Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards Digital Instrumentation and Control Systems Subcommittee
Docket Number:	(not applicable)
Location:	Rockville, Maryland
Date:	Thursday, October 20, 2005
Work Order No.:	NRC-663 Pages 1-191

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE MEETING

+ + + + +

THURSDAY, OCTOBER 20, 2005

+ + + + +

OPEN SESSION

+ + + + +

The Committee met in Room T2 B3 of the Nuclear Regulatory Commission headquarters, Two White Flint North, Rockville, MD, at 1:30 p.m., George Apostolakis, Chair, presiding.

PRESENT:

GEORGE E. APOSTOLAKIS ACRS Member
MARIO V. BONACA ACRS Member
THOMAS S. KRESS ACRS Member
JOHN D. SIEBER ACRS Member
SERGIO B. GUARRO ACRS Consultant
ERIC A. THORNSBURY ACRS Staff

STAFF PRESENT:

CHRISTINA ANTONESCU	RES/DET/ERAB
STEVEN ARNDT	RES/DET/ERAB
FRED BURROWS	NMSS/FCSS/TSG
MATT CHIRAMAL	NRR/DE/EEIB
CLIFF DOVTT	NRR/DSSA/SPSB
MICHELE EVANS	RES/DET/ERAB
HOSSEN HAMZEHEE	RES/DRAA
ALLEN HOWE	NRR/DE/EEIB
WILLIAM E. KEMPER	RES/DET/ERAB/IVC
T. KOSHY	EEIB/NRR
ERIC LEE	NSIR/DNS/RSS
PAUL LOESER	RES/DET/ERAB
SCOTT MORRIS	NSIR/DNS/RSS
PAUL REBSTOCK	NRC/NRR/DE/EEIB-I&C
ROMAN SHAFFER	RES/DET/ERAB
GEORGE TARTAL	RES/DET/ERAB
MICHAEL WATERMAN	RES/DET/ERAB

ALSO PRESENT:

DAVID BLANCHARD	AREI
ROBERT CONTRATTO	Consultant
PAUL EWING	ORNL
TONY HARRIS	NEI
WES ITINES	Univ. TN
ROGER KISHER	ORNL

ALSO PRESENT: (CONT.)

KOFI KORSAH	ORNL
GLENN LANG	Consultant
JERRY MAUCK	FANP
PETE MORRIS	Westinghouse
BRUCE MROWOS	ISC
THUY NGUYEN	EPRI
DAVID SHARP	Westinghouse/Consultant
NORMAN STRINGFELLOW	Southern Nuclear
RAY TOROK	EPRI
RICHARD WOOD	ORNL

A-G-E-N-D-A

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

1:34 p.m.

CHAIRMAN APOSTOLAKIS: The meeting of the Advisory Committee on Reactor Safeguard Subcommittee on Digital Instrumentation and Control System.

I'm George Apostolakis, Chairman of the Subcommittee.

Members in attendance are Mario Bonaca, Jack Sieber and Tom Kress. Also in attendance is one of consultants Dr. Sergio Guarro.

The purpose of this meeting is to discuss three sections of the NRC Staff's draft digital systems research plan and to hear a presentation from EPRI on their guidance for performing defense-in-depth and diversity assessments for digital upgrades.

During this portion of the meeting we will hear from EPRI regarding their guidance document and from the NRC staff regarding Section 3.1 of the Digital Systems Research Plan, the system aspects of digital technology.

The Subcommittee will gather information, analyze relevant issues and facts and formulate proposed positions and actions as appropriate for deliberation by the full Committee. Eric Thornsbury is the designated federal official for this meeting.

The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in the *Federal Register* on September 29, 2005.

A transcript of the meeting is being kept and will be made available as stated in the *Federal Register* notice.

It is requested that speakers first identify themselves and speak with sufficient clarity and volume so that they can be readily heard.

We have received no written comments or requests for time to make oral statements from members of the public regarding today's meeting. We now proceed with the meeting and I call upon Mr. A. Torok of EPRI to begin the presentation.

MR. TOROK: I'm Ray Torok from EPRI. And has already been said, we're here to talk about an EPRI project that we call Defense-in Depth and Diversity Assessments to Digital Upgrades. I guess i can skip ahead.

And what I'd like to do before going anywhere is introduce the Chairman of our Industry Working Group who has guided this effort to talk about the first few slides.

We're going to do sort of a tag team

presentation. Our intent is to do a tag team presentation to go through various areas of it, and we were going to lead off with our Utility Chairman of our Industry Working Group, that's Jack Stringfellow from Southern Nuclear.

Jack, please.

CHAIRMAN APOSTOLAKIS: It's better to sit there.

You don't have to leave. Stay there. There are two chairs, aren't there?

MR. TOROK: Okay. I got your back, Jack.

MR. STRINGFELLOW: All right, Ray. Thank you very much.

As Ray said, I'm Jack Stringfellow. I'm an employee of Southern Nuclear Operating Company. It's licensing manager for the Vogtle Electric Generating Plant. I'm also the Chairman of this EPRI working group that's been tasked to apply risk insights to the process of performing a diversity and defense-in-depth analysis for digital upgrades for nuclear power plants.

And the first thing I want to say is express our appreciation for the opportunity to make this presentation. Thank you very much. We feel very strongly about this program and we feel like we have something that is worth considering and can certainly enhance the process of performing a decubed analysis.

We want to talk for just a few moments in our presentation, to being with, just to provide a little background for the project, why we thought this was a good thing to do, the impetus for this effort. And how it relates to the current regulatory guidance and make some key propositions with respect to how we would envision moving forward with this effort. We're going to give you a high level view of the guideline approach. And then we want to spend most of our time discussing the technical issues; the digital common cause failure. We want to talk about susceptibility to common cause failure. We want to talk bout defensive measures. We want to address the issue of estimating the probability of failure as well. And we want to talk about what our risk insights have been as a result of making this effort; what we found with respect to the impact of diversity on safety and risk and also conclusions that we've been able to come to with respect to modeling digital equipment and PRA.

Then we'd like to offer some recommendations for the ongoing activities of Research and NRR, if we may be so bold as to do that.

You've already heard from Ray Torok. Oh, thank you, Ray.

MR. TOROK: I'm here to help.

MR. STRINGFELLOW: Thank you. What do you do just hit the button to advance that?

MR. TOROK: Yes.

MR. STRINGFELLOW: Or the space bar?

CHAIRMAN APOSTOLAKIS: This is advanced technology. Advanced digital.

MR. STRINGFELLOW: I just want to make sure I don't screw up. Thank you.

CHAIRMAN APOSTOLAKIS: We have a project involving human error also.

MEMBER SIEBER: You hit the wrong button you trip the reactor.

MR. STRINGFELLOW: There you go. There you go. So that tells me to keep my hands off, huh? All right.

Our other presented will be Thuy Nguyen, who is on loan to EPRI. And also Dave Blanchard, Applied Reliability.

Our group represents ten utilities. We have design experience, PRA experience and licensing experience on the group. We also represent four equipment suppliers as well as consultants and integrators in NEI and EPRI. So we're a diverse group and I think we've been able to bring a great deal of varied experience to this effort.

We started our work back in early 2002. And we have invited the NRC Staff to attend working group meetings, and they have both in 2002, 2003 and 2004 in an effort to keep the NRC apprised of what we were doing and the direction that we're headed in.

CHAIRMAN APOSTOLAKIS: But they were not allowed to speak?

MR. STRINGFELLOW: Well, they were there on their term. What am I trying to say?

MR. TOROK: Yes. I guess they weren't there--

CHAIRMAN APOSTOLAKIS: Speak to the microphone, please.

MR. TOROK: I'm sorry. They could probably explain it better than I. My understanding --

CHAIRMAN APOSTOLAKIS: No, you explain.

MR. TOROK: My understanding was, yes, they were not I guess free to offer NRC positions, although to offer their opinions was fine. And because they were EPRI working group meetings and not noticed NRC meetings.

CHAIRMAN APOSTOLAKIS: So basically they were observers?

MR. STRINGFELLOW: That's correct, they were observers.

MR. TOROK: That's right.

MR. STRINGFELLOW: That's correct.

CHAIRMAN APOSTOLAKIS: Okay.

MR. STRINGFELLOW: But we wanted them to be able to be aware of what we were trying to do.

CHAIRMAN APOSTOLAKIS: Absolutely.

MR. STRINGFELLOW: Okay. We published a final product in December of 2004, and that was submitted to the NRC on February 22 of 2005 asking for -- yes, I got my own copy, too.

And then we met with the Staff on April of 2005 to discuss status of the review and also to get first impressions from the Staff with respect to the document.

This last bullet says we are still awaiting an NRC letter on a path forward. We did receive some comments. Tony Pietrangelo received some comments from Herb Berkow on October 18th. Due to these late breaking comments, we haven't had a chance to sit down and look at them in detail. So we're really not prepared to talk about these comments line-by-line today, but we appreciate the comments. And we hope to use them as a basis for constructive dialogue and moving forward with the review of this document. So thank you very much.

CHAIRMAN APOSTOLAKIS: What is it that you want the NRC to do?

MR. STRINGFELLOW: Well, what we envisioned is we have a similar document, our guidelines for licensing digital upgrades that we went back -- when was it first published, Ray?

MR. TOROK: This goes back to 1993, actually the first version of this.

MR. STRINGFELLOW: Yes.

MR. TOROK: And what we wanted to do was establish a rough framework, basically, for licensing digital upgrades that established a common understanding between the Staff and the utilities. Then that was revised more recently in a revision that was published just a few years ago. We hope to do the same --

MR. STRINGFELLOW: Excuse me, Ray, for interrupting. But it was revised to update it to reflect the rule change on 10 CFR 50.59.

MR. TOROK: Exactly.

MR. STRINGFELLOW: Okay. So we set about to revise it for that purpose. And we submitted that to the Staff for review, and it was subsequently endorsed by regulatory information summary, a RIS. And we would hope to be able to accomplish the same thing with this guideline.

CHAIRMAN APOSTOLAKIS: Do you usually incorporate documents like this one in a regulatory guide?

MR. KEMPER: You mean EPRI's?

CHAIRMAN APOSTOLAKIS: Yes. Let's say that you want to approve it?

MR. KEMPER: Exactly. Right. We would --

CHAIRMAN APOSTOLAKIS: You don't just say we approve. I mean there is a regulatory guide --

MR. KEMPER: Well, there's a couple of paths we could take. One is a safety evaluation report could be written. That's been done in many cases in the past.

CHAIRMAN APOSTOLAKIS: Sure.

MR. KEMPER: Or we could possibly endorse this as a regulatory guide on this topic.

CHAIRMAN APOSTOLAKIS: Okay. But it has to be a regulatory guide at the end?

MR. KEMPER: Well, no. Actually an SER works sufficiently as well. Licensees can refer to that.

CHAIRMAN APOSTOLAKIS: I thought you could just say the SER, this is good enough and --

MR. KEMPER: Right. Correct.

MR. TOROK: And may I add to that? There was a similar guideline we produced on evaluation of commercial grade digital equipment for use in safety related applications. And in that case NRC reviewed and approved it and actually referenced it in the standard review plan.

CHAIRMAN APOSTOLAKIS: Correct. Right.

MR. TOROK: So if you look at the standard review plan now it refers you to the EPRI document.

CHAIRMAN APOSTOLAKIS: Bill, regardless of whether you go the SER route or regulatory guide, will you come to us before you issue whatever decision you are --

MR. KEMPER: Oh, absolutely, yes. Well, we have--

CHAIRMAN APOSTOLAKIS: -- SER and go more deeply into the document itself.

MR. KEMPER: Well, as you know, we have a risk program ourself, right, which we presented back in June to this Committee. So we're kind of trying to accomplish the same thing in parallel here, if you will; the agency as EPRI is. So at some point I expect that we're going to probably converge, that's just Bill Kemper's idea or estimation of the work. So hopefully the two programs will come together and we will end up with one way to deal with a risk-informed diversity and defense-in-depth process for licensing digital.

CHAIRMAN APOSTOLAKIS: So you don't see the Agency approving this before your particular project is done?

MR. KEMPER: I can't speak directly for NRR. But my thinking at this time is I would lobby hard that we work together so that we come up with one consistent approach on this.

CHAIRMAN APOSTOLAKIS: What are the plans?

MR. HOWE: Good afternoon. This is Allen Howe. I'm with NRR.

And just to try to clarify this. If this report is submitted to the NRC for review as a topical report, we would treat it under our topical report process. We would review it, we would write a safety evaluation. Part of that process would be that the applicant for the topical report would then supplement their topical report with the safety evaluation to designate that this has been reviewed and approved by the NRC. Then licensees that came in with applications could reference that topical report as a part of their application. So that's the topical report process.

CHAIRMAN APOSTOLAKIS: And this is what's happening now?

MR. HOWE: No. We have not accepted this as a topical report for review?

CHAIRMAN APOSTOLAKIS: But EPRI is requesting that you do that, is that what it is?

MR. HOWE: Yes.

CHAIRMAN APOSTOLAKIS: Okay. And you have issued the SER or --

MR. HOWE: No. We have not issued an SER. We have not even commenced a review on it. We have been given a draft copy of the topical report. As was indicated in one of the bullets, we provided some comments back but the report has not been submitted formally as a topical report.

CHAIRMAN APOSTOLAKIS: Okay. Thank you.

Oh, one last question. Can you explain a little bit what you mean by expends NRC approach.

MR. TOROK: We'll get into that?

CHAIRMAN APOSTOLAKIS: What does that mean? Oh, you will get into that?

MR. TOROK: Oh, yes.

MR. STRINGFELLOW: Yes. We're going to

expand on that in the later slides here very shortly. Very shortly.

CHAIRMAN APOSTOLAKIS: Okay.

MR. STRINGFELLOW: Okay. I guess there's one thing, Ray, I would like to follow up on the comment by Mr. Howe that we had not formally submitted this for review. Because I believe we have.

CHAIRMAN APOSTOLAKIS: See, that's the advantage of coming to the Advisory Committee to find out.

MEMBER SIEBER: It's in the mail.

MR. HOWE: This is Allen Howe again.

Not to belabor the point, but we indicated in a letter to you in March that we were considering the subject topical report as a draft. And we had a presubmittal meeting with you and we were waiting for the formal submittal of your topical report.

MR. STRINGFELLOW: Did we identity this as a draft. Okay.

CHAIRMAN APOSTOLAKIS: It may be a formality anyway.

MR. STRINGFELLOW: Okay. All right. Fine.

CHAIRMAN APOSTOLAKIS: But ultimately, Mr. Howe, you will come to this Committee after you have your SER?

MR. HOWE: I'm sorry, I didn't hear the question.

CHAIRMAN APOSTOLAKIS: After they submit it formally, you issue an SER. And do you expect to come before us for a letter?

MR. HOWE: We evaluate that on a case-by-case basis. But I understand that your interest is in hearing from the staff before we go forward with this.

CHAIRMAN APOSTOLAKIS: Yes. This is an area where there is great interest on the part of the Committee. I would appreciate it.

MR. HOWE: Okay.

CHAIRMAN APOSTOLAKIS: Okay.

MR. STRINGFELLOW: Okay. I want to spend just a minute talking about regulatory environment and why we think that this report can help. I think the industry and the NRC have been struggling somewhat with respect to digital upgrades. For example, upgrades that involve rapid protection system and engineered safety features actuation system.

We feel that it's been our experience that the current guidance in the form of branch technical position HICB-19 and NUREG/CR-6303 can be difficult to implement. It is void of risk insights, certainly --

CHAIRMAN APOSTOLAKIS: Difficult to

implement means it's vague or what? Why is it difficult?

MR. STRINGFELLOW: Well, you know, one of the examples there is with respect to large break LOCA, for example. If you are postulating a digital common cause failure and then trying to address the large break LOCA in light of a digital common cause failure given the guidance and the acceptance criteria that are in HICB-19, it's difficult to address that event, for example, without designing and adding onto the system some sort of diverse actuation system for example. And I guess we're going to get into that later on and in a little more detail, I think. But I think that would be an example.

Ray, can you --

MR. TOROK: Well, yes. Well, there's some other things that requires revisiting FSAR analyses, using different types of assumptions, best estimate analysis that most utilities aren't used to because they haven't done it that way before. And, in fact, it appears that those analyses have very limited value as well.

So, we'll get into some of these other things in a few minutes. So you'll see --

MR. STRINGFELLOW: And that's where we

came - I'm sorry I'm stepping on you, Ray. I apologize.

MR. TOROK: No, no problem. We'll add a lot of detail to that later I think.

MR. STRINGFELLOW: Right. You know, some of the insights that we found is that revisiting many of these Chapter 15 analyses provides a safety benefit from a risk perspective. And so the deterministic focus of the branch technical position I think is where at least part of the difficulty arises in the implementation.

And then we found that some things that had been previously accepted in the past by the Staff are now being questioned.

CHAIRMAN APOSTOLAKIS: Are you going to come to this, too?

MR. TOROK: Some of that.

MR. STRINGFELLOW: Yes. We're going to come to it.

MR. TOROK: Some of it, yes. And the idea here really of what Jack's talking about now is to make the point that there's a lot of problems with the current process for doing this and we think there are ways to improve them. And we think we should be doing that.

MR. STRINGFELLOW: Yes. And don't take this I'm not trying to throw rocks. I'm not trying to throw rocks with this slide. What I'm trying to say is we understand that the review of this systems is evolving. And what we're trying to do with this product is help that and help provide some stability and provide those risk insights.

CHAIRMAN APOSTOLAKIS: Well, just that bullet doesn't really read very well, "NRC Staff not honoring SERs." Is it because the Staff is capricious?

MR. TOROK: There's a specific example of one review that's in progress now where the utility's using a platform, a digital platform that had already been reviewed and approved by NRC in the form of an SER. And now the utility is receiving additional questions on that. And, in fact, the Staff has taken the position, as I understand it, that they may have to go back and reopen that evaluation and start over again. And, of course, that from the utility standpoint, that has a tremendous impact on their schedule for what they're planning to do. So for them the process isn't working very well right now. So that's the example there.

CHAIRMAN APOSTOLAKIS: There probably was a reason for it.

MR. TOROK: Yes. But, at any rate, the problem from the utility perspective is it makes the process unpredictable. And, of course, it makes it difficult to them to estimate cost and schedule and whatnot. So it puts them in a real rough position.

CHAIRMAN APOSTOLAKIS: Yes. And if it's an issue of adequate protection, it makes the process difficult from the Staff point of view?

MR. TOROK: That's right.

CHAIRMAN APOSTOLAKIS: Okay.

MR. STRINGFELLOW: And then finally, one of the comments we got in our meeting in April on our report that Research is doing some work with respect to modeling digital systems in PRA and working on the question of the failure probability of digital systems. But, unfortunately, the timing of that research doesn't support the near term submittals. And so, again, that's another impetus for our work here.

Many utilities are in the process of planning and trying to make digital upgrades today. Many of us are operating our fleet on analog systems that were designed and built many, many years ago. Operating reliably and safely, I may add, but nevertheless these systems are aging. And when we look for replacements they are digital in nature. All the way from things as simple as temperature controllers on chilled water systems all the way up to feedwater control systems and protection systems; the replacements are digital in nature. And so we are having to deal with these digital upgrades on a day-to-day basis. And planning an across the board protection system upgrade that takes a great deal of resources and scheduling. So anything that we can do to help move that process along we feel like in everybody's best interests from both a reliability standpoint and a safety standpoint.

The issue of software common mode failure is still unsettled. You know, we recognize certainly the need to ensure adequate coping capability or diversity, but as I mentioned that the regulatory issues and our experience has been protracted reviews.

As I mentioned before, we've found the current NRC guidance to be problematic. I've already mentioned that it can require backups that add complexity and costs without necessarily improving safety. It may not fully address events that are risk significant, could actually discourage plant upgrades that would enhance safety.

CHAIRMAN APOSTOLAKIS: Do you have an

example of an event that may be risk significant in a current review process?

MR. TOROK: Yes. We'll get to that in a little.

I'm sorry.

MR. STRINGFELLOW: That's all. These are the background slides. We're trying to set the stage for this presentation.

CHAIRMAN APOSTOLAKIS: Yes. You are doing that very well.

MR. TOROK: Work with us here.

CHAIRMAN APOSTOLAKIS: You've made a few provocative statements that keeps us awake.

MR. STRINGFELLOW: We don't want you to go asleep, okay?

CHAIRMAN APOSTOLAKIS: You are succeeding.

MR. STRINGFELLOW: Okay. All right. And I've already mentioned that it can require analysis of events that aren't safety significant from a risk perspective.

Ray?

MR. TOROK: Yes. And we have examples of those.

MR. STRINGFELLOW: We have examples of those, too.

CHAIRMAN APOSTOLAKIS: This is pretty serious stuff there.

MR. TOROK: It's my turn, huh?

MR. STRINGFELLOW: It's your turn, Ray? You want to sit here?

CHAIRMAN APOSTOLAKIS: Okay.

MR. TOROK: Okay. So we wanted to briefly explain the current regulatory guidance that's out there right now. Jack already mentioned BTP-19 which is tied Chapter 7 of NUREG-0800, the standard review plan. And that document references NUREG/CR-6303, which is a contractor report developed by Lawrence Livermore some years ago.

The vintage on these things, I believe BTP-19 came out officially in 1994, but really the work behind it dates back to the late '80s and early '90s when it was put together primarily, I believe, for the advanced reactor program to address diversity and defense-in-depth there.

What it involves here is the idea is to demonstrate that you have adequate coping capability in the event of a common cause failure. I believe they refer to it as software common mode failure. We're quibbling over words here. We call it now digital common cause failure or digital CCF; that's the language here.

BTP-10 NUREG CR-6303 process involves 15 steps where you take your digital systems and break them into blocks, identify blocks. And a block is, let's see, the maximum size -- the maximum section of the system for which a failure inside the system can't propagate outside the block. That's the definition.

And then now you look for blocks that contain common software and you postulate the simultaneous failure of those blocks.

BTP-19 calls special attention to ESFAS and reactor trip system for the purposes of D3 evaluations.

So having identified these blocks that have common software now you go to your FSAR events and reanalyze them with the postulated software common cause failure. And you best estimate assumptions, that's a little different from an FSAR analysis. And the acceptance criteria is based on radiation release criteria from 10 CFR 100.

If the results of the analyses are unacceptable, then you add diverse backups as needed for particular events.

The issue here --

CHAIRMAN APOSTOLAKIS: Now wait.

MR. TOROK: I'm sorry.

CHAIRMAN APOSTOLAKIS: I don't understand the best estimate business. What kinds of assumptions are these? Are these assumptions regarding the plant or assumptions or the behavior of the software?

MR. TOROK: Oh, no. The plant primarily I believe. Yes, it's the plant. Because for example you might use a best estimate decay heat model rather than a conservative bounding decay heat model.

CHAIRMAN APOSTOLAKIS: I understand that.

MR. TOROK: That sort of thing.

CHAIRMAN APOSTOLAKIS: As long as you don't make best estimate assumptions regarding the behavior of the software.

MR. TOROK: Right.

CHAIRMAN APOSTOLAKIS: Because I don't think there are any.

MR. TOROK: That's a difficult part of the problem.

CHAIRMAN APOSTOLAKIS: Yes.

MR. TOROK: Yes. Well, in this case the assumption you make regarding the software is that it fails, that the probability of failure is one.

CHAIRMAN APOSTOLAKIS: Complete failure?

MR. TOROK: Yes. Well, or failure enough

that it defeats the safety function that you care about.

Now, this approach is deterministic --

CHAIRMAN APOSTOLAKIS: Now this failure, again, this digital system does what? Just actuates the safety --

MR. TOROK: It could trip the reactor, for example.

CHAIRMAN APOSTOLAKIS: So actuates trip?

MR. TOROK: It could actuate trip, that would be one thing. Actuates an emergency system, for example a core spray system or aux feedwater on a PWR.

CHAIRMAN APOSTOLAKIS: But it doesn't do anything after that? It doesn't control it in anyway?

MR. TOROK: Let's see, are there cases where CCF systems control? Most of them are simply turn it on. And, yes, I think there are a few examples of control

MR. KEMPER: Yes. For example, engineered safety features that actuates pumps, it repositions valves, it control the flow of --

CHAIRMAN APOSTOLAKIS: It does control the flow.

MR. KEMPER: Oh, yes. High pressure safety and low pressure safety injection flows to reactor coolant systems, that sort of thing. I mean, although it's not modulating flow, but it sets the flow at a certain predesign design basis value.

MR. STRINGFELLOW: It basically starts pumps and open valves. It repositions valves as necessary to establish flow paths. Operators are then stepping through their emergency procedures and once they reach a point where they can reset SI, for example, they manually reset SI, they manually stop pumps that sort of thing. Once everything fires off automatically and the necessary pumps are running, then the operators have to step in and take control.

CHAIRMAN APOSTOLAKIS: So the system is out of the picture?

MR. STRINGFELLOW: The actuation system is.

MR. TOROK: So for the most part it's just switching logic. It's not like feedback control as you would have in the feedwater system, for example.

CHAIRMAN APOSTOLAKIS: I thought it did more than just actuate systems.

MR. WATERMAN: This is Mike Waterman.

With regard to reactor trip and ESFAS that's, like Ray said, trips a relay and then the safety has to go to completion. If you're tripping the reactor, it cuts the MCCs to the control rods, the control rods drop into the core. It doesn't do anything to stop that. If it's ESFAS, it turns on HPI, LPI and all that and then it's up to the operator to control and modulate that. There's nothing in ESFAS that's going to modulate anything. It actuates systems, they turn on, spray turns on, containments isolate, ECCS gets going and things like that. And those things have to go to completion per regulation.

MR. KEMPER: However, there are computations as well. Like for example in the reactor protection systems there's variable pressure temperature, trip set points that are calculated by this platform. There's flux flow, delta flow trips. So there's some sophisticated --

MR. WATERMAN: Up to the point of trip and then once the trip occurs, it really doesn't matter what the system does --

MR. KEMPER: Right.

MR. WATERMAN: -- because the safety function itself goes to completion.

CHAIRMAN APOSTOLAKIS: Right. So it does a monitoring job and then --

MR. WATERMAN: Yes, it continuously tries to trip the reactor and if everything is okay, it fails to trip the reactor. But once it trips the reactor, it may continue to calculate but it has no effect on your safety system because they've tripped. They've gone off and done their thing. And essentially your reactor trip system is disconnected.

MR. TOROK: So it's primarily monitoring and reacting to a trip signal at trip level. Yes. A preset level.

Anyway, now let's get back to the BTP-19 approach. What have I done? Sorry.

Now we're down toward the bottom there, approach characteristics. And we characterize this as a deterministic approach with a focus on reactor protection and ESFAS and the FSAR events. And the reason we say it's deterministic is because we say that it says focus on that system and go reanalyze your FSAR events. Don't worry about which events are more safety significant than others or anything like that. And what that has the impact of doing is distorting the safety significance of the software because effectively you're saying the software probability of failure is one and under that assumption if there are results to these analyses that are unacceptable, then you put in a diverse backup. Ignoring the fact that in many situations there are much more significant contributors to system failure than the instrumentation control in the software. So in that sense it distorts the safety significance of the software.

Now I should say this all came about about 15 years ago. And, you know, then I'm thinking it wasn't such a bad approach. But what it effectively does is it says, look, I don't understand what's inside that box with the software, so I'm not sure what it might do. So I'll assume it fails. So that's fine, you know, as long as you don't know what's inside the box and you have to be sure that it doesn't do something bad. But I would say that at this point we know a lot more now about how to look at a digital system and understand the design features in it to be much more comfortable with what it might do and what it might not do. And that's really what this approach is about.

Now, we believe that a risk-informed method offers very significant advantages. It keeps the focus on safety, and you guys know more about this than I do. The object is to show where the software has risk significance and where it doesn't and worry about defense-in-depth and diversity where, for software anyway, it is significant.

This allows consideration of design features that are built into the digital system. And there are characteristics that protect against failure and against common cause failure. For example, self-testing, data validation and fault tolerance.

And as an example here the deal with the software, as you know, is it doesn't randomly, it fails deterministically. And what typically gets software into trouble is when it sees conditions that the designer didn't anticipate and didn't test. So it's a surprise kind of condition or unanticipated condition.

There are ways to protect yourself against that. One of them is data validation. If the sensor data that the system is looking at goes out of range, you flag it and you don't just use it blindly and do stupid things. Now in that sense there's a big difference between a high quality real time digital system and a not so high quality real time system. And we'll have a lot more discussion on that later.

Also under risk-informed method you can consider the fact that when you add diverse backups, you actually add additional failure modes, possibly additional unanticipated behaviors. Certainly the potential for spurious actuation. And these can all be bad things.

And if you think about it, if you have a system that is not very reliable to start with and you add a diverse backup, you're probably improving the overall reliability of the system. But if you have a highly reliable system to start with and you add backups, now you're not on such firm ground. You can actually make it worse, and we think you ought to worry about that in doing these things.

The risk-informed method is also consistent with the latest trends in terms of technical and regulatory efforts. And there I'm referring to the NRC Management position that risk-informed methods should be used or encouraged where they make sense in more and more areas.

MEMBER BONACA: Before you proceed. Just because I don't want to get confused. I understand you're proposing a risk-informed approach. But now the FSAR for these power plants would have the old deterministic analysis, right?

MR. TOROK: Yes. Yes.

MEMBER BONACA: So now you're proposing to use the new set points or whatever, how are you proposing to use this digital --

MR. TOROK: Oh, I see what you mean. I'm

not proposing to use new set points or anything like that. We're proposing to use risk insights to help determine where extra defense-in-depth is of value.

MEMBER BONACA: Yes. I understand that.

MR. TOROK: That sort of thing.

MEMBER BONACA: What I'm trying to understand is that ultimately you have to have a consistency between your accident or you haven't changed yet, I mean whether you believe or not that this addressing risk or just the traditional safety and this new digital system. You will have consistency there?

MR. TOROK: Well, yes. I agree. And I guess this is an area where I should say the PRA approaches in general face the same issues, I think. And I don't know that we want to get into it right now, but there is a confirmatory review process. I'm looking at Dave Blanchard because he's the expert on this.

MEMBER BONACA: No. I'm trying to understand what you end up with.

MR. STRINGFELLOW: Hang on. Let me try, Ray.

MR. TOROK: Okay.

MR. STRINGFELLOW: Let me try. This is

Jack Stringfellow again.

I may not fully understand your question, but correct me if I go wrong here. We are not proposing to change the Chapter 15 analysis. The Chapter 15 analysis will continue to be met with the design. We're not altering that.

What we're proposing here is the use of risk insights with respect to the Chapter 15 analysis to focus on those areas where diversity can be of the most benefit from a risk perspective. So the Chapter 15 analysis will not be revised.

MEMBER BONACA: You wouldn't have a need to do that? All right.

MR. STRINGFELLOW: That's right. Did that answer your question?

MEMBER BONACA: Yes, I think it does. I was just looking at the previous slide on page 8 -- it's 6 where you're talking about that current NRC guidance is problematic and require backups that add complexity and cost without improving safety. And I got the impression when I was reading this that if you used the current guidance, you would not be accepting criteria. For example in LOCA, therefore you would have to do something else that you don't think is significant from a risk-informed --

MR. TOROK: Yes, the acceptance criteria there. We're really focused on this one issue really of digital common cause failure, which is considered beyond design basis event.

MEMBER BONACA: Okay.

MR. TOROK: Right.

MEMBER BONACA: Okay. I think I understand where you're going. Go ahead.

MR. TOROK: Thanks, Jack.

MEMBER BONACA: Again, I'll ask more questions when you get there.

MR. TOROK: Okay. So let's get back. We're right at the bottom of this thing now. So we like the potential advantages of the risk-informed methods, however there are some technical issues here associated with this, and they're at the bottom there. One is digital system failure probabilities, what do you do with that. And the other is this issue of modeling digital equipment in PRA. Everybody's two favorite issues these days. And these are areas that need to faced to be able to use risk insights. They're also areas where at the present time there is no consensus on the best way to handle these things, right? We want to say that up front.

But keep in mind, however, in looking at this too that our goal here is not to establish absolute knowledge of digital system failure probabilities and not to establish absolute knowledge of the best way to model digital equipment in PRA. What we're trying to do is capture risk insights associated with these things. For example, get a handle on where does the diverse backup help, where is it a bad idea; you know, those kinds of things. So risk insights. And we'll probably say that over and over again.

Let me give you an example. You were asking about examples, so we're going to get that. So the first one here is a large break LOCA. And this is large break LOCA with a digital common cause failure in the low pressure injection system. Under the deterministic method, the BTP-19 when you redo the analysis you find that this is a large break, there is insufficient time for operator action to do something now that he's lost low pressure injection. Now in BTP-19 it says for this event it recommends crediting leak detection as a backup.

CHAIRMAN APOSTOLAKIS: This is design basis?

MR. TOROK: Yes, beyond design basis.

CHAIRMAN APOSTOLAKIS: So --

MR. STRINGFELLOW: The digital common cause failure is beyond design basis?

MR. TOROK: Yes, right.

CHAIRMAN APOSTOLAKIS: So would the NRC look at this?

MR. TOROK: Because of the issue of software common cause failure. Now --

MR. STRINGFELLOW: This is what BTP-19 would have us do. It would have us postulate the common cause failure and then look at the LBLOCA and show how we can continue to meet the LBLOCA within the acceptance of criteria of BTP-19, which is relaxed to the current Chapter 15 acceptance criteria. But nevertheless, that's what it would have us do.

CHAIRMAN APOSTOLAKIS: We're getting into the severe accident --

MR. TOROK: No. What this goes back to is that with traditional redundant trains of hardware as a basis of your safety system, since the failures that can disable the safety system are hardware based failure, then you can say well the likelihood of having all the trains fail at the same time due to a common cause hardware failure is at sufficiently small that we don't have to assume that and analyze that. That's the way it's traditionally handled for hardware.

Then along comes software. We put software based control system on each of the channels of the safety system. And now we say well what if there's a bug in the software that's going to prevent all of the trains from acting together or all at the -- I'm sorry. All of them acting correctly?

CHAIRMAN APOSTOLAKIS: So this is an application of the single failure criterion for digital systems?

MR. TOROK: It would be if common cause failure were within the design basis, but --

CHAIRMAN APOSTOLAKIS: It is not.

MR. TOROK: Right, exactly. So the position that was taken in BTP-19 was look, we understand it is beyond design basis, however we still think it's prudent to look at this and here are the ground rules. And the ground rules are go reanalyze the Chapter 15 events with best estimate assumptions so there's a relaxation there. And then are acceptance criteria based on radiation release. And that was sort of the compromise that was struck for --

MEMBER BONACA: The basic thought I guess behind this is that with digital system you may have common cause failure more likely now that --

MR. TOROK: Right.

MEMBER BONACA: Well, I'm trying to say that's --

CHAIRMAN APOSTOLAKIS: First of all, we don't know that the digital common cause failure is more likely than not --

MEMBER BONACA: I'm not arguing that right now. I'm only saying that --

CHAIRMAN APOSTOLAKIS: Yes, but I mean I'm puzzled why in the case all of a sudden we're jumping into severe accident.

MEMBER BONACA: Well, the question is the point that he made is because of the way it was designed it was presumed that there will be no common cause. So that assumption was not made. Now I'm trying to understand why there is an assumption that common cause failure is more likely with digital systems.

MR. TOROK: Well, here's the deal. When a software system fails it's nearly always because there's a design flawed and it manifests itself in the form of a software bug, right, one way or another.

MEMBER BONACA: That's right.

MR. TOROK: And in that sense digital systems operates with extremely high reliability; if one does it, the next one's going to do it probably.

MEMBER BONACA: Right.

MR. TOROK: And that's the assumption that's built in there. And then there are further assumptions. One is we don't know how to put a failure probability on digital equipment and in software, therefore let's conservatively use one and assume that it does fail and then show that you can deal with it.

CHAIRMAN APOSTOLAKIS: Is anybody from NRR here who can shed some light on this?

MR. TOROK: That would help, wouldn't it?

MR. KEMPER: Yes. I'll get started and, Matt, you can follow up if you like.

The Agency took a position on this, oh gosh it's been what? '94/'92 time frame. They got, I guess, the National Academy of Sciences to do some work for them, to do some studies on this subject. And made recommendations that we form a policy to address this issue. A letter was prepared, SECY letter was sent to the Commission. The Commission agreed that since we can't determine the failure probability of software, whether it's more or less likely to fail than hardware, then we would treat it in the manner that we do. That it's a realistic failure but it will be design basis -- beyond design basis failure scenario. And so that's what gave rise to BTP-19 and then NUREG-6303 was further written to embellish the specifics of how you actually do a D3 analysis.

MR. TOROK: Right. So that was the position 15 years ago, roughly.

MR. KEMPER: Right. That's right.

MR. TOROK: Okay. And effectively we're saying well now we can do better than that.

MR. WATERMAN: This is Mike Waterman on Office or Research.

I went back to 1993 and started doing an operator event report, Part 21 review of all the digital safety system, Appendix B, according to Ray highly reliable digital systems. And I found 24 separate incidents of common cause failure in highly reliable safety systems. I don't think they're that highly reliable when I can find that many over a 12 year period.

Secondly, credit for leak detection backup for BTP-19 disallowed by NRC. If you read BTP-19 there was a for example in there. Leak detection for the system 80 plus. System 80 plus had extensive use of acoustic monitors for leakage detection. We had a licensee come in and say well, leakage detection is highly reliable. In July and August that same licensee was cited because their leakage detection systems in two separate plants failed to detect a gallon per minute over a one hour period.

Leakage backup is only allowed if you're going to put in leakage detection equipment that's reliable. So we've got digital systems that are somehow, even though they're more simple than what's coming down for Oconee, are failing. What's causing the failures? All these things that make them highly reliable; self-testing and data validation are two of the things that cause those systems to fail.

So to say these are the things that make these systems highly reliable when those are the things that add complexity and cause them to fail is really off the mark.

MR. TOROK: Well, you're getting way ahead of our talk here.

MR. WATERMAN: Okay. I just want to clarify the credit for leak detection backup disallowed by NRC, highly reliable digital systems is just not really what I've seen.

MR. TOROK: Okay. Shall I continue.

MR. WATERMAN: Okay. Continue to march.

MR. TOROK: I'm sorry. Okay. So large

break LOCA here's an example, okay. With common cause failure low pressure injection under the deterministic method there's no time for operator action and you can't credit leak detection for whatever, right, as Mike explained. And therefore you need to diverse actuation of low pressure injection and its supporting systems.

Now, if you look at that from a risk insight point of view you would say well, the probability of the digital common cause failure is -- I don't know what it is perhaps, exactly. In fact, I certainly don't know exactly what it is but I have plenty of reason to believe it's much less than one. So that's one factor.

Another is that the likelihood of the large break LOCA itself is quite low. And when I look at those two together I conclude that the overall contribution to core damage frequency from the combination is very low. Very small.

CHAIRMAN APOSTOLAKIS: Well, but you know what you're doing here is you're going back to the original assumption that digital CCF, we don't know how likely they are so therefore we're going to be conservative. And now essentially you're saying don't be conservative. It's a low probability event. That's really what you're saying. I mean, it's not this concise.

MR. TOROK: Well, what I'm saying is I don't know precisely what the number is, but I know it's less than one. Let me pick a number and see what ballpark I'm in in core damage frequency. Just get a handle on where I am.

CHAIRMAN APOSTOLAKIS: Right.

MR. TOROK: I'm trying to capture a risk insight here.

CHAIRMAN APOSTOLAKIS: Right.

MR. TOROK: So that's one thing. If I look at it this way, my conclusion is this event is not a large contributor to core damage frequency.

There's another important fact, though, that comes out of the risk evaluation. And that's that if you do add a diverse backup for the I&C in the low pressure injection system, it turns out it wouldn't reduce the core damage frequency because the failure probability of that system is dominated by the large rotating machinery, the big pumps and valves and spinning things.

CHAIRMAN APOSTOLAKIS: What is their common cause failure rate?

MR. TOROK: Off the top of my head, I

don't know.

MR. BLANCHARD: For a typical low pressure injection --

CHAIRMAN APOSTOLAKIS: You have to come.

MR. BLANCHARD: My name is Dave Blanchard.

For a typical low pressure injection system you would have a common cause factor on the order of 10^{-3} to 10_{-4} per demand.

CHAIRMAN APOSTOLAKIS: And you're saying that the digital system is better than that.

MR. BLANCHARD: On that order or better, yes.

CHAIRMAN APOSTOLAKIS: And how do you know that?

MR. BLANCHARD: We will be addressing that in a few minutes.

MR. TOROK: Yes. We'll get there.

MR. BLANCHARD: Yes. Right. Thank you.

MR. TOROK: Okay.

CHAIRMAN APOSTOLAKIS: I don't know. I am uncomfortable with this. I'm not sure you're using any risk insights here. Am I the only one who feels that way. You're just attacking the original assumptions.

MR. TOROK: Well --

CHAIRMAN APOSTOLAKIS: The Staff say we don't know the details, we'll have to assume one. Why do you say no don't assume one? Is that risk insights?

And also this being more useful after we approve the rule 50.46(a) which allow you to do certain things for break sizes greater than the transition. And the other argument there, you know, the first subbullet at the bottom, don't do anything to this because something is riskier. Well, that's an interesting thought, although in real life I mean we do that all the time, I must admit.

MR. TOROK: Well, under these assumptions the conclusion is that the BTP-19 method drives you at hardware and increase the complexity but the safety benefit is questionable at best. So is that good engineering? That's the question. I'll leave that as the question.

CHAIRMAN APOSTOLAKIS: Wait a minute. Now there is always another hand, you know that. The large break LOCA is supposed to be the limiting accident.

MR. TOROK: Pardon me?

CHAIRMAN APOSTOLAKIS: The large break LOCA is supposed to be the limiting accident. It's supposed to protect us from all sorts of things that we haven't even thought of. So just to say that it has low probability of occurrence, ah, doesn't cut it. Because you know it's the things unknown and knowns that you're so conservative designing the thing using large LOCA as a design basis accident that you are covered, you know. So -- anyway we're getting into territory now -- let's go on. Let's go on.

MR. TOROK: It's still, you know --

CHAIRMAN APOSTOLAKIS: I'm sorry, Jack?

MEMBER SIEBER: It's not clear to me how not installing a diverse system has an impact on overall system reliability. In other words if you install a backup system, obviously you're going to effect reliability as a positive way. And I think you have to come up some real numbers to be able to establish what that's worth.

CHAIRMAN APOSTOLAKIS: Is argument is though that, yes, you are reducing risk but I mean the rotating components are still the same and they have a higher probability of failure, right? That's what you mean by backup? It's a backup to the I&C.

MR. TOROK: Backup to the I&C only.

CHAIRMAN APOSTOLAKIS: Not to the system itself?

MR. TOROK: That's right.

CHAIRMAN APOSTOLAKIS: So the system failure probability is dominated by the failure of the pumps?

MEMBER SIEBER: That's true.

CHAIRMAN APOSTOLAKIS: So by adding the backup system you reduce something else, but this probability is still high. That's their argument.

MR. TOROK: Yes.

MEMBER SIEBER: So don't bother. You could eliminate half the stuff in the plant.

CHAIRMAN APOSTOLAKIS: That's the point. That was my point earlier that you know just because something dominates it, don't eliminate everything else.

MR. STRINGFELLOW: If I might, this is Jack Stringfellow again. If I might offer up a little anecdote with respect to the comment that Mr. Sieber made.

Vogtle recently replaced or we have been in the process of replacing our diesel sequencers with a digital system. And we did a decubed analysis for this system and we identified as a result of the decubed analysis, we added some hardware. Some electronics to some analog hardware to mitigate a potential common cause failure of the system to fail shed load. We installed the first train of that system. And during testing that device actually underwent an infant mortality. There was a compositor in that device that had an infant mortality. It failed and actually caused a failure to shed load during the test.

So, you know, to my mind that's an example of where we added hardware that actually caused a failure due to a random failure of a compositor.

MEMBER SIEBER: Well, since we're telling war stories, I used to be site Vice President of Beaver Valley. And we installed digital sequencers on our diesels and when we went through all the post-modification testing and everything and everything was fine. When we tested them after 18 months both diesels failed to sequence. And the reason was that it was unable to sufficiently reject surges on the DC power system to the extent that it reset the microprocessors to zero and destroyed the timing in there. And it would count out. I mean, it was difficult to troubleshoot that.

So I believe that there are situations that can occur in power plant on simple digital systems that give you common cause failures. And, frankly, when both diesels failed to start and load, that got me upset. It cost $80,000 in enforcement action.

MR. TOROK: Right. Okay. Yes, which is an interesting example and we should talk about that and maybe the software complications there, if there are any. But okay, let's go on.

Now we have another example. In this case we're not talking about a pipe break or an FSAR event, we're talking about risk significant events that are modeled in the PRA but not in the FSAR necessarily. Now this is -- you don't need to read all the small print here. This is an event --

CHAIRMAN APOSTOLAKIS: This is a large LOCA tree -- oh, transient.

MR. TOROK: Yes, it's an event tree.

CHAIRMAN APOSTOLAKIS: No, but what's the initiating. Yes, I know the shape I've seen before.

MR. BLANCHARD: This is a loss of feedwater event tree for PWR.

CHAIRMAN APOSTOLAKIS: So it's really a transient.

MR. BLANCHARD: Yes, it's a transient event tree.

MR. TOROK: So it's a high frequency

initiator. And in this case the PRA looks at the number of paths coming over here and through the bottom and every which way, and many of them result in core damage frequency over there.

CHAIRMAN APOSTOLAKIS: Right.

MR. TOROK: Now the FSAR -- the PRA addresses all those paths. The FSAR addresses that one and this one, the dash lines on there, right?

CHAIRMAN APOSTOLAKIS: The design basis accident you mean?

MR. TOROK: Yes.

CHAIRMAN APOSTOLAKIS: And so BTP-19 would say look at that one and look at this one, don't worry about all this stuff.

CHAIRMAN APOSTOLAKIS: Yes.

MR. TOROK: Well it turns out some of these are significant contributors to core damage frequency. And that's because the PRA routinely considers beyond design basis events that are risk significant.

CHAIRMAN APOSTOLAKIS: Now I'm confused. I mean, the previous slide said the NRC Staff went beyond design basis in BTP-19 and now you're saying here no, no, no that was really bad. I mean, they're staying within the design basis. Which one is true?

Or is it again whatever --

MR. TOROK: No, no, no. In either case the event is considered -- the common cause failure event is considered beyond design basis. In the previous example it's an example of where the BTP-19 method would cause you to put in a diverse backup and that apparently -- or that seems to have little or no safety benefit. In this case the BTP-19 approach ignores some potentially safety significant sequences that probably should be considered. So in a sense -- and this in one both ends.

CHAIRMAN APOSTOLAKIS: Wait. Wait. Wait. What does it mean it missed the safety significance. I mean, safety significance is a relative term.

MR. TOROK: Yes.

CHAIRMAN APOSTOLAKIS: So you're saying that there are some beyond design basis sequences that dominate core damage frequency.

MR. TOROK: Yes.

CHAIRMAN APOSTOLAKIS: But core damage frequency is acceptable in this plan.

MR. TOROK: But if I add common cause --

CHAIRMAN APOSTOLAKIS: And there is always something that dominates.

MR. TOROK: Please, Dave.

MR. BLANCHARD: This is Dave Blanchard again.

The branch technical position reviews the effects of common cause failure for design basis events only. It does not consider the potential introduction of common cause failure in beyond design basis events that are evaluated in the accident sequences of the PRA.

CHAIRMAN APOSTOLAKIS: That's correct.

MR. BLANCHARD: So we can actually introduce a common cause failure from a digital system that can increase the frequency of these accident sequences and it will go unevaluated under branch technical position 19. We won't know about it until someday we update the PRA.

CHAIRMAN APOSTOLAKIS: But when you increase that frequency how many failures do you have to assume exists after the initiating events? Because if you have to assume more than one, you are beyond design basis.

MR. BLANCHARD: Oh, no question. You are beyond design basis.

CHAIRMAN APOSTOLAKIS: So you are increasing the core damage frequency but we don't regulate on the basis of the core damage frequency.

MR. BLANCHARD: What we're proposing here with this guideline is that a risk informed method to review --

CHAIRMAN APOSTOLAKIS: Ah, is more coherent, is more production?

MR. BLANCHARD: Yes. Yes.

CHAIRMAN APOSTOLAKIS: That's different.

MEMBER SIEBER: You don't agree with that?

CHAIRMAN APOSTOLAKIS: Nobody disagrees with that.

MR. TOROK: Okay. We can go on then. Okay.

So there's the two contrasting examples --

CHAIRMAN APOSTOLAKIS: But you know -- go back. Beyond design basis events are considered in the PRA and they are unevaluated using BTP-19. They unevaluated using the totality of the regulations.

MEMBER BONACA: That's the point I was trying to make before.

CHAIRMAN APOSTOLAKIS: Yes.

MEMBER BONACA: Okay. We are killing--

CHAIRMAN APOSTOLAKIS: We are killing BTP-19 as if it were --

MEMBER BONACA: We're beating the same dead horse. And the point is -- but that's the basis of the licenses that the plants you're addressing right now have. So that's the way it is.

CHAIRMAN APOSTOLAKIS: And that's why we're moving to a risk-informed environment as fast as we can. This argument we know.

MEMBER BONACA: Here more than anything else I am trying to understand, you know, and you're doing a good job of how you propose to intermingle this --

CHAIRMAN APOSTOLAKIS: Yes.

MEMBER BONACA: -- deterministic and probabilistic approach in a way that still preserves the licensing basis of this plant because that's what it is.

CHAIRMAN APOSTOLAKIS: Yes. I really -- oh, I'm sorry.

MEMBER BONACA: Yes. That's it.

CHAIRMAN APOSTOLAKIS: I'm really interested in understanding better your three methodologies.

MR. TOROK: Okay.

CHAIRMAN APOSTOLAKIS: Extended, standard risk and simplified risk. That's where the action is. We know this area.

MR. TOROK: Okay. Let's move on. We had

here some different views --

CHAIRMAN APOSTOLAKIS: No, I'm not telling you to skip slides, I mean unless you want to. But don't try to convince us that the risk-informed approach is better than the --

MR. TOROK: Okay. Okay.

CHAIRMAN APOSTOLAKIS: All right. We're with you on that.

MR. TOROK: Okay. Tell you what, I'll do this quickly. We have a list here of ways of looking at the digital reliability issues. The first two questions here -- it's just interesting to look at different ways to look at this.

How reliability is the software? That's a question where we would say -- and it's probably unfair to say focus here, maybe emphasis. But the NRC research emphasis on establishing how reliable software is whereas we're emphasizing how reliable does it need to be. And this is a good example of getting a handle on the second question can help you figure out how far to go with the first question so you don't spend a lot of money going way farther than you really need to.

Now all the rest of the questions on that page, which I don't know how to skip through quickly, are kind of the same thing. It's the same thing over and over again.

One thing that I should call attention to that's a little different, though, is that Research, or NRC let's say, emphasis has been on what process attributes affect reliability. And a difference between what they're pushing and what we're pushing is we say what design attributes affect reliability. So we want to look at the as-built device, not just the process that built it. And we think it's more important to look at the design attributes. And Thuy is going to say a bunch more about that later.

I'm going to skip the rest of these and you can read, I guess, at your --

CHAIRMAN APOSTOLAKIS: So do you really want to send the message that you are disagreeing on everything?

MR. TOROK: Well, no, no, no. That's not the message at all.

CHAIRMAN APOSTOLAKIS: It's not the message I'm getting --

MR. TOROK: The message is that there are different ways to look at these things. And we said "focus" here, and maybe that's too strong.

CHAIRMAN APOSTOLAKIS: Maybe you can

remove RES and EPRI and say one approach is this, the other approach is that. And we like the second one.

MR. TOROK: Well, some combination of them is kind of nice.

MR. STRINGFELLOW: That's why we titled the slide complimentary.

MR. TOROK: Yes. Right. We're saying --

MEMBER SIEBER: We're not fooled by that.

CHAIRMAN APOSTOLAKIS: You're saying that you're interested in establishing reasonable assurance and the Agency is not?

MR. TOROK: Well --

CHAIRMAN APOSTOLAKIS: This is our bread and butter.

MR. TOROK: It's a difference in emphasis. How do I prove my liability claims? That's a tougher question than how do I establish reasonable assurance.

CHAIRMAN APOSTOLAKIS: I still think you should change the headings.

MR. TOROK: Okay.

CHAIRMAN APOSTOLAKIS: And say there may be two -- separate approaches and this is the one we're talking about. Because every single one of these can be challenged.

MR. TOROK: Okay.

CHAIRMAN APOSTOLAKIS: There is no reason to do that. I mean, you know that the Staff doesn't do that.

Let's go on.

MEMBER SIEBER: Actually, you got to answer all the questions if you look at them.

MR. TOROK: The main point was that the right -- the two kind of help each other out if you can fill in all the blanks; that's all.

Now --

MEMBER BONACA: Your question, the way you pose it, how reliable does it need to be. It depends on what criteria you're using. So you're saying well I don't like the deterministic, I'm going probabilistic and then this is that. I can understand how you have to first of all establish a guideline on a process which is acceptable enough to answer the question; how reliable does it need to be? It depends on what criteria you're using.

MR. TOROK: Well, and for example in that one I would say I need to show that it's sufficiently reliable, that it's not going to dominate the failure probability in a system that it's in, right? Okay. Now I can go to my PRA and in other words, probably I can generate a number there. Now I go back to my reliable is it and say hey, here's my target. You know, my target's not 10^{-9}, it's just 10^{-3}. Right? Makes a huge difference in what you would do to show reliability.

MEMBER BONACA: I understand.

MR. TOROK: That's the whole point, right?

MEMBER BONACA: Understand.

MR. GUARRO: There are certain points one could easily argue with. For example when you say which failure facts are important to safety, I don't think that can be contrasted with respect to the previous question, which is I think what it's supposed to contrast, which is how can digital systems fail. If you do not know how they fail, it's pretty hard to see what the effects are, right?

MR. TOROK: Yes. Right.

CHAIRMAN APOSTOLAKIS: I think that was not the most successful slide.

MR. STRINGFELLOW: Well, we've had a couple of those.

MR. TOROK: Yes, we have.

CHAIRMAN APOSTOLAKIS: Probably for other audiences you didn't have the same problem you're having today.

MR. TOROK: So you can be sure we won't

use that slide again.

CHAIRMAN APOSTOLAKIS: That's called learning from experience.

MEMBER SIEBER: Are we supposed to be keeping track of slide quality?

MR. TOROK: I would call that --

CHAIRMAN APOSTOLAKIS: Okay. Let's move on. I want to see the three methods.

MR. TOROK: Yes. I would characterize that as an operating history failure, by the way.

Okay. Now here's the key points we're trying to make it. You guys liked the first one, I think. Use of risk insights helps us do a better job, okay?

CHAIRMAN APOSTOLAKIS: Absolutely.

MR. TOROK: Great. That's one.

Okay. And we believe that it's possible to derive useful risk insights for D3 evaluation, not for general purpose PRA evaluation, but for D3 evaluations now. And we think that you can derive those risk insights without precise knowledge of failure probabilities and without detailed PRA modeling of the digital I&C. And we'll talk about how that works. Okay. And we say that for the purposes of D3 evaluations, not general purpose PRA, we can get a handle on the reliability of the digital equipment based on deterministic evaluation of the equipment. Deterministic evaluation, okay? And we're going to talk more about that.

And we believe that the ongoing and future work by NRC Research and others is just going to help that. There's a framework here as methods to determine software reliability become better and better, that's great because they can be used within this framework. Same thing for modeling digital systems in PRA.

Oh, that was fast.

CHAIRMAN APOSTOLAKIS: Now I want to take a ten minute. Is this a good time?

MR. TOROK: Okay.

MEMBER SIEBER: Ten minutes.

CHAIRMAN APOSTOLAKIS: Yes, we're going to have two breaks this afternoon, ten minutes each. 12½, Jack.

MEMBER SIEBER: That includes travel time.

CHAIRMAN APOSTOLAKIS: We'll 2:55 -- no. Until 2:55.

(Whereupon, at 2:43 p.m. a recess until 2:56 p.m.)

CHAIRMAN APOSTOLAKIS: I can start without some members, but not without the speakers.

MR. TOROK: Okay. Excellent.

Before we start, I have a request that we heard from Mr. Waterman mentioned a number of software common mode failure problems that he discovered.

CHAIRMAN APOSTOLAKIS: Yes.

MR. TOROK: We'd like to see a formal list of those. That would be very helpful to us. You know, we asked our group, but we don't have a good knowledge of that. Thank you.

Now, here's the other thing. We know we want to get through this as quickly as we can. We're going to try and go through the general stuff. Obviously, we're going to need some of your help on that. And what we're really trying to get to is the two technical issues that we have in one of the early slides. All right. They are what we call defensive measures and how we look at susceptibility for software common cause failure and how we estimate failure probability. That's one part. And the other one is the modeling and PRA and the risk insights that come out of that. So we have to get to those things. Everything else builds up to that.

So, please, friend, let us get through the next few slides pretty quickly.

Anyway, so you asked about guidelines

methods. There are three methods in the guide. I want to describe them very briefly and at fairly high level. That are papers that are published that we can provide that give all the details of them. But I think we can describe the methods fairly simply. And since you guys are well versed on PRA, you'll understand what we're talking about very quickly here.

Now the first one we call extended deterministic method. And it basically is the BTP-19 approach, however for problematic events like large break LOCA we would say take a risk-informed look at it to see if that puts the event in a new focus. That's basically what the method does, simple as that.

The second one we standard risk-informed. That's where the idea is capture a risk focus with realistic assumptions and what you're really trying to do there is update your PRA to reflect the digital equipment, which means you need to put in failure probabilities and beta factors and so as it makes sense, and then regenerate your results and look at your core damage frequency. That's the basic idea.

And at some point if you're putting in digital upgrades, regardless of the D3 issue, you'll want the PRA model to be consistent with the plant and you'll face this problem.

The last method is simplified risk-informed. And this is where we take conservative assumptions and use the PRA so you don't have to update your PRA model to do this one. And what you basically do is treat the software common cause failure as a new failure mode and you say for each event, you would say you have an event frequency from the PRA model. And you multiple that by the failure probability of the digital system or of the software. And that gives you a delta core damage frequency for that event. You do that over and over again to see what the total change in core damage frequency is and you also identify the large contributors to it, and that tells you where to focus. That's what the simplified risk-informed method is about.

Now for the risk-informed methods, the acceptance guidance from Reg Guide 1174, which you're all familiar with in looking at delta CDF and so on.

All three methods use what we call a confirmatory defense-in-depth review which is where you do a sanity check on your results to make sure you didn't miss something important. And without getting into the details, and then the idea there is if the acceptance criteria aren't met, you've got some options. You could refine the assumptions if you can defend revisions to your assumptions or you could use one of the other methods. Modify your design so that the common cause failure issue goes away, you know it doesn't exist anymore or add a backup function as you would under BTP-19.

That in one page is what all our methods do.

Now, regardless of which method you pick the first thing you have to do is figure out where you're suspectable to digital common cause failure. And under BTP-19 we talked about this. You identify blocks and if the blocks have the same software, you're suspectable. We do something a little more than that. We say well wait a second, that's not the whole story. You can look inside those blocks and you can identify design features and behaviors and whatnot that are designed into the thing that help constrain the failures that you have to worry about. And Thuy's going to explain that in more detail momentarily.

There are a couple of things that I wanted to mention here. One is that this is a deterministic way to look at a digital device to understand what its failure behaviors might be and how they might get you. So it's deterministic in that respect. That's really important.

Another is it gets beyond the process based way of looking at software quality. A great process does not guarantee a great product. It might guarantee a well documented product. But what we believe is more important for establishing reliability and reasonable assurance that you have high reliability, is that you want to make sure the right defensive measures or the right design attributes are built into the device. You want to understand the final as-built device, and that's what this is about.

MEMBER SIEBER: How do you examine the software to predict all the failure modes that might occur.

MR. TOROK: We'll get to that in a minute.

And I said this already, the defensive measures provides a deterministic basis for estimating likelihoods of failure and digital common cause failure. And we're going to talk about that.

Now still, we want to acknowledge again that this is different from standard PRA treatment of hardware because software fails deterministically in the sense that when it sees the right set of condition, it'll do the same thing every time, or nearly every time. I guess Microsoft may not agree with that statement. Anyway, but what you really have to get a handle on here is the likelihood that the system will encounter unanticipated conditions; that's one thing. And the likelihood that those anticipated conditions will get you into trouble in your plant context.

To do this evaluation where you're looking inside the box is not something that you can do using a handbook of failure probabilities that might be great for modeling pumps and valves and PRA. In this case it requires specific expertise in software and detailed knowledge how a digital device works.

And with that, I want to introduce Thuy Nguyen who is our expert on this.

MR. NGUYEN: So good afternoon.

I'm a software expert, and my job is to analyze -- one of my job is to analyze the software systems at EDF that are safety critical for the EDF plants.

So, in fact --

CHAIRMAN APOSTOLAKIS: So how come you're here? Are you spending time at EPRI?

MR. NGUYEN: Yes. Because EDF and EPRI have cooperation agreements. We would like to share research effort.

CHAIRMAN APOSTOLAKIS: Okay.

MR. NGUYEN: So I'm spending a few years at EPRI in Palo Alto.

CHAIRMAN APOSTOLAKIS: A few years?

MR. NGUYEN: Yes. This is a certain number of important projects where we prefer to have a much tighter cooperation than just phone and email.

CHAIRMAN APOSTOLAKIS: The first ten years are difficult ones.

MR. NGUYEN: In California it's fairly easy.

So I will start by very obvious things first and introduce my terms.

First, the notion of digital faults. A digital fault is a software bug, mostly. And by itself it does nothing.

A digital fault if it's not activated by particular conditions in the digital system will remain latent and have no effect.

And I think we have heard recently of a software bug found at Palo Verde. This is typically the case of a software bug that exist permanently in the software but is activated only when a hardware fault occurs, a particular hardware fault occurs. And as long as this hardware fault doesn't occur, the software fault is dormant.

When there is an activating condition occurs, then you can have a digital failure. If this activating condition effects only one channel of a redundant system, only this channel will fail. So a digital fault does not mean that we had digital failures. This fault in Palo Verde has not been activated in operation.

Now a failure of a channel is not yet a common cause failure. A common cause failure occurs when the activating condition effects multiple channels concurrently. And this is very important because I would say the analysis approach that I will be presenting in the following slides is based on this, I would say, vision of how digital CCF only.

I have also a small remark saying that there are some digital faults that are activated but do not result in failures. And there are failures that are not risk significant. So we here are focused on risk significant failures.

So in order to explain how software systems work and fail, I have taken the metaphor which is a mine field metaphor. I have a very large mine field that I spent a lot of effort to remove the mines, but I'll never be able to say there are no mines left. So if I walk in this mine field without specific pattern or randomly, at every step I might step on a mine.

Now, this is not the case of certain types of systems. Certain types of systems in fact are designed to function cyclically. They follow again and again the same path. So if I think, I'm going back to mine field, if I walk along this path of course the first cycles I will be quite worried that I might step on a mine. But after a certain number of iterations provided that my path is not too wide, I will grow a higher level of confidence that even though there might be still some mines left in the mine field, they will not on my path.

And what is important to understand is what's the width of my path. If it's very large like a highway, I will need quite a number of iterations It's very narrow, after a certain number of iterations I can say, yes, it's quite unlikely that if I stay on this path, I will step on a mine.

And here we're dealing with software that are designed to be what we call deterministic. Of course, totally in theories all software is deterministic. But what I call deterministic is when we understand and know what are the influence factors that will effect the software trajectory. And in this case the software is under the influence of a certain number of factors that will effect the width of its path.

I have listed here in these bullets a number of influence factors. For example, you have the input variables coming from the process.

You have the memory that the software system keeps from one cycle to the next.

You have blocking interrupts. You might have process-related interrupts. And you have also internal resource management like memory allocation and so on.

In most of the -- in all of the systems that I know there are certain number of measures that have been taken to narrow the path of the cycle. For example, all resource management is static. There is no dynamic memory location, for example.

The process interrupts -- rated interrupts are not allowed.

There are clock interrupts in certain systems that occur every millisecond. And there are, I would say in software terms, represented a small amount of curve that can be verified very thoroughly.

Short-term memory is also kept to a minimum. That usually represents only a few variables that can be very formally identified.

The number of processing inputs come from the process and they can be validated before used, and we will see how we will deal with that.

So as long as things stay, I would say, in the nominal conditions the system will ge on this green path and typically a number of situation per year in a single channel in about a billion.

So after a number of situations I think my engineering judgment is that it's very unlikely that it will fail in this condition.

Now, of course, my system must be able to react to a number of, I would say, conditions occurring so that it some use. So I have listed here a number of what I have called infrequent influence factors, influence factors that could take the software system out of its green path on which I am so comfortable.

For example, there is initialization. But this executed only once.

The operator request. For example, every month the operator changes some set points. This can be done channel-by-channel so I do not say that operator request cannot activate a software fault. What I say that we can take measures in the operation and the maintenance of the system so that this does not effect concurrently all the channels of my redundant system.

There are hardware failures like the Palo Verde example. But the hardware failures usually effect a single channel.

There are exceptions. For example loss of power or the operator has pushed the reset button. The reaction of a protection system to an exception is usually to stop the processor. So it's a very, very simple action.

There are particular date and times like the Y2K date, for example. And the usual approach to avoid these kind of parameters is to say we will not manage dates and times in this kind of system

So what is left? Ah, the plant transients. Because the plant transients effect concurrently all the channels and these are, I would say, the main events that could trigger potentially a software common cause failure. And of course if that appears and if it leads me to an unforeseen, untested condition, then there is a possibility that I might step on the mine and that my system fails all its channels concurrently.

So that is an important element to take

into consideration.

So now let's look at the internals of a software system used for reactor protection. Usually it's composed of an operating system and of application software. The application software is usually subdivided into two main parts: Standard elementary functions and application specific software. So the operating system and the standard elementary function usually are bundled with the I&C platform.

Now, an important design feature of I would say a well designed operating systems for applications is that the operating system is independent from the application software and that it is transparent to plant condition. The operating system will read inputs and give them to the application software. But whatever the values of the input, it's not effected. The operating system does not react to interrupts coming from the plant processes. So it's in its own circular path. The application software is in its own circular path.

Now, if I have a plant transient, since the operating system is blind to the plant condition, it will remain on its green path. Only the application software will be taken out of its own green path and follow a different execution path.

So what I'm saying here it is quite important. It's that provided that my operating system has the appropriate properties, and that's a very big if that needs to be substantiated and proven by appropriate argument and evidence, the operating system will not fail or is very unlikely to fail during plant transients. It will stay in its repetitive path.

And that is, I would say, something that is difficult to accept by most people. We have talking in our work group since quite a long time, and it took me quite a number of discussions just to feel that.

The second part of the platform software is the standard elementary functions. There I will take another type of argument. These functions are usually very small and/or assign a delay. They are very small functions but usually independent from one another. They have no internal memory. They're based usually on very well mastered algorithms. You can perform very, very thorough V&V. So on engineering terms the digital faults in the functions of the standard library are quite unlikely.

So this is the basis for my statement.

And, of course, again that will need to be supported by a very argument and evidence.

So our last part that we have not addressed in the previous slide is the application specific software. And I have put here, I would say, the two main sources of potential faults of the application software. We have, of course, the software implementation faults, but we have also the specification faults. And in my experience it has always been the specification that has been the undoing the application software.

In the software implementation you can take very, very strong measures to make sure that it's reliable and as fault free as it can be.

I have signs from Ray to go faster, so I will not go very deep here.

I will try to speak a little more on specification faults. There are two main types of specification faults. What I call the expression faults in the functional specification and the fault that results in an incorrect understanding of the plant and its systems by the specifiers.

You can take means to avoid expression faults. But the lack of understanding is quite difficult to address and they are usually in my experience all the faults that I've seen are faults of these types.

And now if we look at the notion of common cause failure. The main source of common cause failures in a redundant system are here. And if I make a redundant system based on four channels, each channel using a different platform but implementing the same application, I would still say that the beta factor is wrong because of he --

CHAIRMAN APOSTOLAKIS: Software failure.

MEMBER SIEBER: Need we say more?

MR. NGUYEN: Okay. So that's again a very, very strong claim. And I have insisted here that it needs very good argument and evidence.

EDF will be building a new power plant in the years to come based on the Framatome design. And my team has been in charge to provide this type of argument for the analysis for the -- and I had one year or one year and a half to do that.

So now if we try to give some figures on the probability of digital failure, I would say the probability of digital failure resides mainly in the evaluation of the likelihood of a fault in the specification. And the lack of understanding are I would say quite similar for digital or for analog systems. So my point would be to say probability of systematic failure of a digital system should be in the same range as an analog system. After that, we have the probability of failure due to hardware and I think that there are appropriate methods to do that.

So, again, later one we will take beta factors between digital systems. But the beta factors have nothing to do with the I&C platform, again provided the fact that the I&C platform has the appropriate defensive measures.

MR. TOROK: Okay. You know, yesterday we had this problem when the computer was unplugged. Do we know that this is okay?

CHAIRMAN APOSTOLAKIS: It's working.

MR. TOROK: Well, the computer will go for a while.

Okay. So our next guy Dave. Now we're moving it to transitioning from defensive measures to risk insights; how do we get from here to there, right? And Dave Blanchard is our next speaker.

MR. BLANCHARD: My Dave Blanchard. I'm from Applied Reliability Engineering. And I've been working with Ray and the rest of the working group for the last several years in developing the guideline.

Early in the presentation we saw our two major questions were where do the numbers come from in terms of digital common cause failures. But a second question was how do we incorporate the effects of digital common cause failures into risk assessment. And what's my presentation will be on, using the defensive measures approach that Thuy just introduced. He has provided us with methods to show that the potential for failure of a digital channel even is on the same order of that as a similar analog channel. And in addition to that his defensive measures approach as outlined in the guideline allow us also to take a look at the potential for common cause beta factors between redundant channels of instrumentation and control.

Now, where these redundant channels exists has an effect on the probability of common cause failure. Identical trains in the same system, as an example, using the same inputs, using the same signal processing and voting logic will probably have a very high common cause factor just because software behaves deterministically. Between different systems that may use different inputs, different signal processing, different voting logic the common cause factor can be less than one and the guidance document provides information as to how to go about determining the numbers.

We now have to incorporate those common cause failures into the PRA. And the way we do that according to the guideline, is to take a look the defense-in-depth and the diversity that exists in the plant as modeled in the PRA with the existing mechanical and electrical mitigating systems. And in a minute I'll illustrate how that's done.

We'll incorporate those potential effects of digital CCF into the PRA and reevaluate a core damage frequency using one of the three methods that are in the guideline.

And then on completion of that we'll perform sensitivity study to help develop insights with respect to, well several things. Under what accident sequence conditions does I&C diversity have value? Under what conditions does it appear that the risk is insensitive to digital common cause failures? And as important as those first two questions, why are the results sensitive or insensitive to the introduction of digital common cause failures? What design features and operating characteristics of the plant and of the I&C system itself cause those results?

Now, as we developed the guideline we in fact incorporated insights, accepted data, manipulated models from quite a number of PRAs to make sure we understood the nature of the kinds of insights that we could develop. There were some five PRAs that ultimately ended up being used as a part of the development of the guideline. There were three Westinghouse PWRs, differing vintage from a two loop Westinghouse plant up to a four loop. We had a combustion engineering PRA that we were allowed to use for some of these sensitivity studies. And then we also had a BWR 4 who volunteered their PRA for this effort.

And we began pretty simply just looking at some of the mitigating systems and imposing the effects of common cause failures into each of these systems and then varying the likelihood of the common cause failures to try and determine what the effects of introducing digital common cause failure would be on each of these systems.

Recognizing that the systems themselves don't work in isolation to provide adequate core cooling, we then moved on to selecting a few accident sequences and performed some very similar sensitivity studies that we had with the systems to see where digital common cause failure has a most significant impact and where the results are insensitive.

CHAIRMAN APOSTOLAKIS: Now let me understand what you did here.

MR. BLANCHARD: Sure.

CHAIRMAN APOSTOLAKIS: When you say you varied the common cause failure, you varied beta?

MR. BLANCHARD: We varied both the probability and the beta factor.

CHAIRMAN APOSTOLAKIS: Okay. And did you do it on the individual system or cut across systems?

MR. BLANCHARD: In the beginning we defined a fairly simple problem. We just simply took an individual system and imposed on that system the instrumentation of the common cause failure of a presumed digital system to see what effect it would have on the reliability of the system.

Some of the insights we found from that type of a sensitivity study were that if we had a system with multiple trains where the mechanical and electrical equipment within those trains, most of it was active rotating equipment or valves that had to move, that those types of systems were not very sensitive to changes in the common cause failure probability. We could vary the potential for digital common cause failure between the trains of those systems by an order of magnitude or more and have very little effect on the overall failure probability of the systems.

We did find some systems that were fairly sensitive to the introduction of digital common cause failure. Those were systems which contained a lot of passive components. The AC distribution system is an example or buses and breakers and cables that don't necessarily have to change position in order to provide their function during an accident. In addition to that, the AC power system has two very diverse sources of power, off site and the diesel generators. And when we encountered passive systems and systems with that kind of diversity we found it was very easy for the instrumentation and control to dominate. And if a failure of the instrumentation and control were due to common cause where multiple divisions of the system failed, we found the I&C to dominate in those situations.

CHAIRMAN APOSTOLAKIS: The systems that were presented earlier to us by the Staff, the Framatome and Westinghouse, these are supposed to control all the safety systems, aren't they?

MR. KEMPER: This is Bill Kemper again.

With regard to the RPS and ESFAS, they

could also be deployed with other system applications as well.

CHAIRMAN APOSTOLAKIS: The ESFAS is all these,safety injection --

MR. KEMPER: Right. Right. Safety injection. Exactly. Contained in isolation.

CHAIRMAN APOSTOLAKIS: So is it then reasonable to do the traditional common cause failure analysis and do it on individual systems? Is it possible that you will have a digital system fault that would effect the actuation of all the safety systems?

MR. BLANCHARD: Yes. And, in fact, again we recognize these systems don't work in isolation.

CHAIRMAN APOSTOLAKIS: So did you analysis--

MR. BLANCHARD: Some are -- each other, and our next step then was to expand the analysis into looking at entire accidents --

CHAIRMAN APOSTOLAKIS: To multiple systems? So you did that?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: So that's in slide 23?

MR. BLANCHARD: That is coming up next,

yes.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BLANCHARD: All right. And in fact, I will get into some examples of the results in subsequent slides.

Just briefly, we didn't limit ourselves just to looking at selected systems and a few accident sequences from some of these PRAs. We did take a one full scope level one PRA for a PWR and looked at all the accident sequences in posing a plant wide digital upgrade into these models and then performing some of the same sensitivity studies to find out which accident sequences were most sensitive to the introduction of digital common cause failures.

This slide happens to describe the mitigating systems that were in the accident sequences for this particular PRA.

But the way we did the sensitivity study was in line with how the guidelines are written. And what our guidelines suggest that you do when you're trying to get insights from your PRA with respect to common cause failure effects is to view digital common cause failures with three factors:

First the individual channel reliability; second the fact that redundant channels can fail due to common cause reasons, and; thirdly to take a look at the existing diversity in the mechanical and electrical systems into which the instrumentation and control is being installed.

It needs to be kept in mind that when we install this instrumentation and control it is controlling an integrated set of mechanical and electrical systems. And those mechanical and electrical systems have their own inherent defense-in-depth and diversity associated with them, and that's probably not going to change as a result of installing instrumentation and control. So there's some clues from how the plant is designed and the defense-in-depth and diversity that already exits in the mechanical and electrical systems as to where defense-in-depth and diversity may be important in the instrumentation and control.

Now to install or to incorporate the effects of digital common cause failure in the PRAs, I'll use this reliability block diagram, the simple reliability block diagram to illustration that.

What I have here is an initiating event, say, a PWR loss of feedwater. Several mitigating systems are available to cope with that event, one of them is aux feedwater, another is safety injection in the pores for feed and bleed purposes. And I can have operator actions to initiate some of these systems in addition to the instrumentation and control.

Now, for an individual system, say the top mitigating system, it has automatic actuation system that may be digitally controlled. And for the purpose of performing my defense-in-depth and diversity analysis using this PRA, I will insert an event, a super component if you will, into the model that would reflect failure of the instrumentation and control from common cause failure effects that wold simultaneously effect both trains.

Now to assign the failure probabilities to that common cause event I would use the defensive measures approach that are in the guideline, first to evaluate what I believe the failure probability would be of a digital channel and then to come up with the common cause failure probability. And the product of those two then would be the value that I would assign to the digital common cause event that would fail both trains of that system.

Now because it is an individual system and because the instrumentation and the control for each train likely gets signals from the same sensors, same signal processing, same voting logic for an individual system the common cause beta factor is likely to be very high. Probably one. And that kind of guidance is provided in the EPRI guideline when we're talking about an individual system.

Now when we start looking at the second system it may also have digital equipment that is not diverse from the first system. In this case we'd be talking about the safety injection system as a means of doing feed and bleed, which is redundant to the aux feedwater system. In that particular case, again, I would insert a common cause factor in between the two system representing digital common cause failure of both the I&C for both systems. And again I would go back to my defensive measures approach to estimate a failure probability for an individual channel and a common cause beta factor.

Now in this case I may be using different instrumentation to actuate the system, different methods of processing the signals, different voting logic. And so the beta factor between two systems may be less than one. But, again, the guideline line provides guidance as to how to determine both the failure probability of a channel as well as the common cause beta factor.

And then towards the bottom of the diagram you'll see an operator action is available to actuate the second mitigating system. If in fact the operator has to use instrumentation and controls that is not diverse from the digital instrumentation and control that actuates the mitigating systems, I will insert into my PRA a common cause beta factor that represents the failure of the operator to be able to take that action.

And then finally between the initiating event and some of the mitigating system, the instrumentation and control may not be diverse. An example of that is the turbine controls and the feedwater system. If they do not happen to be diverse, then I will again for the turbine trip initiating event, I will insert for the feedwater system a common cause beta factor that represents failure of the feedwater system given a turbine trip. And again I will go back to my defensive measures approach in the guideline to determine a failure probability for that common cause beta factor.

So with the super component type approach we install some fairly simple logic into the PRA first to represent digital common cause failures of redundant trains of equipment within systems, redundant systems and operator actions that may actuate those redundant systems as well as between the initiating event and the mitigating systems.

CHAIRMAN APOSTOLAKIS: What is the definition of failure here? Failure to actuate?

MR. BLANCHARD: For the instrumentation and control it would be failure to actuate, yes. Right.

Now, to determine how well we could get insights out of a process like this we performed a series of sensitivity studies. For this particular PWR PRA for all of its accident sequences we didn't happen to have a particular digital I&C design. And so what we did was to perform a series of sensitivity studies to determine where we thought digital defense-in-depth and diversity was a value. In the case of the channel reliability we varied the failure probability of the I&C channels from 10^{-2} per demand down to 10^{-6} per demand. For the common cause beta factor we varied that from all the way from one to zero. And then for how the I&C system was installed in the mitigating systems, we looked at several different designs or architectures.

CHAIRMAN APOSTOLAKIS: Let me understanding here what you're doing.

MR. BLANCHARD: Sure.

CHAIRMAN APOSTOLAKIS: The common cause failure rate is beta times the probability of failure of one channel, right?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: Now when you go to two systems --

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: -- what is one channel?

MR. BLANCHARD: What is one channel?

CHAIRMAN APOSTOLAKIS: Yes.

MR. BLANCHARD: Is the --

CHAIRMAN APOSTOLAKIS: It's the system itself?

MR. BLANCHARD: I'm sorry. I misunderstood the question.

CHAIRMAN APOSTOLAKIS: Let's got to the top then.

Is there a pointer that I can use from here?

For this system you have the two trains.

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: You got a probability of failure of one, which can be varied like this. And you have beta, so beta times that is the probability of the common cause failure for that system, right?

MR. BLANCHARD: Right.

CHAIRMAN APOSTOLAKIS: Right.

MR. BLANCHARD: And recognizing the train is mechanical and electrical --

CHAIRMAN APOSTOLAKIS: I understand. You have to put a microphone on or sit down. Sit down and use your pointer.

Now if when I go to this beta and you have two systems now, right? This beta couples the two systems?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: How do I get the common cause failure rate? Multiple this beta by what?

MR. BLANCHARD: The failure probability of a channel of one of the systems.

CHAIRMAN APOSTOLAKIS: One channel?

MR. BLANCHARD: One channel.

CHAIRMAN APOSTOLAKIS: One of these four channels?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: And these two are identical? These two are identical, so I pick the largest one?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: The largest probability or whatever.

MR. BLANCHARD: They may be similar, yes.

CHAIRMAN APOSTOLAKIS: Yes. Or may be similar.

So it's beta times the probability of failure of this?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: And when I go here I don't understand how I multiple --

MR. BLANCHARD: Well, let's say I am talking about a turbine trip which has a frequency of about one a year. About a quarter of turbine trips turn out to be I&C related.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BLANCHARD: So with a .25 per year initiating event frequency I will find a beta factor that I can associate between the main feedwater system and the turbine controls. If I find there's functional diversity between the sensors used to control the feedwater system and what's used to control the turbine, then I might assign a beta factor of .1 or .01 --

CHAIRMAN APOSTOLAKIS: But what is the rate of common cause failure or coupling of the initiating event and the failure of the system? I mean, you're talking about two different things now. One is a frequency.

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: The other is a probability.

MR. BLANCHARD: The probability would essentially be .1.

CHAIRMAN APOSTOLAKIS: Yes.

MR. BLANCHARD: If I picked a beta factor of .1 for the conditional probability of the feedwater system given my turbine trip due to instrumentation and control.

CHAIRMAN APOSTOLAKIS: So you would go the accident sequence and say .25 --

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: -- a year occurrence of the turbine trip because of malfunction of the instrumentation control and then times -- times what?

MR. BLANCHARD: Point one.

CHAIRMAN APOSTOLAKIS: Times .1 and that's it?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: And the system is out.

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: I see. I see. So the individual probability of the train is not used in this case?

MR. BLANCHARD: It would not be used in this case.

CHAIRMAN APOSTOLAKIS: Because the --

MR. BLANCHARD: Each one of these common cause factors fails the entire system.

CHAIRMAN APOSTOLAKIS: Okay. Okay. Okay.

MR. BLANCHARD: This common cause failure fails these two systems.

CHAIRMAN APOSTOLAKIS: Yes. Okay. So then I can have also a beta that couples this system, this system and they operator action?

MR. BLANCHARD: That's correct.

CHAIRMAN APOSTOLAKIS: And what are the results of all of this?

MR. BLANCHARD: If I can set up the problem, I'll show you the results.

CHAIRMAN APOSTOLAKIS: You can set it up already.

MR. BLANCHARD: All right. I need to set up one more thing.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BLANCHARD: Okay. Besides just looking at changes in the failure probabilities I looked at different I&C architectures. I looked at different levels of defense-in-depth and diversity within the instrumentation and control system itself. As an example, I could assume all these systems were not diverse from each other or the initiator with the exception of one system, perhaps the auxiliary feedwater system. It would have a beta factor of zero in terms of common cause given failure of instrumentation and control on these other systems in that case.

CHAIRMAN APOSTOLAKIS: Are these assumptions on your part? Are you working with a real PRA?

MR. BLANCHARD: I'm working with a real PRA and I'm assuming a plant wide digital upgrade, but I don't happen to have an actual digital system so I'm performing sensitivity studies to decide where in all the accident sequences do I believe defense-in-depth and diversity in the instrumentation and control is of most value.

CHAIRMAN APOSTOLAKIS: I see. And these are sensitivity studies here, right?

MR. BLANCHARD: These are going to be sensitivity studies.

CHAIRMAN APOSTOLAKIS: Is there one of them where it says everything is identical to each other and --

MR. BLANCHARD: I skipped over that one because that's a really bad answer. Yes. I started with --

CHAIRMAN APOSTOLAKIS: You're surprised we're looking for it?

MR. BLANCHARD: Yes, actually I am. They asked me not to mention that one yesterday when --

CHAIRMAN APOSTOLAKIS: So even if I ask you, you will not tell me?

MR. BLANCHARD: Oh, no. I can probably go back and find --

CHAIRMAN APOSTOLAKIS: So what was the probability of the frequency of the accident sequencing if none of these things had defense-in-depth?

MR. BLANCHARD: Oh, I would have to go back and look on the analysis that I did.

CHAIRMAN APOSTOLAKIS: So you're not

telling?

MR. BLANCHARD: Basically it's an frequency of the initiating event.

CHAIRMAN APOSTOLAKIS: No, for the one you analyzed. You have a table in the next slide.

MR. BLANCHARD: Oh, I'll show you. Yes. I'm sorry.

CHAIRMAN APOSTOLAKIS: Yes, let's look at the next slide.

MR. BLANCHARD: I'm sorry. I thought you were asking for the one where everything was not diverse.

CHAIRMAN APOSTOLAKIS: Yes. That's what I'm asking for. The next table doesn't have that on it?

MR. BLANCHARD: The next table does not have that one.

CHAIRMAN APOSTOLAKIS: Right.

MR. BLANCHARD: Right. But basically it's the initiating event frequency.

CHAIRMAN APOSTOLAKIS: Oh, in 25?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: Times .1, perhaps?

MR. BLANCHARD: Well, if you want to assume some diversity between feedwater and -- yes.

CHAIRMAN APOSTOLAKIS: Yes. So in the worst case, worst, worst, worst case --

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: -- I will have a pretty significant sequence?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: And you are arguing that this worst, worst case is not really realistic? That's really what you're arguing, aren't you?

MR. BLANCHARD: That's right. And so left it out of the presentation. But I think we are interested in looking at the imposing diversity on single systems with respect to everything else, and maybe more than one system and then maybe more than one system plus a diverse actuation system for one other system.

CHAIRMAN APOSTOLAKIS: Now when you say diverse actuation system, can you explain it a little bit?

MR. BLANCHARD: Similar to what is required in the ATWAS rule for aux feedwater.

CHAIRMAN APOSTOLAKIS: Yes.

MR. BLANCHARD: Maybe an analog system that's diverse from the digital system.

CHAIRMAN APOSTOLAKIS: But I thought we

couldn't find analog components anymore?

MR. BLANCHARD: Some of the ATWAS systems are very simple and, yes, they are analog. Some of them are analog.

CHAIRMAN APOSTOLAKIS: They are now. But if you want to replace those will you be able to find other analog components? Isn't that one of the prime reasons why we're working on this?

MR. STRINGFELLOW: Yes. This is Jack Stringfellow again.

This is not to say that analog components no longer exist. I mean many of us are currently maintaining our protection systems, our analog protection systems with parts that we -- cards, for example. ASIC cards that were developed for just for the purpose of maintaining those systems. But we have the capability in specific cases to maintain these analog systems, and many of us are doing that.

MR. BLANCHARD: Otherwise you would have to go to a diverse digital system.

CHAIRMAN APOSTOLAKIS: And what would that be?

MR. BLANCHARD: I'm sorry?

CHAIRMAN APOSTOLAKIS: What would that be? A diverse digital systems means what? Different parameter?

MR. BLANCHARD: Different manufacturer, different symptoms, different signals.

CHAIRMAN APOSTOLAKIS: Look at that results now.

MR. BLANCHARD: Okay. All right. Well, one last thing, if you don't mind. What I've done here is essentially build a three dimensional matrix where I'm going to vary all three of these factors and then look at the final core damage frequency to identify which combinations of these factors get me back to a core damage frequency close to what I started with. That was the purpose of these sensitivity studies.

And I will show you the results for two of the initiators. First is loss of feedwater for this PRA. It happens to have a 8 times 10^{-2} per year frequency. It's core damage frequency is five times 10^{-7} per year.

CHAIRMAN APOSTOLAKIS: You meant the contributing of this sequence is five times to minus seven?

MR. BLANCHARD: This is all the sequences associated with loss of feedwater.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BLANCHARD: All of them.

CHAIRMAN APOSTOLAKIS: Yes, that's what I'm saying. This initiator?

MR. BLANCHARD: This initiator, yes.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BLANCHARD: Now I'm just going to show you a slice of three dimensional matrix. It happens to be the slice where I've assumed the probability of a failure of a single channel is 10^{-4} --

CHAIRMAN APOSTOLAKIS: On what basis?

MR. BLANCHARD: Well, my defensive measures will get me to that basis.

CHAIRMAN APOSTOLAKIS: Yes. But one of the slides earlier said that a strict process doesn't necessarily lead to a highly reliable software. That's a result of a very stringent process controlling the process of developing the software, 10^{-4} or --

MR. TOROK: Plus good defensive measures.

I'm sorry. This is Ray Torok.

Yes. It's a good process plus good defensive measures to justify a number in that range.

CHAIRMAN APOSTOLAKIS: Defensive measures on a single channel?

MR. TOROK: Yes.

CHAIRMAN APOSTOLAKIS: Like what?

MR. TOROK: You apply the defensive measures evaluation that Thuy described --

CHAIRMAN APOSTOLAKIS: So that's the process?

MR. TOROK: No. I'm sorry. I understand. When we refer to process, we usually talk about the software development process.

CHAIRMAN APOSTOLAKIS: Okay. So what defensive -- remind me what defensive measures would apply to a single channel.

MR. NGUYEN: This is Thuy.

CHAIRMAN APOSTOLAKIS: Yes.

MR. NGUYEN: For example, cyclic behavior and a very strict identification of all the factors that could take the software out of this cyclic functioning.

CHAIRMAN APOSTOLAKIS: I'm having a problem with that. I mean, come on. We've had, what is it, Appendix B is it, the quality assurance. Yes. That's as stringent as anything and still we've had failures. So there is nothing unique about what you are doing here, is it?

MR. NGUYEN: Oh.

CHAIRMAN APOSTOLAKIS: Oh.

MEMBER KRESS: What's the probability of failure on demand for the analog system that this replaced?

MR. BLANCHARD: Well, as it turns out we have built a small model of the two out of four taken twice system made of relays, contacts and relays.

MEMBER KRESS: Yes.

MR. BLANCHARD: And for a single channel it happens to be right on the order of 10^{-4} --

MEMBER KRESS: That might be a justification to that, because we heard earlier that you could almost assume that the replacement system has a failure probability of at least as good as the analog.

MR. BLANCHARD: It was better than an assumption. We believe we can justify that.

MEMBER KRESS: Right. You believed you could justify that.

CHAIRMAN APOSTOLAKIS: I'm at a loss here. I don't even know whether the beta factor model applies.

MR. BLANCHARD: Whether the --

CHAIRMAN APOSTOLAKIS: Yes. The beta factor model for common cause failures, why would it apply to a system where the common cause failure may be a specification error? I don't know. Does anybody know? And still, the 10^{-4}, I mean there is nothing unique -- wait.

Mr. Nguyen?

MR. NGUYEN: Yes.

CHAIRMAN APOSTOLAKIS: There is unique about the quality control you are putting here because this business from day one has very strange in quality control processes. And yet things fail. So what's so unique about this? You're giving me a metaphor with a circle, that's very illuminating, you know, for educational purposes. But don't tell me that it's 10^{-4} because you do a circle.

MR. NGUYEN: Well, it's -- no. But what I'm saying is that because I'm working a cyclic behavior, I can identify where are the most likely points that could cause failures.

CHAIRMAN APOSTOLAKIS: And why can't I do that with pumps so the pumps will never fail?

MR. NGUYEN: I'm not a mechanical engineer.

CHAIRMAN APOSTOLAKIS: I know.

MR. NGUYEN: So I don't know.

MR. TOROK: Because pumps wear out is a easy answer.

MR. GUARRO: But in the analogy between the analog and digital systems so that was back on -- let's see, I think it was slide 20 there is the statement "The likelihood of specification errors is comparable for equivalent analog and digital systems." I'm personally not convinced that that's true.

CHAIRMAN APOSTOLAKIS: No. I mean, there are so many assumptions in all this.

MR. GUARRO: Because, I mean, I think that the design process or an analog system is quite different from the design process of something that involves software. And having worked both with engineers and software programmers, they behave very differently. So to say that the specification error would be the same, I think that's a big jump in faith.

CHAIRMAN APOSTOLAKIS: And also, I'd like somebody to convince me why the beta factor model applies here.

MR. TOROK: May I offer a couple of clarifications. This is Ray Torok again.

You mentioned the Appendix B quality assurance process. And that is a process that tries to insure that you end up with high quality software. And for software development it would require that certain documents be generated along the way of software requirements specification and a requirements transability matrix and so on, and you do all the right testing on the software. It's all about process for software development. That's not what was Thuy was talking about when he said defensive measures.

Now some of those process elements do constitute defensive measures. But what he's really looking at is the end product and the design attributes that end up built into it.

A good process does not guarantee a good design. It gives you the well documents design, but not a good design.

CHAIRMAN APOSTOLAKIS: I agree. But how do you know the circle?

MR. NGUYEN: This is Thuy again.

CHAIRMAN APOSTOLAKIS: Yes.

MR. NGUYEN: I can give you the example of what I will be doing for the Teleperm XS for EDF's purposes. We have a requirement from Framatome to have the source code and the design documents of the Teleperm XS. And we'll have them in offices for analysis by advanced tools by, I would say, the formal verification methods that exist currently. And, of course--

CHAIRMAN APOSTOLAKIS: You still don't

know the circle.

MR. NGUYEN: Sorry?

CHAIRMAN APOSTOLAKIS: I mean, you are gaining confidence that the thing will not fail in frequency, but you still don't know the circle.

MR. NGUYEN: I know the circle because -- I'm a software engineer. I can understand and read what are the statement, the individual statements that are put in the software programs that command the behavior of the software. That has been the way we have assessed safety particular software since many years now. And that has been -- we have developed and acquired tools to do that.

MR. TOROK: The other point I'd like to make -- this is Ray again. Is that if you're going to pick numbers for failure probabilities and beta factors, and Dave used them in an evaluation. And we're not trying to make claims about what the real failure probabilities are. What we are trying to do is make claims that we can identify the places where a diversity is important, diversity in I&C is important and where it isn't. Where it's more likely to be important. And that's what the risk insights here are about. I don't believe those specific numbers anymore than you do. And if you want to say well 10^{-4}, that's fine, you do it. Do it at 10^{-3}, and Dave's done those sensitivities. And that's really what the exercise is about in generating risk insights.

CHAIRMAN APOSTOLAKIS: But an actuation system, I'm not really difficult to convince that you have a low probability of failure. I mean, all it does is send a signal to start something. But if you go to more advance platforms, I don't believe -- of course I have to think about the beta factor.

First of all, if the individual channel becomes 10^{-2}, now everything goes up by two orders of magnitude, right? So what does that tell you? I don't know what it tells me. It tells me that if I have one diverse system it's 1.6 10^{-3}?

MR. BLANCHARD: If your goal is to keep your core damage frequency where it was before you installed the system and you install a 10^{-2} channel, it says you're going to have to do a lot more in terms of installing other diverse systems or justifying a very low beta factor in order to maintain that core damage frequency.

CHAIRMAN APOSTOLAKIS: Yes. By the way, these numbers on the table refer to all the sequences initiated by loss of feedwater?

MR. BLANCHARD: Yes.

CHAIRMAN APOSTOLAKIS: So if I make the individual channel 10^{-2}, I end up one 1.6 10^{-3}, which is about four orders of magnitude greater than the current. And I still don't know what that tells me. Four orders of magnitude, you know, is a lot.

MR. BLANCHARD: Yes. Well, if it does get you to 1.6 times 10^{-3}, what it says is we have to go--

CHAIRMAN APOSTOLAKIS: With two systems diverse and so on?

MR. BLANCHARD: Yes. We have to go way down on this list of diversity in the instrumentation and control and way over to the right of the chart in terms of the beta factor before we have an acceptable side --

CHAIRMAN APOSTOLAKIS: Why, by the way, have you shaded some of these dark shade?

MEMBER KRESS: The acceptable regions.

MR. BLANCHARD: These are what I am calling acceptional regions.

CHAIRMAN APOSTOLAKIS: Oh, I see.

MR. BLANCHARD: These are core damage frequencies that are close to what I started with.

CHAIRMAN APOSTOLAKIS: To the original. Yes.

MEMBER KRESS: I would have been tempting to put the dark shading on the next round. You got it lightly shaded I noticed.

MR. BLANCHARD: Yes, those were kind of in between numbers where I wasn't quite comfortable.

MEMBER KRESS: Maybe you could have them, maybe not. Yes.

MR. BLANCHARD: And I have 18 initiating events to do this with. And when I get done my change in core damage frequency has to be small for the sum of them.

CHAIRMAN APOSTOLAKIS: Yes.

MR. BLANCHARD: And so that's what the shading is. I could probably live with the slightly shaded areas. But, again, I have to do a lot of work on the other initiating events to make sure they're small.

CHAIRMAN APOSTOLAKIS: Well, there's the whole issue with bringing software into the PRA becomes trivial the moment you are willing to accept the probability of one channel failing is something you can estimate. Then everything, of course, becomes building on manipulations. It's that PDF of 10^{-4} for demand that is a major problem. I mean, I don't know how you get that.

On the other hand the argument that, look, even if I assume -- because let's face, these things are reliable. I mean, it's not that they're failing every other week. Even if I assume a very high number, I still get results that are reasonable, then maybe you have a point. In other words, your philosophical approach I think is pretty good. How reliable do they have to be?

MR. BLANCHARD: And --

CHAIRMAN APOSTOLAKIS: And what?

MR. BLANCHARD: And the conclusion we come to is the channel of digital reliancy need be no more reliable than a similar channel of analog.

CHAIRMAN APOSTOLAKIS: I don't know. Does everyone agree with that? I'm not sure.

MR. MORRIS: If I could speak to the question of the reliability of a single channel?

My name is Pete Morris. I work for Westinghouse. I'm a designer of reactor safety systems.

And if we step back for a moment and think what kind of equipment is being used for these kinds of applications. In the process control industry, not nuclear power but petroleum refineries, pharmaceutical factories, all kinds of applications in the process control field there are numerous vendors of now all computer-based distributed control system.

The safety systems, and for that matter nonsafety systems, that are being used in modern nuclear power plant upgrades are all based on these different existing platforms that have been dedicated for class 1E service.

If there were no nuclear power industry, there is an overwhelming emphasis on the reliable operation of these process control systems for all kinds of things. Product liability is very important to the maker of pharmaceuticals. Public safety related issues for someone in a high energy industry is very important. And the process control industry is demanding that -- or the process control requirements for many industries are demanding that very reliable platforms must be available for all kinds of safety, and I don't mean nuclear safety, but practical everyday public safety anyway. And so by starting with these kinds of system you know that you are getting systems that have basic reliability characteristics that approach or, frankly, even exceed that of the historical analog-based systems of long ago. Because modern safety and liability issues demand that this equipment, that these systems, that these platforms must be that reliable.

CHAIRMAN APOSTOLAKIS: I guess our problem here is not just that they have to be reliable. I mean, we have to be able to demonstrate that one way or another. That's part of the issue here. It's not just -- I mean, again, you know I have no doubt that they're pretty systems. The question is how reliable are they.

What do we do with our time now? Are you near the end or you still --

MR. BLANCHARD: We are approaching the end here. If I could just summarize this slide.

CHAIRMAN APOSTOLAKIS: Yes. Can you do that?

MR. BLANCHARD: Yes. The conclusion w came to with respect to the loss of feedwater initiator is that if I can show that the I&C for two systems are diverse from the control system that may have caused the initiating event, plus either have a diverse actuation system or allow the operator to be able to initiate the systems, then that is sufficient to bring my core damage frequency back close to where it was originally. All right. And that is with a probability failure of 10^4 --

MEMBER KRESS: If you have 18 sequences,

why don't you do divide that number by 18 or by 10?

MR. BLANCHARD: Well, I know that --

MEMBER KRESS: Because these are dominate is what --

MR. BLANCHARD: I happen to know that some of the initiating event frequencies are low to begin with.

MEMBER KRESS: Okay.

MR. BLANCHARD: And I can --

MEMBER KRESS: You have prior knowledge that allows you to say that they're not going to contribute as much as these?

MR. BLANCHARD: Right. But in the end we did all 18 initiating events. We did look at the change in core damage frequency for all 200 sequences, some together --

MEMBER KRESS: Yes. You could make a matrix like this for all 18 of them, that would include all 18 of them.

MR. BLANCHARD: In fact, we did.

MEMBER KRESS: Okay.

MR. BLANCHARD: In fact, we did. And for different values of failure of a channel. And the results were that with multiple mitigating systems diverse from the cause of the initiating event and the ability of the operator to actuate those systems we could get very close to a change in core damage frequency of 10^{-6} per year, even assuming very high beta factors.

MEMBER KRESS: What constitutes a diverse system in your mind? Is that manufactured by a different company or a different programmers or what?

MR. TOROK: Technically, I suppose, you can establish reasonable assurance that they won't be subject to the same common cause failure. So --

MEMBER KRESS: So that's just another way of saying you're diverse.

MR. TOROK: Well, yes. And the real answer is you have to look inside the systems and the applications to make that assumptions. Just because they're from different manufacturers or use different shifts and whatnot is not the whole story. It's not the whole story.

MEMBER KRESS: They have to have some sort of different programming on them.

MR. TOROK: Yes. Well, there need to be -- Thuy, did you want to get your two cents worth in here?

MR. NGUYEN: Yes. I've tried to illustrate defensive measures that would ensure or give a very high assurance that the same platform would not be a significant cause of common cause failures. I know that it's -- I would say, something that is difficult to swallow. But this is what we can see from the history of these platforms which are used quite heavily in other industries.

MR. TOROK: But it comes back to being able to generate an argument and reasonable assurance that they're not subject to the same common cause failures. Now Thuy's saying when you do that you'll find that just because you have the same platform in two different systems doesn't necessarily mean you have a problem. There are other things that you need to look at that are going to be more important. But that's -- you know, it's a different argument. But you come back to reasonable assurance, whatever that takes, to show that there won't be the same common cause failure. That's what it really comes down to.

CHAIRMAN APOSTOLAKIS: Your conclusions?

MR. TOROK: Have we wrapped that up?

MR. BLANCHARD: Finally, for the medium LOCA which we didn't have a chance to talk about. All we needed was high reliability software. What we assumed in terms of diversity among the mitigating system or a beta factor between those systems that were not diverse played very little role in driving the risk of the medium LOCA. We just needed high reliability channel of --

MR. TOROK: You want to contrast BTP-19 and --

MR. BLANCHARD: Do we want to do that?

MR. TOROK: Okay. That's good.

I think we ought to just skip to the conclusions. You've already hit these things.

CHAIRMAN APOSTOLAKIS: You have a conclusions slide?

MR. TOROK: Yes. We can do conclusions real fast.

CHAIRMAN APOSTOLAKIS: Okay.

MR. TOROK: Okay. And the first one just says we believe that now is the time to start looking at factoring risk insights into defense-in-depth and diversity evaluation.

Let's go to the next one without any detail there. The other one is based on what we're seeing in sensitivity studies and so on, we would recommend, make certain recommendations in regards to what NRC is pursuing. And we tried to list that here. We'd say, yes, this is a good area to pursue, reliability of digital equipment, modeling in PRA that's great. However, the first thing here don't start with the general case.

When I sat here in June and one of the Staff presentations on the Research program, there was a list of issues that can effect digital equipment. And it was sort of a general case issues list. And what you find when you look at systems that might really go into safety applications is they're designed in such a way that those issues are irrelevant for them. So I say constrain the problems for starters. Constrain the problem to a realistic system for a safety related application. That's all.

The next thing there is to keep track of where D3 is a value and what levels of reliability you need. I think it's a big advantage to understand what your target is before you try to get to it.

Let's see, the third one, oh yes. Address designed in behaviors, defensive measures. You know, what the system is actually designed to do and ways to look at the product, to evaluate the product because that is more important in determining reliability than the process elements like whether or not you got a software requirements specification.

So we would say find a way to get that into the NRC program. Now, actually some of the presentations in June did touch on that, but the emphasis was going in a different direction as far as I could tell.

The other thing is let's just coordinate with industry to make sure that we cover all the important issues and that we don't duplicate effort anymore than we have to. But I'd say it's certainly an important area to keep working on.

The only other thing I would like to do is thank you very much for letting us take all this time to talk with you about these. And we'd be happy to come back again if you think it would be helpful.

CHAIRMAN APOSTOLAKIS: Thank you very much, gentlemen.

Any questions from the people sitting at the table?

We do appreciate your coming here and explaining this to us. Thank you. And I hope you are taking our comments the way they were intended, in a constructive way.

MR. STRINGFELLOW: I'd just like to say I think we had a very constructive conversation and I really appreciate the depth of the questions and the challenging that we got here today. And we're going to take this back and I hope we can move forward with the review of this document.

Thanks.

CHAIRMAN APOSTOLAKIS: Thank you.

I propose we take ten minutes break and then come back to the NRC presentation.

(Whereupon, at 4:13 p.m. a recess until 4:28 p.m.)

CHAIRMAN APOSTOLAKIS: Okay. We're back to the Staff presentations.

Bill?

MR. KEMPER: Thank you.

Yes, again, I'm Bill Kemper. I'm with my colleague Steve Arndt who will provide most of the presentation.

This discussion will focus on the systems aspects of digital technology, which is Section 3.1 in the Research Plan.

CHAIRMAN APOSTOLAKIS: Yes.

MR. KEMPER: Current issues. As we all know, there is an ever increasing use of digital systems that requires new information and continuous improvements to the NRC review process. Digital systems will take on an ever increasing role in the protection and control systems of nuclear power plants and also fuel facilities, I might add, and even some nonpower production facilities, you know, such as a medical group.

New system challenges will continue to emerge. For example, tin whiskers has become an issue with us. Also INC instrumentation and control. Circuit board aging has been a somewhat long issues that we're dealing with, not only here but across the world as well as to digital safety systems. So this Research program will assist the Staff to develop a fundamental understanding of how digital technologies are used in safety systems and, again, develop review guidance, tools, review procedures and training to the staff to support NRC Staff reviews and evaluation of the systems.

Now this next slide is an overview of the various components of this area. We're going to talk about environmental stresses in detail in just a little bit. I believe that's next on the agenda. Ms. Christina Antonescu will talk about that. And so we'll give you a brief overview of the rest of these systems, the COTS digital safety systems, effective total harmonic distortion on digital systems compared to diversity and defense-in-depth, least ways what we believe we intend to do from a research environment in that area. Systems communications, power distribution system interfaces with nuclear facilities and finally operating systems.

So, with that I'll turn it over to Steve to provide an overview of each of these sections.

CHAIRMAN APOSTOLAKIS: So there are two presentations? One by Steven and one by Christina.

MR. KEMPER: Yes.

CHAIRMAN APOSTOLAKIS: Okay.

MR. KEMPER: Yes. This one is scheduled to go until -- well, it's scheduled to last an hour. We'll try to get through it quicker than that if we can.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: Yes. What we thought we'd do is go over very quickly all the different programs in this program area. And in keeping with the recommendations of the Subcommittee at our last meeting, we're going to talk in more detail about the ongoing program and give you some results that you can understand.

CHAIRMAN APOSTOLAKIS: Good.

MR. ARNDT: And that's why the environmental stressors is highlighted in green. That's of these programs, that's the only ongoing program we have. The rest of these will be started in the future. Of the ones here, I will tell you when we plan to start the work. The diversity and defense-in-depth program is the next one to be started. That will be started this year.

MR. KEMPER: Oh, and I did want to highlight one thing, George. You asked a question earlier today about the priority. In the Research Plan back in section Table 4 there actually is a priority assigned to each one of these in terms if high, medium, low. Okay.

CHAIRMAN APOSTOLAKIS: Thank you.

MR. KEMPER: And that supports the schedule, the associated schedule for the projects.

CHAIRMAN APOSTOLAKIS: Is the rational given, too, or just -- it's performance based. We've just got the result?

MR. KEMPER: It relates to the strategic goals, the objectives and goals of the strategic plan of the agency.

CHAIRMAN APOSTOLAKIS: I'll make sure I read that. Thank you.

MR. ARNDT: Also before we go forward I also want to highlight a couple of issues. Bill mentioned that the program plan is not just an NRR program plan, it's an agency program plan. Some of the areas are more emphasis on reactor issues. For example, the defense-in-depth issue is a specific reactor issue. But particularly in this section a lot of these issues apply equally to field fabrication facilities that have distributed control systems, issues about individual components in a medical -- a radiator and things like that for the operating system that's in the THD and things like that are applicable in many cases to nonpower reactor applications that we're interested in.

CHAIRMAN APOSTOLAKIS: That will be useful.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: We'll come back it.

MR. ARNDT: Okay. The systems aspect is a set of projects that follow this category primarily because they effect the system as a whole from either internal or external factors, but are broad scoped. So they're things like environmental stressors, the interactions with the digital systems with the rest of the support systems in the plant like power supplies and things like that. The issue of operating systems and systems architecture which are not specific to a particular component but are generic across a system. And, of course, the issues we're facing with the use of COTS and things like that. So that's how this particular group got grouped together.

CHAIRMAN APOSTOLAKIS: By the way, let's go back to this. Isn't the identification or the failure modes of software part of the system aspects?

MR. ARNDT: Yes, but that's really a crosscutting issue. That's something that we have to deal with in all the different programs.

CHAIRMAN APOSTOLAKIS: So where will it be handled?

MR. KEMPER: Well, we have a section Software Quality Assurance. And that's where that's treated. That's where we're dealing with that.

CHAIRMAN APOSTOLAKIS: Really?

MR. KEMPER: Yes, I believe it is. What is that?

MR. ARNDT: 3.2

MR. KEMPER: 3.2. Yes, we talked about that at the last meeting as well.

MR. ARNDT: So the research is, and this similar to slides you've seen before, designed to look at improving the fundamental understanding of the digital technology, understanding their strengths, weaknesses, limitation, capabilities. Identifying what technical information is needed by the reviewers in developing more quantitative review criteria where possible. Improving the licensing technologies, the tools, the methodologies and acceptance criteria.

So in many cases, and actually most cases, we already have a process by which to review these systems. But either because of their ever increasing complexity or because we want to do it better based on newer information, we have research programs in these areas.

I'm going to hit this very, very briefly because we're going to have a full presentation on this program, but this program is basically looking at how the systems are maintained in the expected environment. What are the issues associated with EMI, with lightening, the environment in which they exist? And as we mentioned earlier, Christina will have a full section on that.

The systems communication issue, this was discussed in detail this morning, but what we're really looking at is the safety aspects associated with how the systems communications are put together. The internal and external architectures, the protocols both proprietary and off-the-shelf protocols; what makes a good safety system and what are the particular aspects of communications and protocols that we need to work at. So the idea is to look at these systems, the complexity, and understand what that is.

CHAIRMAN APOSTOLAKIS: Now if what we are talking about is actuation systems --

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: -- systems that actuation signals, how relevant is all this? In other words, by just listening to what you are saying one gets the impression that you're talking in very general terms, general software systems. And I think the EPRI guys also said something to that effect. And I remember that, you know, when that Academy work came out there were a lot of debates behind it and all that. And one argument by the industry was that the systems you're talking about are extremely simple. They're not talking about controlling the space shuttle where you have continuous feedback and control and all that. So a lot of these general findings and, you know, communication and this and that, may not apply to the simpler systems that an industry is thinking of employing.

Like actuation systems, do I really have to worry about communications and all that? What do they communicate?

MR. ARNDT: Okay. There is both an issue

with what you said and a lot of truth in what you said. When you talk about general, general you're exactly correct. When you talk about the fact that there are lots and lots of different protocols out there, there's lots and lots of different software communication, the hardware communication bus configurations and like that; you're absolutely correct. That is not something that we are particularly concerned about.

The kinds of systems that we regulate, safety systems, and the kinds of systems that we're interested in, nonsafety systems that are used in actual nuclear power plants or could be in the future, are the things that we're most interested in and we're trying to direct our research toward. So in that case what you're saying is correct. The research needs to be focused on those kinds of things that could have direct implications on our regulated systems or those systems that are important to safety from a risk standpoint.

CHAIRMAN APOSTOLAKIS: And not expected to be implemented in the next several years

MR. ARNDT: Are either currently being used.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: Or currently being proposed or some reason to believe --

CHAIRMAN APOSTOLAKIS: Or in the near term?

MR. ARNDT: -- will get into a plant.

CHAIRMAN APOSTOLAKIS: Yes.

MR. KEMPER: And if you'll recall that diagram that we went over this morning during the security program, we illustrated where some of those interchannel communications were being deployed in systems that were being proposed to us for safety system applications.

So you know we have specific reg guide guidelines. Regulatory requirements, excuse me, that require separation and deal with communications. But this research will explore that to ensure that we fully appreciate the ramifications of this communication protocols and establish review criteria, again, that the Staff can use in reviewing and accepting these types of applications.

MR. WATERMAN: This is Mike Waterman, Research.

Anytime you have data moving from one point to another you've got yourself a network by definition. And the way you move that data is by using some kind of a protocol, be it SINEC L2 or something like that.

The issue that arose with me when I was trying to review was is I really didn't have acceptance criteria for what features of SINEC L2 protocol were good features and which features ought the developer to stay away from. And what I envisioned off of looking at these various protocols was to come with guidance for the Staff so that when they were looking at a digital system such as that complicated diagram that we kept referring to this morning, the reviewer would be able to look at that and say okay, they're using SINEC L2. Let's dig in to how they're using it to make sure that they're only using those features of SINEC L2 that are safe. And we don't have any guidance for that right now, but the TSX system has a pretty complicated network structure. They have an AMD K6 E2 microprocessor. That's a 266 megahertz microprocessor just to do the communications.

So, you know, these systems need to be reviewed. And right now our criteria for what protocols are good and bad is sort of vague and it depends on whoever is reviewing it and what they know about protocols. So we're trying to develop some more definitive information for the reviewer to use when he's doing a safety evaluation.

I guess that was the point --

CHAIRMAN APOSTOLAKIS: Okay. Okay. Let's go on.

MR. ARNDT: Let me rephrase that just slightly before we go on. The issue is, as I said, very general we're not that interested in because of the application issues. But the simplicity issue is something that we really need to be looking at now. Because we're not just talking about simple ladder logic anymore. There's a lot of fairly complicated implementations of these trip functions and basic control functions because of the kinds of issues that Mike just pointed out.

MEMBER SIEBER: Let me ask probably a too simple question. GDC 24 talks about separation between protection and control. The way I read that it doesn't necessarily say that you can't use a single processors for both functions.

MR. ARNDT: That is a -- Bill, you want to--

MEMBER SIEBER: Can you or can't you?

MR. KEMPER: I'm sorry?

MEMBER SIEBER: Can you or must you use

separate CPUs between control systems and protection systems?

MR. KEMPER: Between the control system and protection system?

MEMBER SIEBER: Yes. Can you run it all through the same box?

MR. KEMPER: Well, typically you don't have a control system and a protection system in the same box. Typically they're not commingled, okay? Just from a design strategy.

MEMBER SIEBER: Yes. The question is is it outlawed? GDC 24 when I read it really doesn't tell me that.

MR. KEMPER: Well, GDC 24 is specified as a separation criteria, right, applicable to --

MEMBER SIEBER: Right. And it looks like more transducers and cutout switches and stuff like that.

MR. KEMPER: Right. Yes. That's the idea so that faults are not promulgated, obviously, from one channel to the other.

MEMBER SIEBER: Right.

MR. KEMPER: Communication strategies, though, are different and the task here is to make sure that the communication strategies don't interfere with the electrical separation that's required by GDC 24. So that's what we're trying to do here is evaluate various means that the vendors are using for communications between channels and understand the ramifications of that. And, as we said, develop acceptance criteria ourselves or if we find problems, maybe establish some coping strategies on how to deal with that.

Did that answer your question?

MEMBER SIEBER: No.

MR. KEMPER: I'm not sure I did.

MEMBER SIEBER: No, it didn't. It leads me to another question. From one channel to another do you need separate CPUs?

MR. KEMPER: Yes.

MEMBER SIEBER: Are they truly independent or not?

MR. KEMPER: Yes. Yes, they typically are, right. Each channel is typically implemented by its own separate CPU.

MEMBER SIEBER: Okay.

MR. KEMPER: It's own box is separation.

MEMBER SIEBER: And "typically" means not always or is there a regulation, a standard or a requirement that says this is the way it's got to be?

MR. KEMPER: Well, to comply with the separation requirements of GDC 24 it has to be that way. At least, I don't know of any way to skin that cat, put more than one channel into one box.

MEMBER SIEBER: That's the way I look at it. CPUs are cheap.

MR. KEMPER: Well, safety related CPUs, though, are not quite so cheap actually.

MEMBER SIEBER: They're more expensive?

MR. KEMPER: Yes.

MR. ARNDT: Paul?

MR. LOESER: Yes. I'm Paul Loeser. I'm with NRR.

In your questions the safety system cannot be commingled with the control system. They have to have a number of degrees of separation as specified in 6308, the one that was talked about earlier where you break it down into blocks where you have functional diversity, equipment diversity, programming diversity, language diversity. And if someone tried to use the same, for example, Intel microprocessor, a 486, for both systems, we would then have to do a fairly intricate diversity and defense-in-depth analysis to see if they were adequately diverse that they could be considered not subject to the same common mode failure or not.

MEMBER SIEBER: Okay. That answers the question.

MR. LOESER: As far as the channels themselves being separate, two channels in the same system may be exactly identical but have to be physically different. They use the same process and the same software, but they have to be separated.

MEMBER SIEBER: Okay.

MR. LOESER: We run into problems when people start putting multiple safety functions on the same four channels. And then you have to, again, do a diversity and defense-in-depth analysis to see if you do have a particular kind of accident and combined with that you have a common mode failure under the provisions of branch technical position 19 do you still have enough defense considering this is considered beyond design basis, to adequately cope.

MEMBER SIEBER: Okay.

MR. LOESER: But those things are taken into consideration when we do our reviews.

MEMBER SIEBER: That answers my question. Thank you.

MR. KEMPER: Dr. Sieber, with regard to your question about a control system and a safety system on the same microprocessor, there's nothing that specifically prohibits that. And indeed, we ran into that question when we were doing Draft Guide 1130 which will eventually become the NUREG Guide 1.152.

At first we had a regulatory position in there that said you couldn't do it because there was no barrier that would separate the two. And then somebody from the public mentioned well you could run a safety system on the safe protected mode of a microprocessor and run your control system in the nonprotected mode. And that would be an adequate barrier, to which I guess we conceded that that was a possibility.

So you could conceivably do it on the same microprocessor even though, you know, it's --

MEMBER SIEBER: Yes, that's sort of the way I read it. And I could picture people trying to jam everything into minimum amount of hardware.

MR. KEMPER: At the risk of cutting off conversation, we need to kind of --

CHAIRMAN APOSTOLAKIS: Can you tell me the GDC was again, Jack.

MEMBER SIEBER: Twenty-four. It's on page 23 of the plan.

MR. ARNDT: Yes. Right.

So basically what we're trying to do is understand and develop the issues and the procedures and policies and acceptance criteria for these particular kinds of issues. Use communication systems that are most likely to be used for the safety functions, the failures in areas that we're interested in and these kind of issues. And develop realistic ways of doing these kinds of analysis. This project is currently scheduled to start in '07.

As we've heard several times today COTS systems are a continuing challenge for us. They're being used extensively in the retrofit and there are both issues associated with the dedication of the systems and how they're interconnected and things like that.

Licensees typically qualify COTS systems for nuclear applications through a combination of special tests and inspections, supplier surveys, source verification and performance history. We then do a qualitative review of their dedication.

This project, which is going to start on '07, is designed to try and improve that review process. Make it easier, more quantitative, look at the tools that are out there to assess these systems in a box kind of way. Look at issues like model checking, statistical testing these kinds of things and understand what is adequate, what level of information do you need, what kind of samples do you need to take. Do you do a thread audit? If you do a thread audit, how many threads do you have to look at? Try and get better more efficient process for the review of these systems.

Okay. The next two projects look at the issues associated with the electrical power for digital systems. In the plan you'll read a couple of LER examples of challenges we've had to the operation of digital systems due to intermediate power, loss of power, voltage fluctuations and things like that that digital systems behaved differently than the analog systems that they replaced.

CHAIRMAN APOSTOLAKIS: Yes, they did.

MR. ARNDT: And there's been a number of examples of these. So we really want to look at these issues and see whether or not they're going to be a problem. There's been some anecdotal experience that says that there may be some problems. So we want to look at the systems, understand the systems, develop methods to analyze these systems and determine whether or not we need to look at them harder when we do the reviews.

Again, this is a relatively low priority but it's scheduled to start in '08. Okay.

The next project is a project on a similar line but looking at a different aspect. Digital systems, particularly some of the newer high density digital systems are very sensitive to power quality, particularly issues like zero crossing and things like that, timing issues associated with nuclear power quality. As the systems become more and more dependent on the low voltage memory states, high Cs densities this is something we really want to look at.

One of the interesting --

CHAIRMAN APOSTOLAKIS: I --

MR. ARNDT: Go ahead.

CHAIRMAN APOSTOLAKIS: Go ahead. Go ahead.

MR. ARNDT: One of the interesting aspects, of course, is that this is not just switching power supplies and things like this. This is everything downstream of the power supplies. And one of the big issues is nonlinear loads. Well, one of the things that's a nonlinear load is digital systems themselves. So for relatively simple systems it's not a big deal. But when you start loading down a power supply with a lot of nonlinear loads like digital systems, you can actually end up with serious issues associated with nonlinear loads.

So the research will look at what's currently out there, what's being developed. There's a new IEEE standard 519 that looks at this particular kinds of issue. Again, try to develop methodologies and acceptance criteria, what are the important characteristics and what should we be directing the reviews to look like.

CHAIRMAN APOSTOLAKIS: Now, again, one of the issues that has been raised over and over again is what will be the specific contributions of each of these projects that can be used by the agency groups that are actually making decisions?

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: And one of the questions before you answer that question is how is the agency handling this issue now? Okay. Because we've heard there's a Chapter 7 -- is this issue of THD handled in some way now?

MR. ARNDT: There is a power quality requirement, and I don't remember the specific area in Chapter 7. Maybe my NRR colleagues can refresh my memory. But support system type issues are reviewed.

CHAIRMAN APOSTOLAKIS: Are reviewed or are not?

MR. ARNDT: Are part of the review.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: Paul?

MR. LOESER: Paul Loeser from NRR again.

Yes, this is an issue now and has been for some time. We have some requirements. For example, we only allow a five percent total harmonic distortion under worse case and items like this. The problem we're beginning to see is that as voltages drop we're now getting into 2.4 volt circuitry whereas in the past it was also 5 volts. Some of it's getting to 1.6 and .8 volt. The line thicknesses are getting much thinner. The loads are getting much greater on the items.

So while we're handling now with exiting equipment, we're worried that in the future the rules we have in effect may not hold and we need some research or some guidance from somebody to tell us what kind of rules should we have for the future.

CHAIRMAN APOSTOLAKIS: Bill, I really think that statements of this type should find their way into the plan. I think it will strengthen it so much. and I urge you when you come before the full Committee in November to do that as much as you can.

MR. KEMPER: Okay.

CHAIRMAN APOSTOLAKIS: I realize it's only, what, two or three weeks back and you have to have your 15 reviews if you change anything. But it's so important. I mean, judging from past experience with other research plans, most notably the human factors research plan that this Committee reviewed a few years ago, what the members want to see is that kind of motivation. They don't want to see -- I mean this is not the National Science Foundation. We are not trying to advance science for its own sake. We have a regulatory objective. So by citing things like that in all projects ideal even, you know --

MR. KEMPER: Right.

CHAIRMAN APOSTOLAKIS: -- within reason, I think it's going to go a long way towards convincing people that this is a solid research plan.

So please in the presentation, I mean we're going to discuss this tomorrow again. But the presentation in my view, this is one of the most critical aspects.

Both of you have thought about it already. I mean, it's not that it's new to you. It's just that some criteria hasn't found its way in the written documents and the slides. Because every time I ask the question, there is an answer.

MR. KEMPER: Well, if you'll notice the last three tick bodies embody really the issues that Paul just spoke to. He just gave it a much more passionate and heartfelt description --

CHAIRMAN APOSTOLAKIS: Put it in -- he gave it a different spin.

MR. KEMPER: And you're absolutely right. Because that's why we're doing this is to support NRR and our stakeholders.

CHAIRMAN APOSTOLAKIS: Right.

MR. KEMPER: You know, we're not doing research for the sake of just doing research.

So good comment. I agree with you.

CHAIRMAN APOSTOLAKIS: Yes. So let's make sure that this is one of the top priorities in preparing for the full Committee meeting. Because, as you know, the letter will be written then.

MR. KEMPER: Right. Right.

CHAIRMAN APOSTOLAKIS: It's very important to be sensitive.

Okay, Steve.

MR. ARNDT: Yes. And I want to point out one other thing. At the bottom of all these I basically say when the project is going to kick off, if it hasn't already. And one of the things we're trying to do in a very proactive way because we've been less than successful in the past, is for all the new programs we've got the general outline of what the issue is and what we're trying to solve and how we're basically planning on doing it in the research program plan. But the real details will be developed in the statement of work of the program for either in-house work or contract work. And that's going to be done in conjunction with our stakeholders, be it NRR, NMSS or whatever.

Operating systems. I'm going to go through this reasonably quickly, even though it's a very complicated issue. And this is an area where it's really a multiple stakeholder issues. There's issues for operating systems in materials, issues in medical devices and fuel fabrication issues in the plant systems, both the safety systems and nonsafety systems. So this is one of the ones that is pretty broad based.

As we've been talking. The systems are a lot more complex now than they were in the early days. In the day of the National Academy study many systems didn't have operating systems. They were very simple systems. That's much less so today.

In most cases we can get access to the operating system. Hardware less so in the COTS environment. So understanding the characteristics of systems and what potential problems with the characteristics of the system become more and more an issue as we have less information in COTS space. And we really have to understand how this works.

We've looked at this in the past and we think we need to do more work in this area.

So this program, which is also starting in '08 depending on input from other stakeholders it may get pushed up, but it depends. Right now it's scheduled for '08. We're really looking at issues associated with best practices and failure modes. Try and understand what is an acceptable review standard for these systems. And also looking at what tools are available out there and what the fidelity of the tools are. For example, if the licensee comes in and says we really really looked at our operating system, we understand it, it's not a problem. We've used these tools, we've used this kind of assessment methodology.

As Thuy pointed out earlier, there are methodologies out there to look at reliability and availability of these kinds of systems. But until you've looked at that it's very hard to give any real credit to those kinds of systems. So we really need to understand the characteristics of operating these systems and how do you validate them, how do you understand they really are performing properly? So that's really what this project is all about.

And now for everyone's favorite issue. As we told you in June, we have a very extensive research program in the area of risk of digital systems and how do you model them and what's in the important modeling characteristics and things like that. And we won't go into that in detail here because we've already talked about it in other places and I don't want to digress anymore than I have to. But the other part of that is how good is our current deterministic process?

As EPRI mentioned earlier in the day, there's a lot of issues associated with whether or not that process which was developed a number of years ago is a good process. Now it's a process we have and there's nothing wrong with it. We haven't licensed anything that is not going to be sufficiently diverse. But there's a lot of issues that are being raised by the nuclear industry. So one of the things we want to do is understand whether or not this is the current state of the art for deterministic analysis of defense-in-depth.

So basically what we're proposing to do is perform some case studies and look at the way the deterministic analysis is laid out in 6303. Review the risk insights, both our own risk insights and EPRI's risk insights and verify from a deterministic standpoint whether or not this is the best we can do.

So that's the primary aspect of this. And as I mentioned, this project is going to start later this year.

MR. KEMPER: Yes. For example, a licensee right now has an application that NRR is reviewing that they propose to a certain strategy for their design configuration with regard to diversity and defense-in-depth. That's kind of the baseline. That's where we're starting from because we don't have any other specific case studies, if you will, that we can draw from to make judgments, if you will, and provide that feedback to the licensee. So we're thinking for at least the generically qualified platforms it would be good to perform these studies and come up with some numbers ourselves. You know, or some conclusions ourself which what's the best fit, if you will, from a topology an a design strategy of these I&C systems for various safety applications.

MR. GUARRO: Just trying to understand. Is essentially the intent to identify the improvements to the deterministic approach that would seem to satisfy some risk-informed criteria as well. Because you've mentioned risk, so I'm' trying to understand what the connection is.

MR. ARNDT: The objective of this is simply that last bullet there, to verify from a deterministic standpoint the existing criteria is the best we can do in a deterministic space.

The bullet above that is basically just to learn from whatever information is out there, both what the licensees have submitted, what's been done in foreign applications and what if any information is available from risk insights. Things that people have looked at, things that people have done that will help us understanding whether or not the deterministic --

MR. GUARRO: Some of the objections that we have heard are based on risk considerations of some sort.

MR. ARNDT: Right.

MR. GUARRO: So trying to figure out if that fits into the formulation of some other or improved deterministic formula.

MR. ARNDT: As I stated a few minutes ago, we haven't kicked this off so we don't have the exact details yet. But the idea is simply to look at everything that's out there that we are aware of that we're knowledgeable about to try and understand if what we're currently doing is the best we can do in deterministic space.

So, for example, looking at the EPRI study. They've pointed out that there are some issues that may not be covered in a bounding Chapter 15 type analysis. That's something that we want to know if we're going to look at whether or not this is the best deterministic way of doing the deterministic analysis. If not capturing something that's important or if we are worrying about things that are not important from a deterministic standpoint, then we want to look and see whether or not we can do better. That's truly the point of having that there.

MR. KEMPER: Let me just try to run through a case study for example just off the top of my head.

A licensee could propose to deploy the same hardware throughout his plant, primary and secondary. Okay. If you assume common mode failures of that equipment and then you run the thermal hydraulic analysis using best estimate calculations per BTP-19 -- we intend to go look at the effects of plants in a deterministic role. Now it was not written from a probabilistic perspective because that's the program that we have right now to deal with. You could choose a different strategy. You could choose to combine the RPS and the ESFAS. You could choose to combine the RPS, ESFAS and your post monitoring system. Any number. You know, you can just pick them. And the idea is we want to run through a few of those case studies and see if we can establish for ourself what is the best fit in terms of a design philosophy for using the same microprocessors, for using the same software, that sort of thing.

MR. ARNDT: The other, if you go up one tick mark, one of the real issues here is in 6303 there's a set of rules associated with how you put together blocks, how you put together coping strategies and things like that. When we review this, we've got to make some assumptions about how that makes sense and the licensee has got to make some characteristics. You put a line around this block, you put a line around that block. But one of the things we want to do is as Bill just mentioned is do some case studies. Do it ourselves to understand what makes sense and what doesn't make sense so we can have a definitive technical basis to go back and say no, you really can't do that because if you do that, you run into problems. And we're not willing to accept that.

CHAIRMAN APOSTOLAKIS: Okay. Let's move on.

MR. ARNDT: Okay. So those were the programs that were highlighted in the research program plan.

CHAIRMAN APOSTOLAKIS: Very good.

MR. ARNDT: As Bill mentioned, as things change we get requests for additional programs from NRR, MNSS, they'll get thrown into the budget prioritization process and they may bubble to the top. But that's currently where we are on those issues. And we will continue to work these programs in conjunction with our colleagues in MNSS and NRR to try and get --

CHAIRMAN APOSTOLAKIS: Very good.

MR. ARNDT: -- the best product for our customers.

MR. KEMPER: Okay. We'll we're getting close to being back on track. All right.

Okay. Christina Antonescu is going to provide a presentation of environmental stressors, as we promised earlier, Section 3.1.1.

CHAIRMAN APOSTOLAKIS: Now, Christina, you have something that's against you before you even sit down. It's 5:10 after a long day and you have 27 slides.

MS. ANTONESCU: No, they are backup.

CHAIRMAN APOSTOLAKIS: What, 20 of them are backups?

MS. ANTONESCU: Yes.

MEMBER SIEBER: Yes, there's only one real slide.

MS. ANTONESCU: Only 18 I believe are--

CHAIRMAN APOSTOLAKIS: Can you be nice?

MS. ANTONESCU: I will be nice.

MEMBER BONACA: You should be nice to her and tell her we like what you do, and then she'll be nice to us.

CHAIRMAN APOSTOLAKIS: And then we'll be done in a minute, huh?

MEMBER BONACA: Right.

MS. ANTONESCU: All right.

CHAIRMAN APOSTOLAKIS: This is a very unusual color for the heading. I mean that's nice.

Go ahead.

MS. ANTONESCU: So my name is Christina Antonescu. I've been working in the I&C group for the last 15 years. And I would like to discuss with you today the status of our research on environmental stressors and the impact on instrumentation and control technology.

I have with me Richard Wood from Oak Ridge National Lab. He has been principal investigator for our projects on environmental stresses. He has a background in the nuclear engineering and he has over 20 years experience with the -- power plant.

And contributing on the discussion, I also have Paul Ewing, he's somewhere in the back from Oak Ridge National Lab. He is a principal investigator for our electromagnetic compatibility and lightning protection projects. His background is electrical engineering. He has 25 years experience with EMC radio frequency transmission.

So our research on the environmental stressors it's currently addressing three main topics. The lightning protection one. The Committee recently reviewed DG-1137 on lightning protection, so I will not repeat the details of the guide in this presentation. But it was presented to ACRS on July 6th of this year and reviewed by the ACRS in July. And we're ready to issue the draft guide as a final guide by the end of this year sometime as Reg. Guide 1.204.

The second main topic on environmental stressors is the environmental compatibility for mild environments. DG-1077 was developed in response to a user need from NRR. And the need for DG-1077 is to provide an all in one roadmap for acceptable practices for the applicant. Previously the reg guide on mild environment qualification was distributed among several documents. So the Committee has seen and approved DG-1077 before, but its release was delayed to allow the revised IEEE standard to be reviewed and to address some scope consideration which is focused on mild environment rather than harsh and mild environment.

So I will discuss the status of the DG-1077 in my presentation.

And the third main topic is the electromagnetic compatibility. And EPRI has requested that NRR consider relaxation of the text limit for series 114 because it is substantially higher than the limit in certain frequency ranges. So the reasons for the higher limit in Reg. Guide 1.180 and past versions of the EPRI guide is that some plant measurements taken by EPRI were very high. And EPRI had committed to bound those measurements with its susceptibility limits, but now suggests that it's analysis of the measurement was flawed. So my presentation will describe the issue on what has been done so far.

So as stated, the Committee has seen the DG-1077 before, however it's release was delayed to permit updating endorsement of the most recent standard and to enhance the guidance by sharpening its focus.

DG-1077 was presented in February of 2003. ACRS approved it for release and the final effective guide was granted --

CHAIRMAN APOSTOLAKIS: What does that mean, "final effective guide?" That's new terminology to me.

MS. ANTONESCU: The final guide was granted or --

CHAIRMAN APOSTOLAKIS: So we approved it and now you guys say no we're not going to publish it, we're going to go back and do some more work?

MS. ANTONESCU: Yes. And I'm going to let you know what the reason is. One of the reasons is to permit updated endorsement of IEEE standards 323, which was released in 2003. And then we just -- the scope of it was also changed from mild and harsh to mild only.

CHAIRMAN APOSTOLAKIS: Okay.

MS. ANTONESCU: However, following the ACRS review of DG-1077 NUGEQ, that's the Nuclear Utility Group on Equipment Qualification, requested that the pending update of IEEE 323 be considered for endorsement. So that's the 2003 version.

So in response finalization of DG-1077 was delayed so that the standard could be reviewed. And IEEE 323 was released on September 11, 2003. A review was conducted by our office with the help of Oak Ridge. And DG-1077 has been revised and is now DG-1142.

So because of the scope reduction of this DG-1077 we plan to release it for public comment again. And it will be designed as DG-1142. For simplicity I'll refer to it as DG-1077 in my presentation.

So IEEE 323-2003 is very similar to IEEE 323-1983. The primary difference involves practices for hash environment qualification. Provisions were added to IEEE 323-2003 to allow condition monitoring to be used to support on-going qualification. Changes were made to address previous NRC objections, in particular of dual transient as part of the DBA test profile. And some wording changes were introduced to add clarity, but in some cases they have introduced or exacerbated some issues regarding harsh environment qualification.

So the guidance on documentation for mild environment remains the same in both versions. And is consistent with regulatory practice.

The qualification practices in 323-2003 are appropriate for mild environments with some clarification conditions which I'm going to cover in a few minutes. And the technical basis for endorsing IEC 60780 remains ineffective and are equivalent to the practices in IEEE 32-2003. But with reduced scope of DG-1077 which limits the endorsement to mild environment application only.

So endorsement of both standards is limited now for mild environment for safety related computer-based I&C systems.

So let me remind you what DG-1077 is. What does it do? It endorses qualification practices in 323-2003 and IEC 60780 as acceptable for application to safety related computer-based I&C systems located in mild environments.

And where does it apply? It applies for new and modified --

CHAIRMAN APOSTOLAKIS: Excuse me, did I miss, but what is a mild environment?

MR. WOOD: This is Richard Wood.

It's an environment that does not have a design basis accident condition. So for harsh environments there's a substantial change under an accident condition. For a mild environment, the environment doesn't change substantially under the normal or abnormal conditions.

MEMBER SIEBER: It presumes that it is in the containment during a LOCA?

MR. WOOD: Yes.

MEMBER SIEBER: So you have pressure temperature radiation spray, chemical spray.

MS. ANTONESCU: EQ would be --

CHAIRMAN APOSTOLAKIS: That's mild?

MEMBER SIEBER: That's harsh.

CHAIRMAN APOSTOLAKIS: Oh, harsh.

MS. ANTONESCU: Harsh.

MEMBER SIEBER: Mild is like in here.

MR. WOOD: Normal operation.

CHAIRMAN APOSTOLAKIS: Less than that.

MS. ANTONESCU: Harsh would have to be -- the qualified language has to be established for DBA.

CHAIRMAN APOSTOLAKIS: Okay.

MS. ANTONESCU: So where does it apply? I already said that.

What does it provide? It addresses unique characteristics of computer-based I&C systems as well as acceptable evidence for mild environment qualification.

What has changed in DG-1077? The revision of the draft guide involves endorsing, again, the updated IEEE standard in 2003 and also the current international standard.

The regulatory revise scope and provides pointers to guidance on key related issues.

And the reduced scope to focus specifically on mild environment qualification of computer-based I&C systems. Thus since the revised DG-1077 only applies to mild environment qualification of computer-based I&C system, the standards are only endorsed for mild environment application by this guide. As a result, all previous positions related to harsh environment qualification were deleted and replaced by position to point to Reg. Guide 1.89 which is for harsh environment as the prevailing guidance on qualification on those environments.

So it was determined that harsh environment qualification should remain the exclusive domain of Reg. Guide 1.89.

So because of the revision we proposed

that the guide be released for another round of public comments.

MEMBER SIEBER: Did you ask us to review it before you released it?

MS. ANTONESCU: We will.

MEMBER SIEBER: Okay.

MS. ANTONESCU: That's our intent.

MR. KEMPER: That's coming. That's the next step.

MEMBER SIEBER: Okay.

MR. KEMPER: We're going to send it to NRR and let them review it and the next step will --

CHAIRMAN APOSTOLAKIS: That's you, right?

MR. KEMPER: Yes. Bill Kemper.

MEMBER SIEBER: Yes.

MS. ANTONESCU: So what are the position of DG-1077? We have covered its endorsement of standards, so now let's look at the enhancement exceptions.

DG-1077 provides one enhancement to IEEE 323-2003 and IEC 60780 to address unique characteristics of microprocessors. And the enhancement is for computer that must be functioning or the software has to be executing while being tested.

The second, the system level effects must be considered as a whole, and then test as parts and confirm no acceptable cumulative effects. So that what I mean is use analysis to supplement testing.

And the exception, we don't have enough the exception -- at least one exception that we are looking at is that enough documented evidence must be available to show qualification. So we're taking exception to clause 7.1. And 7.1 says that very little evidence of qualification needs to be documented for mild environments. And we're taking exception to that, and that's why we're consistent now with clause 7.2, which specifies full documentation of qualification processes including test plans and results. This documented evidence necessary for the Staff to adequately confirm that the functioning complex computer system is in fact qualified for the environment in which it was operated.

So the pointers, there are two pointers that we have. And one is to Reg. Guide 1.180 on my guidance that we'd retained from our previous revisions. And another pointer to Reg. Guide 1.89 on harsh environment qualification guidance. And this replaces all previous harsh environments qualification position in DG-1077. We just point now everything to

Reg. Guide 1.89.

Now I'm going to look at the last topic on electromagnetic compatibility and change the subject.

The industry response to NRC on its regulatory guidance on EMC nuclear power plant has been generally positive. Regulatory guidance on EMC began with review and acceptance of EPRI TR-2323 with stipulation in an SER in 1996. Reg. Guide 1.180 was released in 2000 and recognized the SER and its acceptance of TR-2323. Then Reg. Guide 1.180 was updated in 2003 to incorporate changes in the acceptable EMI/RFI practices. TR-2323 has been updated over the years, but these updates have not been endorsed by NRC since similar practices are included in Reg. Guide 1.180.

So the industry response to regulatory guidance on EMC has been generally positive. However, there is one significant issue that concerns the industry, and that is CS114 operating envelope and the feeling that it's too harsh. So I'm going to tell you the problems from EPRI's point of view.

EPRI has requested that NRC review CS114 operating envelope in Reg. Guide 1.180 Rev. 1 because the envelope was based on EPRI's planned measurements and the measurements were flawed. CS114 is a high frequency conducted susceptibility test and it has proven problematic for nearly all equipment tested to date. And very few pieces of the equipment have passed the test without being redesigned. This is a very harsh test.

So CS114 operating envelope in Reg. Guide 1.180 actually incorporated plant data obtained from EPRI and now EPRI says its measurement and the original analysis of plant data were flawed.

So EPRI says that CS114 is a continuous wave test and its operating envelope should be based on continuous wave data, not the transient data. And we do have separate power surge susceptibility testing for that, which is IEEE 662.41.

So it then follows that CS114 operating envelope in Reg. Guide 1.180 Rev. 1 is subsequently flawed. The result is that EPRI wants to see the operating envelope changed.

So to explain where we are, I'm just going to give you some background.

EPRI collected its conducted emission data in 1994 in seven plants and it captured power transients. So the subsequent EPRI data profile then showed high conducted emission levels in the plant.

So Research was only infrequently allowed to make limited conducted emission measurements in plants because of their intrusive nature and our data profile showed lower levels. Because of the limited measurements our data had a high degree of measurement uncertainty.

And how does this effect Reg. Guide 1.180? We incorporated the EPRI data into a development of our CS114 operating envelope. We started with operating envelope for the military ground facility in 461D and then addressed it to incorporate EPRI plant data so that we could be consistent with the SER based on EPRI's TR-102323 guide. Our goal was to ensure that safety related equipment could withstand ambient conducted emission in plants, and we assumed that EPRI data was relevant. And we have documented the technical basis in NUREG/CR-6431.

So of course EPRI is now revising its data collection analysis rationale and they are now saying their conducted emission data should not have included captured power transients because we have a separate test for that. Because they're addressed by power surge susceptibility testing IEEE C62.41 and C62.45. Their argument is that CS114 operating envelope was not intended to be tested on conducted emission measurements, but rather should be based on a radiated emission environment. And this is to say that radiated emissions will couple onto signal and power leads and interference with the normal operation of the piece of the equipment. Hence, EPRI is saying that the original rationale was flawed and the SER operating envelope based on 102323 was then also flawed.

And I'm illustrating visually what the issue is. And we have here a comparison of the operating envelope for Reg. Guide 1.180 Rev. 1 and EPRI TR-102323 and Rev. 3.

The NRC operating envelope is shown in red. The EPRI envelope that have been accepted in Rev. 0 are shown dark green. And the EPRI operating envelope that they are recommending is showing blue.

So note that the power and signal operating envelope is the same for 102323. This is based on EPRI's assumption that the radiated emissions will couple onto both power and signal leads in the same manner. Thus, the operating envelope should not be different.

Also note that Rev. 2 EPRI envelopes are shown in black and actually separate the power and signal lead envelopes.

Also you can see that the Reg. Guide and

EPRI Rev. 2 envelopes for power leads are very similar.

So the problem area that we're looking at is this triangle shown in light green. For most equipment on this is the frequency range below -- where the existing operating envelopes have problem to be stringent and hard to pass.

So in summary, we have agreed to look into EPRI's request and we have reviewed the information received from EPRI regarding the CS114 operating envelope and in the TR-102323 guide. And we are now investigating the rationale for EPRI CS114 operating envelope and if justified, will develop a revised position on CS114 operating envelope.

So we will update the Reg. Guide based on the results of the investigation and the revised position.

MEMBER SIEBER: Are you planning to get more data or are you going to use EPRI's data?

MS. ANTONESCU: If necessary. I'm not sure. Depending on how we're going to -- what we're going to find out or what our rationale will be or what we need to justify.

MR. WOOD: The real issue is whether or not the argument that's presented is a compelling technical argument. If not, then it may require some more measurements.

MEMBER SIEBER: But you aren't really contesting the data that became available at plants? It's how it's applied?

MR. WOOD: We haven't had an opportunity to look at the details of the EPRI data. So we're not contesting their argument. What we're trying to do is figure out whether their argument fully explains all the potential sources.

MEMBER SIEBER: Okay. They're contesting, your arguing?

MR. WOOD: Well, they're contesting their previous argument.

MS. ANTONESCU: Because we have to take theirs --

MEMBER SIEBER: If you have to argue, it's best to argue with yourself.

MR. WOOD: I think so.

CHAIRMAN APOSTOLAKIS: Any other comments or questions from people at the table?

Thank you Christina and Richard.

MEMBER SIEBER: Okay.

CHAIRMAN APOSTOLAKIS: Appreciate it. We'll see you tomorrow, Christina, I suppose.

MS. ANTONESCU: Yes, see you tomorrow.

CHAIRMAN APOSTOLAKIS: With few slides.

MS. ANTONESCU: Fewer slides. All right. I'll try to shorten tonight.

MEMBER SIEBER: This was actually very good. This was very good.

MS. ANTONESCU: Thank you.

CHAIRMAN APOSTOLAKIS: You raise expectations by showing the backup slides, then you use a topical list.

MS. ANTONESCU: Thank you.

CHAIRMAN APOSTOLAKIS: That was a good move.

MS. ANTONESCU: Thank you.

CHAIRMAN APOSTOLAKIS: Okay. As I said earlier, judging from the experiences we've had with the human factors research plan where the developers had to come back two or three times to us, and also from some of the comments that we've heard here in the last two or three meetings, a separate meeting, it is extremely important to show how a research plan -- what's the rationale. How it relates to what we are doing already and why do we need something new, you know, to supplement or compliment or improve on what we're doing already.

Every time I asked a question, you guys have been answering. So you have thought about it. But what has not happened is that that kind of argument is not in the plan and in your presentations usually you ignore it. So what I think you should do is really focus on it and make a big deal out of it when you come back in November. Because we'll write -- the letter will be, as I understand it, on the plan not on individual projects even though you guys described a lot of them. We'll wait for that for the future after you have reasonable progress.

So as I was thinking about this last night, because I do think that there's a lot of good stuff in the plan, I was trying to think how can one show what you are doing and how what you are doing fits in the bigger picture. And the bigger picture that came to my mind was the reactor oversight process.

Now, I want to say up front what follows is not something that you must do. We are not recommending that you do it. We ourselves, you know, are not sure that everything there is on solid ground. But it's a thought.

This diagram, by the way, do you have it in front of you or can you look it?

MR. KEMPER: We can look at it. Yes.

CHAIRMAN APOSTOLAKIS: Well, you can have copies. It's over there. They may want to take notes.

MR. KEMPER: We have a copy here.

CHAIRMAN APOSTOLAKIS: Yes. Mike, you have a copy?

So the diagram was of tremendous value to the people who developed the reactor oversight process because they were able to communicate to the world at large, in fact, what the agency cares about. So here is some thought.

The overall mission of the agency is the top box. Public health and safety. And I put as a result of severe nuclear reactor operation with different color in parenthesis because you probably had to drop that because you are adding now an NMSS. The strategic performance areas were reactor safety, radiation safety workers, safeguards and then I put in purple there NMSS.

Now the cornerstones are exactly the same from the reactor oversight process. Now the purpose of those is really to see, to help you communicate to the reader or the viewer or the reviewer what kinds of systems you're talking about and what parts of the broader picture they're effecting. You will need some cornerstones for the NMSS, I guess, and the safeguards I'm not sure how much you can put there. But, again, this is their idea. In fact, some of my colleagues have doubts that even the cornerstones for reactor safety are appropriate in your case.

So the message here is don't take this literally, okay. Don't take it literally all by -- you know, he said mitigating systems, I have to have something on there. No, no, it's the idea.

Then under each one, and I think this comes really from the questions that have been raised, let's say I'm giving as an example the mitigating systems cornerstone, okay? But you can have arrows going to barrier integrity and so on. What is the function and the unique characteristics of the system that we are dealing with in this project, this particular 6.5.3.2? As an example, what was said today. It's just a simple actuation system. That's important to know that you are dealing with a simple actuation system and not trying to control the area.

How is the agency reviewing it now? What is the current state of the art, in other words, or the practice? Are we reviewing them? Are we approving these things, disapproving and so on.

The third bullet -- again, even these

bullets should be subject to revision and so on. Why do you want to change it? I mean, you know, you remember several months ago Mr. Calvert told and we are happy with what we have. Well, if you are happy, then why are we spending money doing anything, you know. Today we got different responses from the NRR representative. Okay. Every time I ask why you want to do that -- I forget your name. I'm sorry.

MR. LOESER: Paul Loeser.

CHAIRMAN APOSTOLAKIS: Paul stood up and said for such-and-such a reason and made perfect sense to me. That kind of thing would be nice to communicate.

Then the heart of the matter, and that was really the fourth bullet is what killed the human factors plan several times. If you are successful in project X, how are you going to change the present situation? Are you going to shorten the review time and make it more efficient? Are you going to enhance it and bring in more staff and make it more effective? Are you anticipating what's going to happen, as we said today, so you want to be prepared and understand it better? Can you be a little bit specific in other words. You know, this is really what we expect.

Now the last bullet was -- I'm not sure

that I could do that either. Would there be any metrics for the previous staff? I find that very difficult to do many times, most of the time. But just in case.

But this again gives you the thrust of the thing. I mean for each project you answer these or similar questions and place them in the context of a bigger picture, then it seems to me we are really well on our way.

And then at the bottom, of course, the cost cutting issues that you guys have a lot of. And that's fine. You can say, look, what we're doing here will effect, you know, detecting that an initiating event has occurred. At the same time we will look at the mitigating system. In fact, the beta factor example from EPRI was one example of that. You know, you have a loss of feedwater flow and then the argument was that 25 percent of the time it's the turban, and that may be coupled with the mitigating, the safety system. Great. Okay. So we're doing this project and we're affecting that.

I don't know. Is wireless technology primarily related to emergency preparedness? Could be, huh. I don't know about barrier integrity. But that helps the reviewer understand a little better what we're talking about and where.

MEMBER SIEBER: Part of this work is already done. If you look at page 125 there's a lot of pages like that. You already have which supported strategies are for each project. They're already listed.

MR. ARNDT: Yes. And some of that --

CHAIRMAN APOSTOLAKIS: If I under the impression that you guys had not even thought about it, I wouldn't raise it. Because I know you can't do this in three weeks.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: But I know you have done it. It's just that you haven't documented it in a way that other people can appreciate that you've done it.

MR. ARNDT: Yes.

MR. KEMPER: Well, if I could -- Bill Kemper here.

The supportive strategies, though, again, is out of the strategic plan.

MEMBER SIEBER: Right.

MR. KEMPER: It's not a one-one mapping that you can do to the IOP. But this is just a different way of slicing the agency's mission.

CHAIRMAN APOSTOLAKIS: I'm sorry. Jack.

MEMBER SIEBER: I think the most important thing is that fourth bullet.

CHAIRMAN APOSTOLAKIS: Yes.

MEMBER SIEBER: There's the direction of the agency and here's how these programs fit in.

MR. ARNDT: Right. Okay. And that's a very good comment. And we can certainly do that in most, maybe not all, but most of the cases.

CHAIRMAN APOSTOLAKIS: Okay. But especially in the presentation

MR. ARNDT: Right. Some of our programs are quite -- are individual technology focused. How do we get ready or do we do a better job of reviewing a particular piece of hardware or piece of software. And many of them are crosscutting type issues. How do you model --

CHAIRMAN APOSTOLAKIS: But when you see a better job, you must have something in your mind.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Why do you need to do a better job? I mean, in what sense? Do we need to understand it better?

MR. ARNDT: Yes. And there's a set of things that we hope to accomplish, and that's what you want us to articulate better?

CHAIRMAN APOSTOLAKIS: And in many of these you are very explicit.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: This project will result in tools as follows: A, B, C, D. That's great.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: In other places you're not so explicit.

MR. ARNDT: Right. In some cases we simply didn't articulate as well as we can. Some cases we don't know --

CHAIRMAN APOSTOLAKIS: Well, this is a document that is evolving.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: I mean, this is just an extra thought to help you --

MR. ARNDT: And I appreciate that.

CHAIRMAN APOSTOLAKIS: -- communicate better what you have already done in my view.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: Most of the time, anyway, you have done it.

MR. ARNDT: Okay. Let me ask another question that will hopefully help the presentation.

We're scheduled, I think, an hour and a half --

CHAIRMAN APOSTOLAKIS: On what?

MR. ARNDT: Next --

MR. KEMPER: November.

MR. ARNDT: -- November.

MEMBER SIEBER: The full Committee.

MR. ARNDT: We can structure that anyway that you think is going to be best for the Committee. Obviously, there's some things we want to say. One way we can do it is to review very quickly like I did for environmental stressors this afternoon all the programs. That may not be the most effective use of time.

CHAIRMAN APOSTOLAKIS: In my view it is not.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: I would structure it around something like this. Here's the big picture, we have six areas right around. This is how they fit into this.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: You know, this is the way it's being done now. We need to better a job because of A, B, C, D and here is what we're offering.

Now to go over all the projects will probably -- I don't know. It's over kill.

MR. ARNDT: Yes.

MR. KEMPER: We've already done that anyway. In May that's what we did, right? That's why we're here.

MEMBER BONACA: But you have those tables, you know, in page 11 with all your programs, etcetera, so you have really logical step.

MR. ARNDT: Sure. We can structure it in that way and then maybe use a couple of examples

CHAIRMAN APOSTOLAKIS: Absolutely.

MR. ARNDT: That go to particular issues.

MEMBER BONACA: Because you do have a series of tables with all the --

CHAIRMAN APOSTOLAKIS: And don't hesitate. You know, this morning I noticed -- was it the morning, or whatever? That -- and I appreciate that. I mean, you really don't want to criticize what your colleagues of NRR are doing now and say we need to do this because you're not doing right. But at the same time to say that what we're doing now is fine and excellent and we're spending a million dollars to improve it, I mean -- so it's okay. I mean, it's the state of the art. How are we doing it now? Maybe we are doing it overly conservative because that's what you do if you're a regulatory, right?

MR. ARNDT: Right. Well, and it's --

CHAIRMAN APOSTOLAKIS: But I think the fundamental thing that this is a new technology, new failure modes and we're all as a community trying to understand it is a very powerful argument in my view.

MR. ARNDT: Yes. And it also has the virtue of being true.

CHAIRMAN APOSTOLAKIS: Which sometimes helps in my estimation.

MEMBER BONACA: You know one thing that certainly struck me was well we were discussing common mode failure, you know, because we're left to question in our mind. And then I saw the table that you developed, which is the events that took place.

MR. ARNDT: Right.

MEMBER BONACA: You know, to me is one of the most convincing arguments. Here are the facts that whatever the estimation is going to be right now, etcetera, there are issues that we have to deal with in advance out there in the field that have been cropping up.

MR. ARNDT: Yes.

MEMBER BONACA: And that in and of itself to me is justification for work, in a goal sense of course. And I'm saying that which you can address also the examples, of not giving examples to us, but I think that gives justification to the plan.

I would like to add one thing that, you know, that I am in general am quite impressed with the plan because here we are now, you know, performing our review of the RES research plan and here we're scheduled to develop one. And I wish there was a document like this for every area we're looking at. And there isn't.

MR. ARNDT: Well, you're partially responsible for it because as you recall the first version of this was as a answer to the mass recommendations that were part of this Committee's--

MR. KEMPER: But thank you. We appreciate your help on that.

MEMBER BONACA: I think it's a good base to start it and I think it's going to help you through the next few years very years.

MR. KEMPER: Well, we've put a fair amount of effort trying to vet this with our stakeholders. You know, since we first met in May, quite honestly. And I think it's a much better product now as a result of that than it was when we started out four or five months ago.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: Jack?

MEMBER SIEBER: I'm curious about one thing. Will you prepare the research plan in such detail? Obviously you have to think about it. Did it actually in preparing the plan change your conception of what it is you should be doing or did you already have fixed in your mind I'm going to do these things, all I have to do is write it down?

MR. ARNDT: It's a little bit of both.

MEMBER SIEBER: Okay. I sort of sensed that.

MR. KEMPER: It's an iterative process.

MR. ARNDT: It's very much an interactive process. Because we get -- and I'll mention this a little bit tomorrow morning when I talk about the emerging technology section. But part of the process of planning, particularly out year planning, is figuring out where we want to be.

MEMBER SIEBER: RighT.

MR. ARNDT: And that involves polling our stakeholders, talking to ourselves, looking at the research that's out there and all the other areas. Some of us are involved in proposal reviews for DOE and other areas. So you get a lot of different things and you work through the issues. And some of them come up as we look through the data and issues and things like that.

And as unpleasant as putting one together one of these things is, it's kind of useful to do it every few years simply to force yourself to do that kind of thinking.

As you know, we did our first one, this is the second version. We're planning now in the future to do yearly updates, which is a little less resource intensive.

MEMBER SIEBER: Yes.

MR. ARNDT: But also having that continual update both in terms of prioritization what's important to do sooner rather than later as well as what are the hot issues and things like that. You need, to misuse an old adage, it doesn't do you a lot of good to look under the street light when you realize the wall across the street. But actually in point of fact, it's important to look under the street light the things that you know are important, it's also important to look outside there the things you don't know that are important and keep searching and figuring out what may be coming down the pike.

MEMBER SIEBER: Yes. It seems to me that this plan compared to the last plan is more practical.

MR. ARNDT: Yes.

MEMBER SIEBER: And is driven more toward real needs.

MR. ARNDT: Yes.

MEMBER SIEBER: As opposed to this broad research.

MR. ARNDT: Right. And that's been an evolutionary process dealing with and working with our stakeholders.

MEMBER SIEBER: Well, to me it's a good trend.

MR. ARNDT: Yes.

MEMBER SIEBER: I like it.

MR. KEMPER: Thank you.

MR. ARNDT: It has a specific intent.

MR. KEMPER: That's on purpose. That's not an accident.

MEMBER BONACA: The one thing that I add, again the issues of operating experience. I mean there is experience that is there I'm sure has been pulled together theorizing certain events and whatever specifics they're interested to, the some that are common cause some may be other things. And, you know, to the degree to which that information can be provided, even in research important to this measure, as an introduction, as a history, I think it's helpful. I mean, certainly it would be helpful probably to the whole Committee if you had synopsis of it, you know, sometime in the presentation. This is not talking about hypothetical situations. We have had events.

CHAIRMAN APOSTOLAKIS: Tom, do you want to say anything?

MEMBER KRESS: No. I agree.

CHAIRMAN APOSTOLAKIS: And we're meeting tomorrow.

MR. ARNDT: And we welcome input after the meeting, too.

MR. KEMPER: No. But this has been very helpful and, please, let's continue to talk any ideas you get. Because quite honestly, I've been kind of scratching my head trying to figure out what do we need to talk to you all about in November --

CHAIRMAN APOSTOLAKIS: Scratching you're head trying to figure out why does the ACRS have such a bad reputation? We're such nice people.

MR. KEMPER: Well, we've spent so much time in front of you --

CHAIRMAN APOSTOLAKIS: Undeserved. Undeserved.

MR. KEMPER: We've so much time.

CHAIRMAN APOSTOLAKIS: A lot of it is unfair.

MR. KEMPER: You're right. It's unfair. But anyway, we still have to live with it.

CHAIRMAN APOSTOLAKIS: And in fact, I was telling Eric earlier it seems that, you know, the magnitude of this and the interest in the kind of work you guys are doing, we'll probably have to continue these Subcommittee meetings, especially as you start producing stuff.

MR. KEMPER: Absolutely.

CHAIRMAN APOSTOLAKIS: Because this is a big project, very important and we are all trying to learn here what is going on.

MR. KEMPER: Right.

MR. ARNDT: And that's actually one thing not necessarily in the letter, but informally we would be very interested in which areas you would be most interested in hearing from us.

CHAIRMAN APOSTOLAKIS: Well, you know my area.

MR. ARNDT: Yes.

MR. ARNDT: Now seriously for scheduling purposes it helps us a lot. But we're always happy to come and talk to folks like you.

CHAIRMAN APOSTOLAKIS: Any other comments from our colleagues here?

MR. WATERMAN: This is Waterman.

The other thing I see in the research plan since I bought so much into it is you talk about the plan growing. One of the things I'd like to see the plan start doing is as we finish those projects up, we start a new section in that plan that gives a synopsis of the products we developed. So when somebody picks it up and says they can look at one plan and see where were you, where are you and what are you going to do all in one document. So that document is going to continue to grow as new projects get added in at the front and as the completed projects get added in down at the bottom so you can say well this is what they intended to and well, this is what came out of that.

CHAIRMAN APOSTOLAKIS: And another thing for the major items here, one for example being how to bring all this stuff into PRA, I would strongly recommend that you don't come here at the very end of the project. It would be better to brief the Committee or the Subcommittee at least, as those milestones are reached, so you get some feedback.

MR. ARNDT: Absolutely.

CHAIRMAN APOSTOLAKIS: And possibly valuable advise.

MR. ARNDT: Right. Right.

CHAIRMAN APOSTOLAKIS: All right. I think we've had enough for today. Thank you, gentlemen and lady. And we shall see you again in the morning at 8:30.

(Whereupon, at 5:52 p.m. the meeting was adjourned.)