus on failure modes which can affect the correct, and more importantly, the safe operation of a system

General Comments on CCF OE Report

- Fundamental concepts, definitions, and assertions:
  "Potential CCF v. actual CCF"

  - The distinction between potential CCFs and actual CCFs is an artificial boundary

  - A potential CCF is a latent defect waiting to happen, it is not a near miss that has already occurred

General Comments on CCF OE Report

- Data integrity and data characterization
  - Of the 27 software failures reported in the LER database from 4/2009 through 11/1997 only one of these failures is included in the EPRI study
  - Data prior to 1996 is of questionable value or relevance today because of its age and the rapid evolution of digital equipment
  - Instead of using the LER abstracts verbatim, the abstracts were rephrased which occasionally led to a loss of data fidelity

General Comments on CCF OE Report

Data integrity and data characterization

- Root causes
  - Categories of root causes are not mutually exclusive:
    - Ineffective change management, inadequate requirements, inadequate testing, inadequate CM, inadequate V&V, …
  - Occasionally the root causes listed are not consistent with the text in the abstract

- Corrective action
  - Categories of corrective actions are not mutually exclusive
    - Analysis(?), corrective maintenance, software change, parameter change, design change, …
  - Occasionally the corrective actions listed not consistent with the text in the abstract

General Comments on CCF OE Report

- Data integrity and data characterization
  - Three events are not counted as a CCF in the statistics, even though the text describes the event as a CCF
  - Three events are not counted as potential CCFs in the statistics, even though the text describes the event as a potential CCF
  - Failure of an analog system is included in the data records
  - An event record is included that has bogus LER number: 00-000-00, this event cannot be traced

General Comments on CCF OE Report

- Because of our comments on data integrity and data characterization, NRC staff conducted an independent review of the LER data to see if we could reproduce the same results.

- Our findings in this area are presented next.

- Note: the threshold for reporting an LER is defined in Table 3 of NUREG 1022 (page 28 of back-up data)

Results of NRC Staff Independent Review of the LER Data

- **Approach**
  - An independent analysis of software events reported in the LER database was conducted to determine the frequency with which software CCFs have been experienced by operating reactors.
  - A search of the LER database using the keyword "software" within the LER title or abstract returned 200 records.
  - To obtain the most relevant data, the most recent records were examined, those from April 2009 - November 1997.
  - This set of operational experience is representative of the digital I&C equipment installed and being deployed today.
  - The complete final LER report was examined, not just the abstract, to make a determination as to the type and cause of failure.

Results of NRC Staff Independent Review of the LER Data

- Software failures were defined to include:
  - Requirements errors
  - Design errors
  - Algorithm errors (calculation was incorrect)
  - Implementation errors (errors introduced when translating a design into code)
  - Interface errors
  - Parameter errors
  - Timing errors

- Human error, by operators or maintenance staff, was not considered a software failure or CCF.

Results of NRC Staff Independent Review of the LER Data

- Software was defined to include:
  - Operating systems
  - Utilities
  - Applications
  - Firmware (ASICs, PLDs, FPGAs, etc.)
  - Data

- Four categories of CCFs were recognized:
  - Failure of a primary and a back-up system
  - Failure of multiple systems operating in parallel
  - Failure of multiple units at a single location
  - Failure of a common vendor's product at multiple locations

Results of NRC Staff Independent Review of the LER Data

- During the timeframe of April 2009 - November 1997, 45 final LER records* were returned from the search. They were examined and classified as follows:

❖ Legitimate software failure, as defined above	27	60%
❖ Human error (operator or maintenance staff)	10	22.2%
❖ Hardware failure	1	2.2%
❖ N/A digital hardware or software	7	15.6%
❖ total	45	100%

*Only one LER record examined in this independent study was included in the EPRI report.

Results of NRC Staff Independent Review of the LER Data

- The 38 digital system failures were examined and classified as follows:

❖ Legitimate software failure as defined above	27	71.1%
❖ Human error (operator or maintenance staff)	10	26.3%
❖ Hardware failure	1	2.6%
❖ total	38	100%

Results of NRC Staff Independent Review of the LER Data

- The 27 legitimate software failures were examined and classified as follows:

❖ Common cause failure	21	77.8%
❖ Not common cause failure	6	22.2%
❖ total	27	100%

Results of NRC Staff Independent Review of the LER Data

- The common cause failures were examined and classified as follows:

❖ Failure of a primary and a back-up system	2	8.3%
❖ Failure of multiple systems operating in parallel	8*	33.4%
❖ Failure of multiple units at a single location	10*	41.7%
❖ Failure of a common vendor’s product at multiple locations	4*	16.6%
❖ total	24	100%

*Note: 2 failures of multiple systems also involved failures of multiple units, 1 failure of multiple systems also involved failure of a common vendor product.

Results of NRC Staff Independent Review of the LER Data

- The types of software failures were examined and classified as follows:

❖	CCF		Non-CCF		Total	
❖ Requirements	1	4.8%			1	3.7%
❖ Design	10	47.7%	3	50%	13	48.2%
❖ Algorithm (calculation)	2	9.5%	1	16.3%	3	11.1%
❖ Implementation	0	0%	1	16.3%	1	3.7%
❖ Interface	2	9.5%	1	16.3%	3	11.1%
❖ Parameter	6	28.5%	0	0%	6	22.2%
❖ Timing	0	0%	0	0%	0	0%
❖ total	21	100%	6	100%	27	100%

Results of NRC Staff Independent Review of the LER Data

Examples of failures

Requirements	Rod Position Deviation Monitor alarm was defined to alarm from a “greater than‘” set point rather than a “greater than or equal to” set point.	Technical Specification shutdown
Design	Control rod drive (CRD) processor software was designed to expect the day of year field to roll over to one, not zero. In addition, the software was not designed to range check the day of year field (1-366).	Reactor Trip
Algorithm (calculation)	The Electro-Hydraulic Control (EHC) System microprocessor software divided the generator output power signal by 1.5 instead of the correct value of 1.15.	Reactor Scram
Interface	A communications software error was introduced when attempting to fix another communications problem (Arcnet coupler communication boards)	Reactor Scram
Parameter	To correct excessive RFP control valve oscillations, a time constant in the Digital Feedwater Control System (DFCS) software was changed, which had an unanticipated effect (downstream transmitter delay).	Operation prohibited by the plants' Technical Specifications

Results of NRC Staff Independent Review of the LER Data

- An equivalent analysis of the EPRI software failure data yields the following results

	CCF		Non-CCF		Total	
1E Software Events	1	25%	3	75%	4	100%
Non-1E Software Events	14	70%	6	30%	20	100%
Total	15	62.5%	9	37.5%	24	100%

Results of NRC Staff Independent Review of the LER Data

- If the software failure data from the EPRI study and the NRC staff review are combined, the following results are observed

	CCF		Non-CCF		Total	
EPRI software failures	15	62.5%	9	37.5%	24	100%
NRC LER software failures*	20*	76.9%	6	23.1%	26*	100%
Total	35	70%	15	30%	50	100%

*One LER software failure from the NRC staff review was included in the EPRI study. In order not to count it twice, that event is subtracted from the NRC LER CCF failures in this table.

General Comments on DAS Report

- Report is based on ISG-2 Revision 1 which was issued 9/07 and staff guidance on D3, including the 30-minute criterion
  - ISG-2 Revision 2 and ISG-5 Revision 1 are the current documents
  - They address several of the issues raised in the report

General Comments on DAS Report

- Report assumes automated backup systems would be subject to spurious actuations[1], which would defeat the benefits of automation

- This assumption is not valid
  - Automated backup systems have not yet been designed, especially for new reactors
  - Not all spurious actuations have the same consequences to the plant
  - There are solutions to prevent spurious actuations
  - The staff expects 'enhanced quality' for the diverse systems as stated in BTP-19 and ISG-2 Revision 2

1 – A query of the LER database using “spurious actuation AND diverse actuation system” returned no records. A query of the LER database using “diverse actuation system” returned 1 record from 1991. See back-up data p. 38.

Recommended Next Steps

- Following the execution of the 5-Year Digital I&C Research Plan and the EPRI MOU, reassess policy in this area

- There is a small set of data at this time, so it is difficult to draw a valid conclusion. Therefore, industry and NRC should continue to collect data, including data from international sources, and analyze it as digital systems are installed in NPPs.

- Industry should find a more precise, accurate, and consistent way to collect, categorize, and analyze failure data.

Backup Data

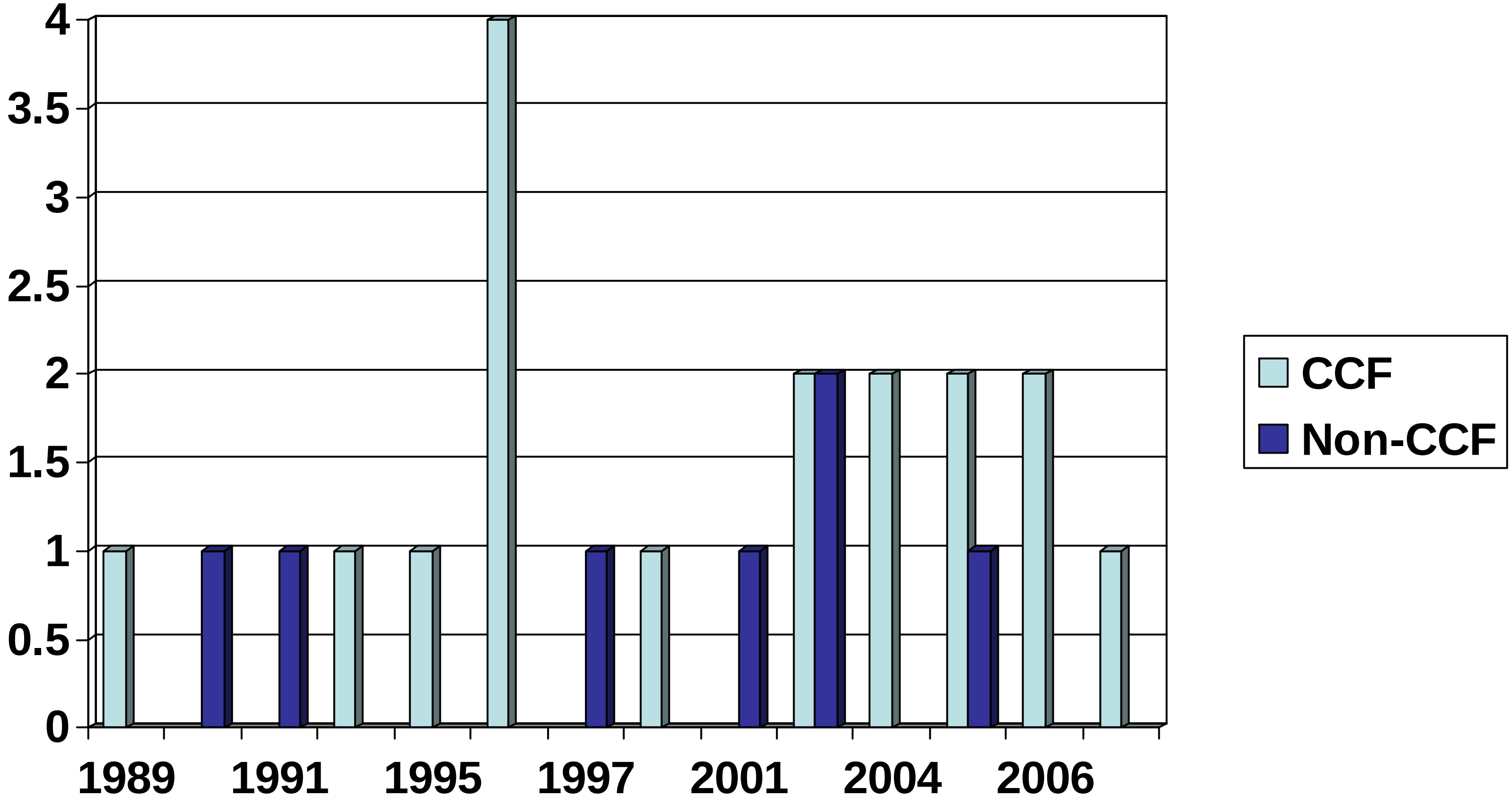
- LER Reporting Threshold
- Specific Comments on OE CCF Report
- Specific Comments on DAS Report

Threshold for LER Reporting Criteria: NUREG 1022, Table 3

- Plant Shutdown Required by Technical Specifications
- Operation or Condition Prohibited by Technical Specifications
- Deviation from Technical Specifications under § 50.54(x)
- Degraded or Unanalyzed Condition
- External Threat or Hampering
- System Actuation
- Event or Condition That Could Have Prevented Fulfillment of a Safety Function
- Common-cause Inoperability of Independent Trains or Channels
- Radioactive Release
- Internal Threat or Hampering
- Transport of a Contaminated Person Offsite
- News Release or Notification of Other Government Agency
- Loss of Emergency Preparedness Capabilities
- Single Cause that Could Have Prevented Fulfillment of the Safety Functions of Trains or Channels in Different Systems

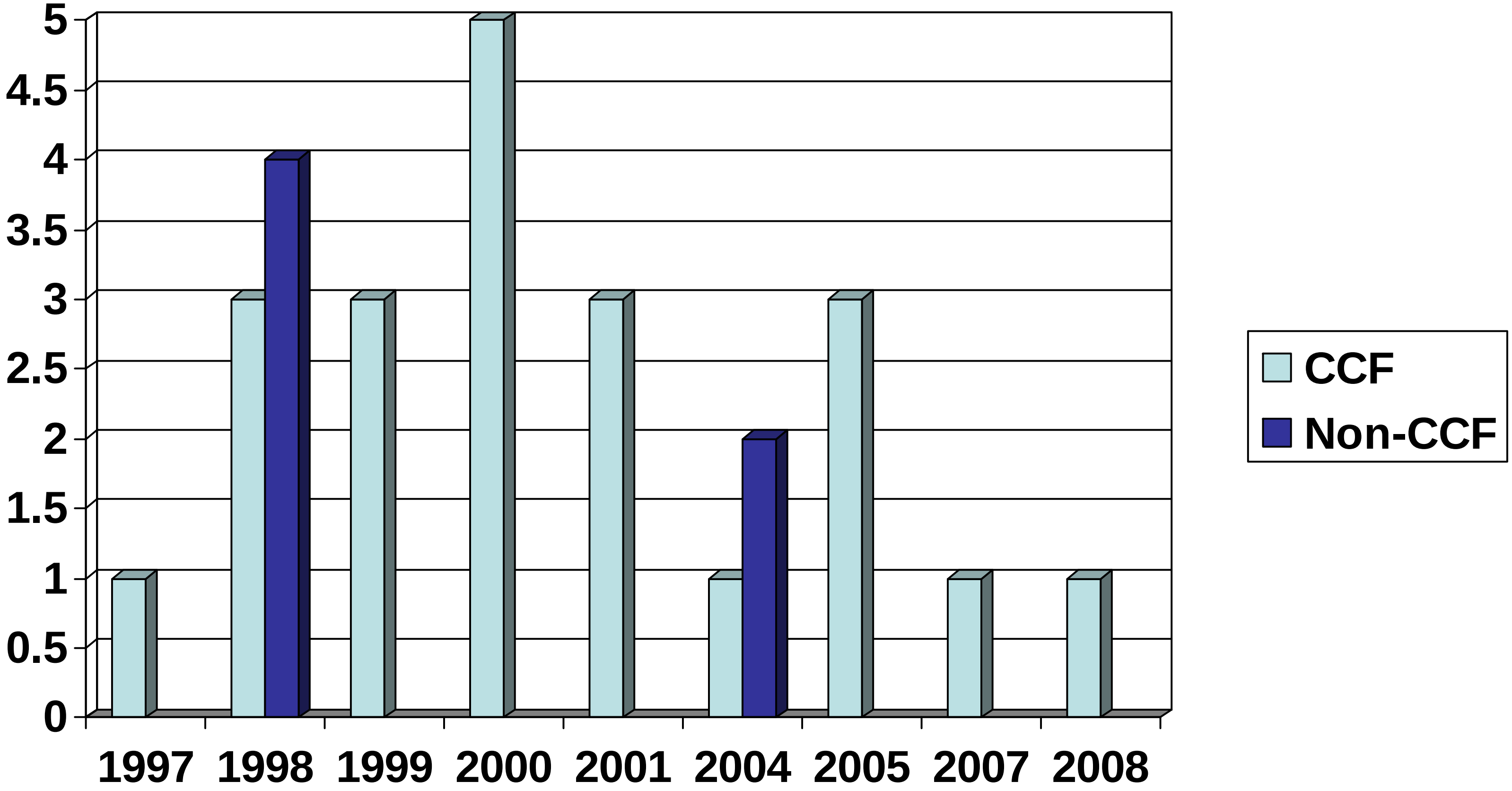
Specific Comments on CCF OE Report

Chronological Distribution of
Software Failures: EPRI Data



Specific Comments on CCF OE Report

Chronological Distribution of
Software Failures: LER Data



Specific Comments on CCF OE Report

- Peaks in events EPRI evaluated between 2000 and 2006
  - EPRI: One likely explanation is that a large fraction of the reported events correspond to learning curve design errors and mistakes in first of a kind upgrades that are discovered and corrected in the first or second fuel cycle after initial installation, and once corrected, are not recurring
  - NRC Response: All new reactor designs and most current reactor upgrades will be using first of a kind systems. Therefore, should the public expect a similar peak in reported events as new, more complex systems are implemented?

Specific Comments on CCF OE Report

- Fig 3-1, Event Breakdown (page 3-3)
  - Failure Events for each class
  - 1E common defect event rate as a fraction of total 1E events are nearly 100% higher than the corresponding class of Non-1E common defect event rate.

System Class	Non-1E (273 Events)		1E (49 Events)	
Failure Type	Events	% of Non-1E Events	Events	% of 1E Events
SINGLE DEFECT	196	71.8%	22	44.9%
COMMON DEFECT	77	28.2%	27	55.1%

Specific Comments on CCF OE Report

- Fig 3-1, Event Breakdown (page 3-3)
  - Common Defect Events_for each class
  - 1E common defect event rates as a fraction of total 1E events is higher than the corresponding classes of Non-1E common defect event rates

System Class	Non-1E (273 Events)		1E (49 Events)	
Failure Type	Events	% of Non-1E Events	Events	% of 1E Events
SW	20	7.3%	4	8.2%
Non-SW	57	20.9%	23	46.9%

Specific Comments on CCF OE Report

- EPRI: “Reactor protection systems contain significant built-in diversity in the form of different input signals that can initiate trips, such that a software fault in the processing of any one of the signals has limited impact on overall safety function. For most events, at least two diverse signals can initiate a trip in time to avoid exceeding design basis acceptance criteria.”

- NRC Response: This conclusion may not be supportable for systems in which all trip functions are integrated into a single protective system component such that a failure in one part of the system might adversely affect the whole system.

Specific Comments on CCF OE Report

- EPRI: “. . .Software Changes are performed in twice as many events as those where Software Design issues were reported as causes (Figure 4-3). This trend suggests that licensees are using software to add features that protect against recurrence of non-software failures.”

- NRC Response: Industry has been adding complexity to safety systems to increase reliability. This trend contradicts the industry argument that diverse actuation systems would adversely affect safety and add more complexity to the safety systems and thereby reduce safety system reliability.

Specific Comments on CCF OE Report

- EPRI described an event in which the control element assembly (CEA) calculation software did not account for CEA slips and delayed Rx trip by 16 seconds.
  - The defect originated in a system design that allowed multiple RPCBs coupled with an incomplete understanding of specific details of rod drop phenomena, which was then reflected in the application software logic.
  - A claim is made that a diverse platform <u>running the same logic</u> would have had the same problem, compounded by increased complexity in its design, operation and maintenance.
- NRC Response: If the diverse platform was <u>running the same design or logic</u>, the diverse platform would not have been sufficiently diverse.

Specific Comments on DAS Report

- Report assumes automated backup systems would be subject to spurious actuations, which would defeat the benefits of automation

- This assumption is not valid (continued):
  - A query of the LER database using "spurious actuation AND diverse actuation system" returned no records
  - A query of the LER database using "diverse actuation system" returned 1 record
    - 2691991009, 7/03/1991, Oconee 1, 2, 3, title: "One of Two Diverse Actuation Systems for Loss of Main Feedwater Mitigation Systems Was Found Inoperable Due to a Design Deficiency"
    - The other two Oconee units were subject to the same potential problem.
    - The root cause of this event was a design deficiency, failure to anticipate the interaction of systems, during the original design of the these systems.
    - The design of a major EFDW modification in 1979 which added the motor driven pumps and upgraded the instrumentation and controls did not consider the role of HDPs.
    - Similarly, the installation of the loss of feedwater anticipatory RPS trip in 1981 also did not consider the role of the HDPs.

Specific Comments on DAS Report

- The 2nd paragraph of 6.1.2 states the failure probability for digital systems is 10^{-4}
  - No basis is given for this claim

Specific Comments on DAS Report

- Row 5 of Table 4-2 (BWR steam line break outside containment) shows 11 minutes to fuel damage, assuming no MSIV closure or reactor makeup

- The report states for this example:
  - "the proposed automated DAS is not needed for steam line break outside containment."

- It is hard to make the conclusion that a DAS is not needed in the absence of a human factors analysis

Specific Comments on DAS Report

- For Table 5-6 CE #1, the spurious DAS CDF of 1.2E-8/yr can not be reproduced

- Spurious ECCS IEF of 0.0024/yr times 2.1E-5 CCDP should give 5E-8/yr not 1.2E-8/yr
  - Correct math error -- there appears to be a transcription error between spurious ECCS and spurious SG isolation
  - Same error is in Tables E-2, E-4, and E-6

Specific Comments on DAS Report

- For Table E-8 CE #1, the spurious SG isolation CDF of 5E-8/yr can not be reproduced

- Spurious SG isolation IEF of 0.0024/yr times loss of FW CCDP of 5E-6/yr should give 1.2E-8/yr not 5E-8/yr
  - Correct math error -- there appears to be a transcription error between spurious ECCS and spurious SG isolation

Specific Comments on DAS Report

- Two major human error probabilities are quantified
  - Case 1 is for operator to initiate low pressure injection for the RPV flooding contingency with a time window of 9 minutes and cognitive human error probability of 0.16
  - The second case is for RPV level control with a time window of 19 minutes and cognitive HEP of 1.2E-3
- The performance shaping factors and type of response are basically identical. The analyses are based on T-H (MAAP) runs. The factor of 2 difference in time window results in nearly two orders of magnitude difference in HEP, indicating a hypersensitivity to available time and hence great sensitivity to the T-H analyses. The T-H analysis used as input to the HCR model is clearly a major source of uncertainty.
  - This source of uncertainty should be addressed in Section 6.1.4.

NRC DIGITAL SYSTEM RESEARCH PLAN
FY 2010 THROUGH FY 2014

Advisory Committee on Reactor Safeguards
Digital I&C Subcommittee
August 20, 2009

Russell Sydnor
Daniel Santos
Division of Engineering
Office of Nuclear Regulatory Research
(301-251-7405, russell.sydnor@nrc.gov)
(301-251-7664, daniel.santos@nrc.gov)

AGENDA

- Purpose and Objectives
- Background and the current FY05-FY09 Digital System Research Plan
- Development of the new FY10-FY14 Digital System Research Plan
- Proposed Research Programs
- Research prioritization, schedule, metrics, and tools

Purpose and Objectives

- To obtain a letter of endorsement from the ACRS for the FY10-FY14 Digital System Research Plan
- To discuss and obtain insights from ACRS members on the strategic direction of Digital System regulatory research and improving the research plan
- Help answer the question: Are we missing something?

BACKGROUND

- **NRC reviews of digital I&C systems are challenging**
  - **Need to supplement and augment current review guidance**
  - **Need to develop technical bases to support risk-informed digital system reviews and operational assessments**

BACKGROUND, cont.

- **Issues include**
  - Complexity and potential new failure modes
  - Enhancement of appropriate skills and knowledge base
  - Limited operating history
  - Higher level of system integration and complex communication schemes
  - Cyber vulnerabilities

BACKGROUND, cont.

- **RES develops technical bases, guidance, and methods to support regulatory decisions**
- **Accomplished through**
  - **Confirmatory and anticipatory research**
  - **Testing and analyses**
  - **Development of tools, data, and analytical models**
  - **National and International Collaboration**

BACKGROUND, cont.

- Research plans are a communication and planning framework to identify necessary research initiatives to support regulatory decisions
- NRC research collaborates with industry research when the research and products are complementary and beneficial

BACKGROUND, cont.

- 1997 NAS report “Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues”
- NRC Digital System Research Plan FY01 - FY04 focused on several 1997 NAS report recommendations and I&C vendor development efforts

BACKGROUND, cont.

- **NRC Digital System Research Plan FY05 - FY09 continued previous research and added significant new research topics such as:**
  - **Cyber security**
  - **What constitutes adequate diversity?**
  - **What are the guidelines for developing FPGA-based safety systems?**
  - **Highly integrated control rooms**

BACKGROUND, cont.

- **NRC Steering Committee for Digital I&C established in 2007**
  - **Created to address specific industry questions**
  - **Re-prioritization of research, with focus on supporting development of ISGs**
  - **Research provided technical support and information to various TWGs**

FY05 - FY09 Digital System Research Plan

Covers Seven Research Programs

- Digital system research
  - Diversity and Defense in Depth
  - Highly Integrated Control Rooms
  - Other issues
- Software safety/dependability/reliability
- Risk assessment of DI&C systems
- Security of digital safety systems
- Emerging technology research
- Advanced reactor DI&C
- Collaborative research and Standards development

FY05-FY09 Digital System Research Plan

- Status as of 8/09: 7 research programs made up of 29 research projects and tasks
  - In 21 of 29 areas - significant research progress
  - 23 research products delivered
  - 17 Projects in progress
    - 7 expected to be completed by the end of 2009/early 2010
    - On-going projects carried over to the new plan
  - Research was not initiated in 8 project areas
    - 3 carried over to the new plan
    - 5 will not be pursued based on User Office input and re-prioritization

- **FY05 – FY09 Projects that were not started and not selected for FY10 – FY14 scope**
  - **COTS Digital Systems**
  - **THD effects on DI&C**
  - **Radiation Hardened ICs**
  - **Smart Transmitters**
  - **Advanced NPP Digital Risk**

FY05-FY09 Digital System Research Plan

- **Challenges**
  - **Staff Turnover**
  - **Resource issues (e.g., continuing resolutions, DOE Lab COI)**
  - **Re-prioritization to support emerging needs**
    - **DI&C Steering Committee and TWGs**
    - **Licensing Office User Needs**
  - **New information on actual applications of the technology**

DIGITAL SYSTEM RESEARCH PLAN FY10- FY14

- **Collaborative efforts with supported Offices**
  - **Multiple meetings and presentations with staff**
  - **Working drafts provided to solicit informal inputs**
- **Current draft is the result of input from the I&C staff, I&C branch chiefs, and senior advisors from program offices (NRR, NRO, NSIR and NMSS)**

DIGITAL SYSTEM RESEARCH PLAN FY10- FY14

- **Comments, needs, and priorities of the various offices have been incorporated. Comments included**
  - **Include NRC training courses as an optional task for each research project statement of work**
  - **Avoid duplicate efforts, leverage information readily available in the public literature, and encourage industry to take the lead on research topics more applicable to industry (e.g., sustainability and obsolescence management)**

DIGITAL SYSTEM RESEARCH PLAN FY10- FY14

- **Comments included, cont.**
  - **Continue digital I&C PRA work**
  - **Evaluate the capabilities and limitations of automated tools used in various life-cycle activities**
  - **Improve understanding of digital technology failure modes and effects and their analyzes**
  - **Provide specific deliverables**
    - **Staff guidance, acceptance criteria, tools and methods, review procedures, training curricula**

RESEARCH PROGRAMS

- **Digital System Research Plan FY10 - FY14**
  - **Safety Aspects of Digital Systems 3.1**
  - **Security Aspects of Digital Systems 3.2**
  - **Advanced Nuclear Power Concepts 3.3**
  - **Knowledge Management 3.4**
  - **Additional Carry-over Projects from Digital System Research Plan FY05 – FY09 3.5**

Communications Among Plant-wide systems

- **Background**
  - **10CFR50, GDC 24 – “Separation of Protection and Control Systems”**
  - **IEEE Std 603 requirements for independence, etc.**
  - **ISG#4 provides guidance for interdivisional communications and network configurations**
- **Technical Basis**
  - **Address issues such as independence, interdivisional two-way communications, data density, communication protocols, and vulnerabilities through the development of a generic model**

Communications Among Plant-wide systems

- **Outcome, cont**
  - **Additional regulatory guidance on DI&C network characteristics and communication protocols**
  - **Recognition of network-based challenges to reliability, redundancy, and independence among systems**
  - **Development of a generic model of plant-wide digital systems**

Safety Assessment of Tool Automated Processes

- **Background**
  - **Lifecycle activities are becoming more automated (e.g., code generation, V&V)**
  - **“Proven in use” claims are not easily assessable**
- **Technical Basis**
  - **Shift in source of errors from the primary engineering activity (e.g., coding mistakes) to mistakes in the process design and tool automation**
  - **Lack of error detectability and errors could be exacerbated through other life-cycle phases**

Safety Assessment of Tool Automated Processes

- **Outcome, cont**
  - **Regulatory guidance to provide acceptance criteria regarding the use of tool-assisted or tool-automated engineering activities**

Development of Benchmark Reliability Data

- **Background**
  - **Continuation from the previous plan**
  - **UVA fault injection process to estimate digital system dependability for use in PRA models**
- **Technical Basis**
  - **High quality design, defensive measures, and rigor may not prevent or mitigate all faults**
  - **Invasive method to detect faults that were not discovered during the system development process**
- **Outcome**
  - **Develop a testing tool to augment determinations of "reasonable assurance" and develop a process for evaluating reliability**

Integrated Plant & DI&C System Modeling

- **Background**
  - **Digital I&C lacks supplementary tools and proven models for validation**
- **Technical Basis**
  - **An integrated plant model enables better simulation of overall plant response to digital systems failures**
  - **Assist in the validation and safety impact of proposed software based enhancements**
- **Outcome**
  - **Develop a model to assist reviewers in the validation and characterization of DI&C on reactor safety**

Digital System PRA

- **Background**
  - **Need to establish processes to support risk informing regulatory reviews of digital technologies**
  - **Proof-of-concept benchmark studies conducted including various modeling methods**
  - **In May 2009 workshop, experts established philosophical basis for modeling software failures in a reliability model**
- **Technical Basis**
  - **Remaining long term issues (e.g., understanding of failure modes; failure propagation; quantification of reliability, including software; uncertainty analysis; human-reliability associated with digital systems; integration of risk insights)**

Digital System PRA

- **Technical Basis, cont.**
  - **Lack of international consensus**
  - **Feasibility and practicality of methods and development of standard regulatory framework**
- **Outcome**
  - **Development of PRA methods, tools, and guidance, if practical, to support:**
    - **Nuclear plant licensing decisions using information on the risks of digital systems**
    - **Including models of digital systems into nuclear plant PRAs**

Operating Experience Analysis

- **Background**
  - Ongoing project that responds to ACRS recommendation for the staff to evaluate the OpE with digital systems in the nuclear industry and other industries to gain insights regarding potential failure modes
  - Work to date has supported work on diversity strategies
- **Technical Basis**
  - Data from operational experience obtained and analyzed to date have been found to be inadequate and not statistically significant to identify and analyze failure modes, partially exacerbated by rapid changes and different application domains

Operating Experience Analysis

- **Technical Basis, cont**
  - What constitutes adequate Ope information that would support concluding that a component/system is acceptable? What meaningful information can be extracted from OpE?
- **Outcome**
  - Document insights gained from OpE data reviews
  - An improved failure reporting framework for DI&C related incidents and for “proven in use” claims
  - A digital component failure parameter database to support PRA research

Analytical Assessment of DI&C Systems

- **Background**
  - **ACRS 2007 recommendation – (inventory and classification of the various types of DI&C systems and components in use; EDO letter to the ACRS dated May 28, 2008 (ML081290195)**
  - **Staff Requirements Memorandum M080605B dated July 2008 (Identify failure modes; feasibility … risk quantification)**
  - **Enable research in DI&C PRA and HF**
  - **Inadequate information from OpE**
  - **NRR need for analysis of 3 pre-approved platforms in highly integrated environment**

Analytical Assessment of DI&C Systems

- **Technical Basis**
  - **Advancement in understanding DI&C failure modes**
  - **Feasibility of applying failure analysis in risk quantification**
  - **Focus: Application domain characterized by currently approved + emerging systems.**
  - **Framework useful in analyzing OpE for root cause**

Analytical Assessment of DI&C Systems, cont.

- **Outcome**
  - **Inventory and classification/characterization of DI&C systems for safety functions in NPPs**
  - **Identification of credible systematic failure and fault modes typical of software-intensive DI&C systems**
  - **Framework of contributing factors**
  - **Support for other research projects**

Diagnostics and Prognostics

- **Background**
  - **Proper use of diagnostics, prognostics, and self-testing techniques in non-safety systems has shown improvements in reliability and availability**
  - **Expect use on safety systems and in more integrated systems (e.g., new and advanced reactor designs)**
- **Technical Basis**
  - **Need to assess the safety impact of these systems and techniques and their impact on equipment operability**
- **Outcome**
  - **Regulatory acceptance and review criteria**

Security of Digital Platforms

- **Background**
  - **Ongoing project by Sandia National Laboratories**
  - **Conducting cyber-vulnerability assessments on NRC approved digital platforms**
- **Technical Basis**
  - **Cyber vulnerabilities, if exploited, represent a source of potential failures that could lead to safety significant consequences**
- **Outcome**
  - **Gain an understanding of cyber vulnerabilities in approved platforms**
  - **Investigate the appropriate elimination and mitigation of potential security hazards**

Security of Digital Platforms

- **Outcome, cont**
  - **Provide additional regulatory guidance and acceptance criteria to support assessments of digital systems in nuclear facilities and applications**

Network Security

- **Background**
  - **Ongoing projects by Sandia and Oak Ridge National Labs**
  - **ORNL Letter Reports on Wireless Network security**
- **Technical Basis**
  - **Cyber vulnerabilities, if exploited, represent a source of potential failures that could lead to safety significant consequences**
  - **Networks can present additional vulnerabilities as network architectures increase in complexity and system reach**
- **Outcome**
  - **NUREG/CRs discussing wireless and wired network security vulnerabilities and mitigation strategies**

Network Security

- **Outcome, cont**
  - **Additional regulatory guidance for identifying potential vulnerabilities and performing network security assessments**

Security Assessments of EM/RF Vulnerabilities

- **Background**
  - Ongoing project by Sandia National Laboratories
  - NUREG/CR Study of EMP from early 1980s
  - Preliminary Reports to date evaluate two NPPs
  - The Commission has not specifically identified EM/RF emitting weapons as a credible threat to nuclear stations, however, some limited anticipatory research is considered prudent
- **Technical Basis**
  - Digital technologies tend to have a higher vulnerability to EMP than analog systems due to different operational environments (voltage, current, frequencies, materials)
  - The nature of EM/RF weapons continues to evolve

Security Assessments of EM/RF Vulnerabilities

- **Outcome, cont**
  - Support a new regulatory position on EM and RF
  - Recommendations for potential mitigations, as appropriate

Advanced Reactor Instrumentation

- **Background**
  - **Need to conduct anticipatory research to analyze the requirements and potential safety issues involved with instrumentation of advanced reactors**
- **Technical Basis**
  - **Advanced reactors (high temperature gas cooled and liquid metal) will operate in conditions different from the current generation of reactors.**
  - **Different transducers may require different approaches for accuracy assessments and compensation methods**

Advanced Reactor Instrumentation

- **Outcome, cont**
  - **Regulatory guidance for reviewing advanced instrumentation for use in advanced reactor (e.g., HTGR) safety systems**

Advanced Reactor Controls

- **Background**
  - Anticipatory and exploratory research for increased used of automation and advanced control algorithms in safety systems
- **Technical Basis**
  - Increased use of automation in control rooms including startup, shutdowns, and operating mode changes would present new regulatory review challenges
- **Outcome**
  - Identify key areas that may become important in the future

Survey of Emerging Technologies

- **Background**
  - **Ongoing and periodic series of reports on emerging capabilities that have potential applicability for safety systems**
  - **Results have been helpful in reducing the time required to identify emerging technology that may require regulatory review in the digital area**
  - **Examples include FPGAs, wireless technologies**
- **Technical Basis**
  - **Identify key areas on R&D stage and early adoption that may become important in the future**
  - **Help develop and maintain staff capabilities to support identification and resolution of issues that develop as the nuclear industry employs state-of-the-art digital technologies**

Survey of Emerging Technologies

- **Outcome, cont**
  - **Additional reports and training modules for staff**

Collaborative and Cooperative Research

- **Background**
  - **Ongoing collaboration with other Federal agencies for research in safety assessment & security assurance of DI&C systems (e.g., NITRD program, DOD, NASA)**
  - **COMPSIS project to collect international operational experience**
  - **Halden Reactor Project**
  - **Addendum to the MOU between EPRI and RES that includes specific DI&C and Human Factors research activities such as:**
    - **Digital I&C system operational experience**
    - **Digital I&C time responses for manual actions and effects of degraded I&C on human performance**

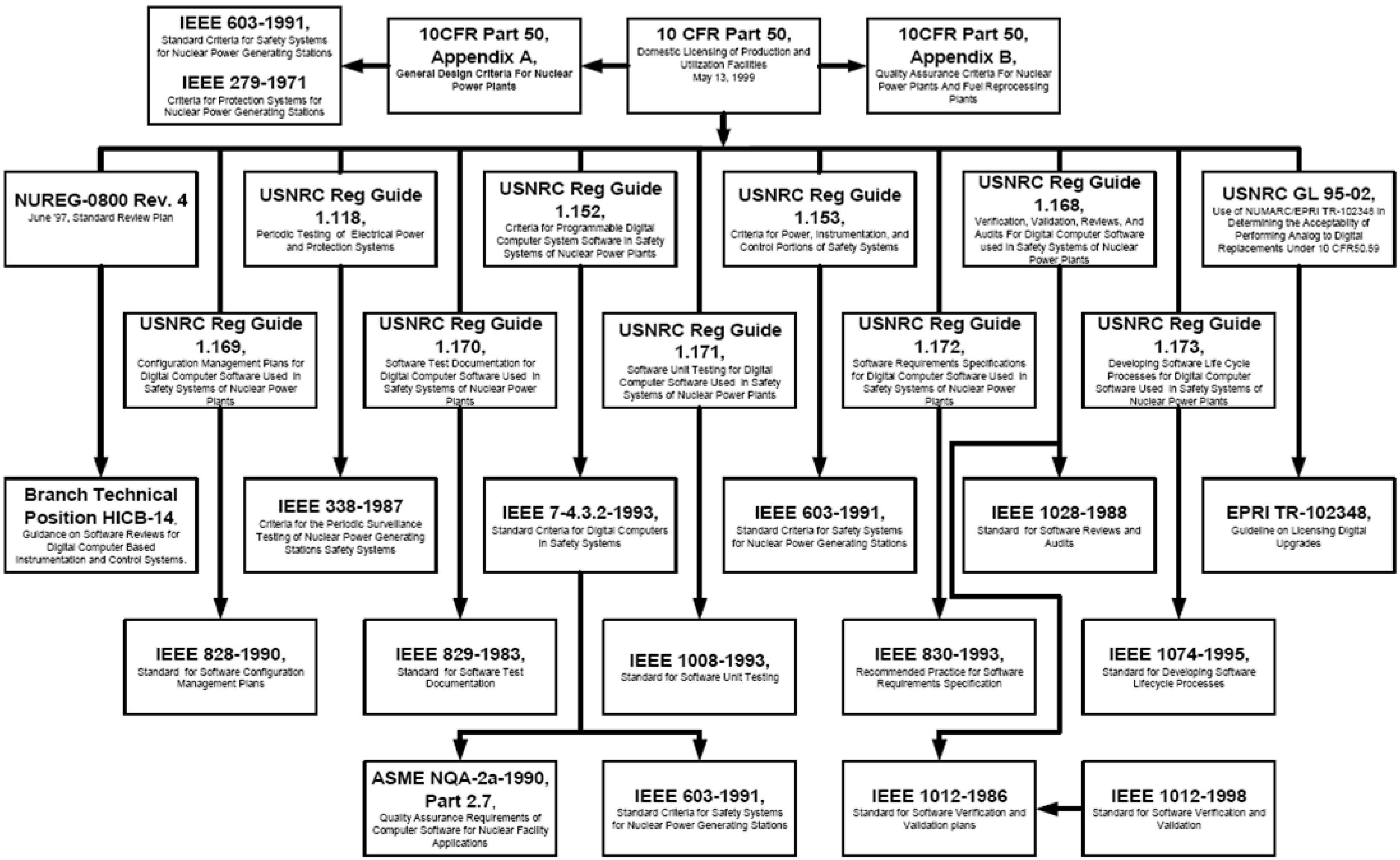
Collaborative and Cooperative Research

- **Technical Basis, cont**
  - **Need to leverage the capabilities and products of other agencies and organizations to keep up with the rapidly changing DI&C technologies and to better understand best practices and lessons learned with the deployment of digital technologies**
- **Outcome**
  - **Technical reports, workshop results, and training modules for staff**

Standards Development, Regulatory Guidance, and Review Guidance

- **Background**
  - Ongoing effort to understand, evaluate, and participate in national and international standards
- **Technical Basis**
  - Globalization of nuclear power technology and previous application of digital technologies by other industries (e.g., aviation) with their own sets of standards may provide important insights and relevant guidance that could be leveraged to complement NRC reviews
- **Outcome**
  - NUREG providing an evaluation of relevant standards and guidelines, as applicable to regulatory activities concerning safety systems. Work will leverage on-going efforts such as the MDEP program and IAEA working groups

Organization of Regulatory Guidance Knowledge



Electromagnetic Compatibility

- **Background**
  - **Carry-over of project that remained unfinished. Portions were conducted by Oak Ridge National Laboratories**
  - **Regulatory Guidance 1.180 provides guidance for the required confirmation that safety-related I&C systems are compatible with the EM environment at nuclear facilities**
- **Technical Basis**
  - **Industry claims that the high-frequency conducted susceptibility limits are overly conservative because the NPP emissions data upon which the test limits were based should not have included capture power transients (which are addressed in separate tests)**

Electromagnetic Compatibility

- **Outcome, cont**
  - Interact with EPRI via the MOU and update the guidance in Reg Guide 1.180, if necessary

Electrical Power Distribution System Interactions with Nuclear Facilities

- **Background**
  - **Need to address degraded power grid effects and power fluctuations (e.g., overvoltage spikes) on digital components**
  - **Project stems from the 2003 power blackout in the northeast**
- **Technical Basis**
  - **Increase used of power electronics and its risks are not well understood.**
  - **Dependencies on power supplies across distributed networks are not well understood**
- **Outcome**
  - **Develop models, tools, and regulatory guidance to better understand the effects of power fluctuations on digital equipment**

Operating Systems

- **Background**
  - **Evaluation criteria for operating systems likely to be used in NPPs**
  - **Will leverage existing research from other sectors**
- **Technical Basis**
  - **Increased complexity, capability, “proven in used” claims for proprietary versions complicates reviews**
  - **Added features that may not be necessary to support the safety functions**
  - **Safety impact of self-testing features**
- **Outcome**
  - **Tools and review guidance to evaluate operating systems including self-testing features**

PRIORITIES FOR CONDUCTING THE RESEARCH

- **Inputs included**
  - **Completing ongoing work**
  - **Commission Direction, Program Office inputs, ACRS recommendations**
- **Based on 3 categories for developing the research products**
  - **Support development of a new regulatory position**
  - **Improving quality, clarity, and consistency of regulatory guidance**
  - **Improving efficiency, effectiveness, and timeliness of regulatory reviews**

PRIORITIES FOR CONDUCTING THE RESEARCH, cont

- **Incorporated in the Plan as**
  - **Relative priority (high, medium and low)**
  - **Determined based on program office requests and likely application schedule**
  - **Projects scheduled based on priority and available resources**
- **Used to support RES budget process**

SCHEDULE

- The draft plan plan was made publicly available on July 29th, 2009 and is on NRC's ADAMS under accession number ML082470725
- As of August 17, 2009, the staff had not received any public comments
- Public and stakeholder commenting period until September 20th, 2009
- Plan is to go into formal NRC concurrence (office director concurrence) following incorporation and resolution of all ACRS and public comments

SCHEDULE, cont

- **The staff aims to have the research plan published by the end of calendar year 2009**
- **Working under a MOU between EPRI and RES, the parties intend to use the research plan to help identify areas for potential collaborative research**

Schedule for Research Projects

	FY10	FY11	FY12	FY13	FY14
New Start	4	2	2	1	1
Finish	2	3	2	7	6

METRICS

- RES programmatic, schedule, and budget metrics
- RES peer review process
- NRC concurrence process including surveys
- Licensing offices periodic assessments of RES
- ACRS quality reviews
- New technical metrics to measure success of RES digital I&C products
  - RES will consider establishing new metrics
  - Based on your experience are there any proven technical metrics to measure success of a project that you would recommend?

TOOLS

- **Use of NRC internal website and internal Microsoft Sharepoint environment to communicate seamlessly with internal customers**
  - **Baseline and current resource loaded schedules (updated periodically and with new information)**
  - **User needs and source requests**
  - **Research priorities and selection criteria**
  - **List and links to each research SOW and deliverables**
  - **RES points of contacts and associated contractors**
  - **Access to performance metrics**
  - **Capability mapping and common templates to improve effectiveness and efficiency of initiating and modifying work**

TOOLS, cont

- **Working to improve Research section in the NRC public website to improve visibility, organization, and timeliness of research deliverables and information**

RES - Office of Nuclear Regulatory Research - Microsoft Internet Explorer provided by USNRC

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.internal.nrc.gov/RES/about/Divisions/DE/DICB/index.html Go

Glossary | Site Index | Contact Us Public Site

Intranet Search Only RES Everything Go

U.S.NRC UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Office of Nuclear Regulatory Research

Home Organization Employee Resources Services News Information Resources Policy Security Training Travel

Aug 12, 2009

RES Home > RES Organization > Division and Branches > DE > DICB

- RES Home
- RES Organization
- Human Resources
- Projects & Programs
- IT & Web Resources
- Now in RES
- Operations & Budget
- Communications
- International
- Policy & Office Instructions

Content owner: Luis Betancourt

Digital Instrumention and Controls Branch (DICB)

Branch Chief: **Russell Sydnor**
Email: Russell Sydnor@nrc.gov
Phone: 301-251-7405

Mission Statement

The United States Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) Digital Instrumentation and Control (DI&C) Branch develops and applies methods, data, tools, standards, and guidance to assess the adequacy of DI&C systems. Our mission is to develop and implement a broad research program in the area of DI&C addressing digital system contributions to risk, software attributes that can affect safety or security, new reactor designs, and development of consensus standards. The DI&C Branch coordinates research and development activities with the program offices and external stakeholders(e.g., Universities, National Labs). It also maintains expertise in Instrumentation and Control (I&C) Engineering to support the identification and resolution of I&C issues important to nuclear power plant safety.

Plan of the Day
Plan of the Week

Related Sites

NRC Non-Publics Sites to DI&C
- NMSS / TSB
- NRR / EICB
- NRO / ICE1
- NRO / ICE2
- NSIR / ISCP
- RII / CIP

National Labs
- AMES Laboratory
- Argonne Nat'l Lab
- Brookhaven Nat'l Lab
- Fermi Nat'l Accelerator Lab
- Idaho Nat'l Laboratory
- Lawrence LivermoreNat'l Lab
- Los Alamos Nat'l Lab
- Oak Ridge Nat'l Lab
- Pacific Northwest Nat'l Lab
- Princeton Plasma Physics Lab
- Sandia Nat'l Lab

University Labs
- Ohio State University
- University of Virginia
- University of Maryland

Organizations
- ANS
- ANSI
- ASME
- IAEA
- IEC
- IEEE
- ISA
- ISO
- NEA
- NEI

Home - Digital Instrumentation and Control Branch Internal Page - Microsoft Internet Explorer provided by USNRC

File Edit View Favorites Tools Help

Back Search Favorites

Address http://portal.nrc.gov/edo/res/de/dic/default.aspx Go

NRC SharePoint Site > Office of Nuclear Regulatory Research > DE > Digital Instrumentation and Control Branch Internal Page

Welcome Santos, Daniel | My Site | My Links |

Everything Advanced Search

Digital Instrumentation and Control Branch Internal Page

US Nuclear Regulatory Commission

Digital Instrumentation and Control Branch Internal Page | Digital System Research Plan FY2010-FY2014 Communications Tools | Site Actions

View All Site Content

- Home
- Hub and Spoke Worksite
- Digital System Research Plan FY2005-FY2009
- Digital System Research Plan FY2010-FY2014
- Digital System Research Plan FY2010-FY2014 Communications Tools
- The COMPSIS Project
- DICB Toolbox
- Training
- Documents
  - References
- Digital I&C Branch Members
- Discussions
- FAQs
  - SharePoint Guidelines Documents
  - How Do I Use This Wiki Library?

Recycle Bin

Version 0.01

Version 0.01

Welcome Message

Welcome to the Digital Instrumentation and Controls Branch (DICB) Internal Web Page. This page is intended for the use of the DICB staff. It is to be used as part of the implementation of the "Hub and Spoke" Program model. It will be used to track programs and projects internally prior to updating the rest of the agency and the public. Please note that this is a tool to be used by the branch. It is not a substitute for agency accepted methods for archiving documents.

Announcements

There are currently no active announcements. To add a new announcement, click "Add new announcement" below.

Add new announcement

Links (Clicking these links will take you outside the Sharepoint Website)

- NRC Office of Nuclear Regulatory Research
- NRC DI&C Webpage (Public)
- Digital I&C Branch Page
- Digital I&C Research Programs and Activities Page

Add new link

Digital Instrumentation and Controls Branch

Branch Chief Contact Information

Russell Sydnor
301-251-7405
Russell.Sydnor@nrc.gov

SUMMARY

- **NRC Digital System Research Plan FY10 - FY14 provides a flexible, adaptable framework for supporting NRR, NRO, NMSS and NSIR regulatory bases**
  - **Broad-based program oriented toward providing more consistent processes for regulating nuclear applications**
  - **Improving review methods for new applications of existing technologies, advanced technologies and new issues**
  - **Developing regulatory acceptance criteria**

SUMMARY, cont

- **The staff requests that the ACRS endorse the plan and continue to provide inputs on how to improve the research plan**
- **RES is looking forward to working closely with the ACRS as the research is implemented**

Glossary

- **Common Cause Failure - A single event that causes failure of two or more components at the same time.**
- **Defect (software) A product anomaly. Examples include such things as omissions and imperfections found during early life cycle phases; and faults contained in software sufficiently mature for test or operation**
- **Dependability –**
  - **a) A broad concept that incorporates various characteristics of digital equipment, including reliability, safety, availability, and maintainability. (NRC RIS 2002-22)**
  - **b) The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance. (IEC 50-191)**
- **Error – A discrepancy between a calculated, observed, or measured quantity and the true or theoretically correct value or condition. (IEEE)**

Glossary, cont

- **Failure – The termination of the ability of an item to perform a required function. (IEEE)**
  - **Note: “Failure” is an event, as distinguished from “fault” which is a state. (IEC 50-191)**
- **Failure Effect - A description of the events that occur because of a specific Failure Mode**
- **Failure mode - The physical or functional manifestation of a failure. For example, a system in failure mode may be characterized by slow operation, incorrect outputs, or complete termination of execution**

Glossary, cont

- **Fault – The state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.**
  - **Note 1: Item (or entity): Any part, component, device, subsystem, functional unit, equipment, or system that can be individually considered. Am item may consist of hardware, software, or both, and may also, in particular cases, include people.**
  - **Note 2: A fault is often the result of the failure of the item itself, but may exist without prior failure (as in the case of software).**

Glossary, cont

- **Latent fault – an existing fault that has not yet been recognized (IEC 60050-191).**
- **Mistake –**
  - **a) A human action that produces an unintended result (electronic computation, IEEE).**
  - **b) A human action that produces an incorrect result (software, IEEE).**
- **Probabilistic risk analysis – A systematic method for addressing risk as it relates to the performance of a complex system to understand likely outcomes, sensitivities, areas of importance, system interactions, and areas of uncertainty.**
- **Random hardware failure – A failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware. (IEC 61508-4, section 3.6.5)**
- **Reliability – The ability of an item to perform a required function under stated conditions for a specified period of time. (IEEE)**
- **Risk – Combination of the probability of occurrence of loss and the severity of that loss [ISO/IEC Guide 51:1990]**

Glossary, cont

- **Risk analysis – A procedure to develop probability estimates of occurrence of each specific hazard. (IEEE)**
- **Risk assessment – The overall process of identifying all the hazards in a system (internal and external), estimating the risk from each hazard and the overall risk resulting from their combination. See also: Risk estimation.**
- **Risk estimation – The process of assigning values to the severity of loss and the probability or likelihood of its occurrence. See also: Risk assessment.**
- **Risk-Informed – An approach to decision-making in which risk insights are considered along with other factors such as engineering judgment, safety limits, and redundant and/or diverse safety systems. Such an approach is used to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety. (NUREG 1614)**

Glossary, cont

- **Safety – Adequate protection of public health and safety and the environment. (NUREG 1614 p. 4)**
  - **Note 1: Adequacy is determined with respect to the safety goals for a NPP defined in the Commission policy statement [17] in terms of a broadly defined acceptable level of radiological risk. This policy statement enables a mapping of the NRC definition of safety to that in ISO/IEC Guide 51:1999 and IEC 61508-4, viz. "freedom from unacceptable level of risk."**
  - **Note 2 relevant to DI&C PRA: The NRC policy statement defines "acceptable level of risk" in terms of individual risk and societal risk (life and health) goals and quantitative targets. Guidelines relevant to NPP PRA map the policy level health goal into performance objectives such as "core damage frequency" from which the performance objective ("risk budget"; "risk responsibility") can be derived and allocated for a reactor safety DI&C system.**

Glossary, cont

- **Safety-related – In the regulatory arena, this term applies to systems, structures, components, procedures, and controls of a facility or process that are relied upon to remain functional during and following design-basis events. Their functionality ensures that the key regulatory criteria, such as levels of radioactivity released, are met. Examples of safety related functions include shutting down a nuclear reactor and maintaining it in a safe shutdown condition.**
- **Systematic failure – A failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design of the manufacturing process, operational procedures, documentation or other relevant factors. (Adapted from IEC 61508-4, Section 3.6.6)**
- **Systemic cause – A cause related in a deterministic way to an effect or result.**
  - **Note: Related term & definition: Failure cause: The circumstances during engineering, manufacturing, installation, configuration, usage, or maintenance leading to a failure deterministically. (Adapted from IEC 60050-191)**

Acronyms

- ACRS – Advisory Committee on Reactor Safeguards
- DI&C – Digital Instrumentation and Controls
- DOD – Department of Defense
- EM- Electromagnetic
- EM/RF – Electromagnetic/Radio Frequency
- EMP – Electromagnetic Pulse
- EPRI – Electric Power Research Institute
- FPGA – Field Programmable Gate Array
- FY – Fiscal Year
- HF- Human Factors
- HTGR – High Temperature Gas Reactor
- I&C – Instrumentation and Controls
- IAEA – International Atomic Energy Agency

Acronyms, cont

- **ISG – Interim Staff Guidance**
- **MDEP - Multinational Design Evaluation Programme**
- **MOU – Memorandum of Understanding**
- **NAS – National Academy of Science**
- **NASA - National Aeronautics and Space Administration**
- **NITRD - Networking and Information Technology Research and Development**
- **NMSS – Office of Nuclear Material Safety and Safeguards**
- **NPP – Nuclear Power Plant**
- **NRC- Nuclear Regulatory Commission**
- **NRO – Office of New Reactors**
- **NRR- Office of Reactor Regulation**

Acronyms, cont

- **NSIR – Office of Nuclear Security and Incident Response**
- **OpE – Operational Experience**
- **PRA - Probabilistic risk assessment**
- **R&D – Research and Development**
- **RIL- Research Information Letter**
- **RIS - Regulatory issue summary**
- **SOW – Scope of Work**
- **SRP – Standard Review Plan**
- **TWG – Task Working Groups**
- **UVA - University of Virginia**
- **V&V - Verification and validation**

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital I&C PRA

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee
August 20, 2009

Alan Kuritzky
Division of Risk Analysis
Office of Nuclear Regulatory Research
(301-251-7587, Alan.Kuritzky@nrc.gov)

Outline of Presentation

- Background
- Objective
- Previous research
- OECD/NEA/CSNI/WGRisk technical meeting
- Software reliability quantification
- Milestones and future interactions

Background

- Current licensing process for digital systems is based on deterministic engineering criteria
- Commission's 1995 probabilistic risk assessment (PRA) policy statement encourages use of PRA to the extent supported by the state-of-the-art
- Risk-informed analysis process for digital systems has not yet been satisfactorily developed

Objective

- Identify and develop methods, analytical tools, and regulatory guidance to support:
  - Nuclear power plant (NPP) licensing decisions using information on the risks of digital systems
  - Incorporation of digital system models into NPP PRAs

Previous Research

- Previous RES projects (2004-2009) have:
  - Identified a set of desirable characteristics for reliability models of digital systems
  - Applied various probabilistic reliability modeling methods (traditional and dynamic) to an example digital system
- This research is documented in a series of NUREG/CR reports
  - Traditional reliability modeling methods (NUREG/CR-6962 [2008], draft NUREG/CR-6997 [2008])
    - Brookhaven National Laboratory (BNL)
  - Dynamic reliability modeling methods (NUREG/CR-6901 [2006], NUREG/CR-6942 [2007], NUREG/CR-6985 [2009])
    - Ohio State University, ASCA, University of Virginia

NUREG/CR-6997 (1 of 3)

Key Findings

- The level of detail of the digital feedwater control system (DFWCS) model is adequate for capturing many of the system design features, while not being too complicated to be developed and solved.
- However, at this level of detail, the study requires a deterministic simulation tool (model) to determine the component-level sequences resulting in system failure.
- The use of the simulation model to determine component-level failure sequences reduces the event tree/fault tree and Markov models solely to means for quantifying system reliability.
- Performing a failure modes and effects analysis and running the simulation tool revealed two failure scenarios (one involving differences in signal delay times, and the other involving both CPUs operating in tracking mode) that were not identified by the plant hazards analysis.

NUREG/CR-6997 (2 of 3)

Key Findings (Continued)

- The order in which component failure modes occur can affect the impact the failures have on the system.
- The Markov method can easily account for the order in which component failure modes occur, and was used for quantification.
- Due to modeling limitations (including lack of a model for incorporating software failure), as well as the weakness of publicly available digital component failure data, the current model and results cannot be used to support decision making.
- The approach applied in this study to the DFWCS should also be applicable to protection systems.

NUREG/CR-6997 (3 of 3)

Areas of Potential Additional Research

- Improved approaches for defining and identifying failure modes of digital systems
- Software reliability methods for quantifying software failure rates and probabilities, and addressing software common cause failure (CCF)
- Better data for hardware failures (both independent and common cause) and a break down of the failure rates by failure modes of digital components
- Methods and parameter data for modeling self-diagnostics, reconfiguration, and surveillance, including using other components to detect failures
- Methods for human reliability analysis (HRA) associated with digital systems
- Determining if and when a dynamic model of controlled plant processes is necessary in developing a reliability model of a digital system

OECD/NEA/CSNI/WGRisk Technical Meeting on Digital System Reliability

- NRC (with support from BNL) led an Organisation for Economic Co-operation and Development (OECD)/Nuclear Energy Agency (NEA)/Committee on the Safety of Nuclear Installations (CSNI)/Working Group on Risk Assessment (WGRisk) activity on digital system reliability.
- Objectives: Make recommendations regarding current methods and information sources used for quantitative evaluation of digital system reliability for PRA applications and identify, where appropriate, the near and long term developments that would be needed in order to improve reliability assessments
- Technical meeting with participants from over 20 organizations and 11 countries held in Paris during October 21-24, 2008
- Summary report of technical meeting prepared by BNL and recently approved for publication by CSNI

WGRisk Meeting Results

- Useful forum for sharing and discussing respective experiences
- Spectrum of opinions on methods for modeling digital systems
- Wide variation in terms of scope and level of detail for existing models of digital systems
- General agreement on need to account for software failures
- General agreement on need to address scarcity of probabilistic data
- General agreement on need to continue research to address technical challenges

Recommendations (1 of 2)

- Method development
  - Develop a taxonomy of digital component failure modes for common use
  - Develop methods for quantifying software reliability, capturing benefits of fault tolerant features, and addressing human-system interfaces unique to digital systems
  - Evaluate the need and approaches for addressing dynamic interactions
- Data collection and analysis
  - Collect hardware failure data, including CCF data, that can be used for PRA purposes
  - Use operating experience for identifying software failure modes to be included in reliability models

Recommendations (2 of 2)

- International cooperation
  - Share approaches, methods, probabilistic data, results, and insights gained from relevant projects among NEA members
  - Jointly develop methods on software modeling (including CCF), quantification of software reliability, assessing the effect of failures of components of a digital system on the system, reliability modeling of a digital system, and HRA
  - Perform benchmark studies of the same systems to share and compare methods, data, results, and insights
  - Publish technical documents, such as “CSNI Technical Opinion Papers”

Software Reliability Quantification (1 of 2)

- In 1997, a National Research Council committee completed a study requested by the NRC on application of digital instrumentation and control (I&C) technology to commercial nuclear power plant operations. It concluded that:
  1) "*Explicitly including software failures in a PRA for a nuclear power plant is preferable to the alternative of ignoring software failures*"
  2) "*As in other PRA computations, bounded estimates for software failure probabilities can be obtained by processes that include valid random testing and expert judgment*."[1]
- In April 2008, the ACRS Subcommittee on Digital I&C Systems recommended:
  1) "*The staff should explore the fundamental philosophical aspects of software failures and their use in developing a probabilistic model of a digital system.*"
  2) "*The staff should consider the relevant aspects of developing and evaluating a reliability model of a digital system that integrates hardware and software failures...*"

[1]Committee member Nancy Leveson did not concur with this conclusion.

Software Reliability Quantification (2 of 2)

- NRC/BNL organized and convened a workshop involving experts with knowledge of software reliability and/or NPP PRA in May 2009.
- Workshop objectives:
  - Obtain a consensus, or at least agreement among the majority of workshop participants, on the “philosophical basis” for incorporating software failures into digital system reliability models for use in PRAs.
  - Discuss issues associated with methods for modeling software in a reliability model and quantifying software failure rates and probabilities.

Panel of Experts

- Mr. Steven A. Arndt, NRC
- Mr. Bob Enzinna, AREVA
- Dr. Hyun Gook Kang, Korea Atomic Energy Research Institute
- Prof. Michael R. Lyu, Chinese University of Hong Kong
- Prof. Bev Littlewood*, City University, London
- Dr. Allen P. Nikora, Jet Propulsion Laboratory, California Institute of Technology
- Prof. Martin L. Shooman, Polytechnic Institute of New York University
- Prof. Nozer D. Singpurwalla, George Washington University
- Prof. Kishor S. Trivedi, Duke University

*Prof. Littlewood was unable to attend the meeting, but did provide responses to the questionnaire.

A Philosophical Basis for Modeling Software Failures Probabilistically

- Software failure is basically a deterministic process. However, because of our incomplete knowledge, (e.g., the number and nature of residual faults, and occurrence and timing of fault-triggering inputs) we are not able to fully account for and quantify all the variables that define the failure process. Therefore, we use probabilistic modeling to describe and characterize the software failure process.

- The above basis is essentially the same basis for many other probabilistic processes, e.g., tossing a coin. In the case of a coin toss, if one can control all aspects of the toss and repeat it each time, the result will always be the same. However, due to our inability to precisely repeat all aspects of the toss, the outcome is uncertain and can be modeled as a random variable.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Current and Near-Term Activities

- Due to resource limitations and competing priorities, not currently pursuing hardware models of an example protection system or integration of digital system models into an NPP PRA
- Instead, NRC/BNL currently pursuing software reliability quantification
  - Workshop on philosophical basis (completed)
    - BNL preparing letter report
  - Reviewing quantitative software reliability methods (QSRMs)
    - Building upon BNL's earlier reviews of software reliability methods
    - Including more recently completed studies
  - Plan to develop one or two technically sound approaches to modeling and quantifying software failures in terms of failure rates and probabilities
  - Assuming such approaches can be developed, plan to apply them to an example software-based protection system in a proof-of-concept study
- Bottom line: It is expected that detailed reliability models of digital systems (including software) can be developed and quantified; the lingering question is whether it is practical and useful to do so.

Milestones and Future Interactions

- Publish NUREG/CR-6997 (Sep/Oct 2009)
- Issue final letter report on software PRA workshop (Oct 2009)
- Issue draft letter report on review of QSRMs for peer review (Jan 2010)
- Issue final letter report on review of QSRMs (Jun 2010)
- Brief ACRS Digital I&C Subcommittee (~Feb 2010?)
  – Final letter report on software PRA workshop
  – Draft letter report on review of QSRMs
  – Project plans for developing candidate QSRMs

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Back-Up Viewgraphs

United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary of Dynamic Methodologies

- Two dynamic methodologies, Markov/Cell-to-cell-mapping technique (CCMT) and Dynamic Flowgraph Methodology (DFM), were applied to the benchmark digital feedwater control system
- These dynamic methodologies have ability to include timing and order of component failures by using multi-valued logic representation of system components and states
- Results are generated to demonstrate incorporation into a traditional PRA framework
- Ability to account for dynamic process interaction
  - may not be necessary for all digital I&C systems (i.e., protection systems)
  - requires interfacing with process simulator (i.e., steam generator simulator)
- Documented in NUREG/CR-6985 (February 2009)

NUREG/CR-6985 (1 of 2)

<u>Assumptions</u>

- Plant assumed to have 2 identical steam generators - one of which is analyzed. Physical behavior of this steam generator is assumed to be well represented by a simulator developed to support this research.
- Benchmark model based on assumed set of failure modes from supporting analyses (FMEA)
- Assume the model's required failure rates can be obtained using fault coverage estimates

<u>Limitations</u>

- Software design errors, common cause failures, and communications are not modeled
- Application methodologies raised concerned about the computational practicality and usability
  – Markov/CCMT model construction requires high level of user skill and has computational limitations due to the large number of possible system states and transitions which must be reduced by the user
  – DFM has a more developed software implementation tool

NUREG/CR-6985 (2 of 2)

Key Findings

- Results are demonstrative in nature and cannot be used for decision making
- Dynamic interaction between the process and the control system may be important for certain systems (e.g., feedwater control system)
- The application to the Benchmark raises some serious doubts about the usability and computational practicality of the dynamic methods, especially Markov/CCMT
- Work relies greatly on the use of coverage to estimate component failure rates - this topic warrants further discussion and evaluation
- Further investigation on data acceptability and failure modes is being conducted