Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards Subcommittee on Digital Instrumentation and Control Systems
Docket Number:	(not applicable)
Location:	Rockville, Maryland
Date:	Wednesday, April 18, 2007

Work Order No.: NRC-1527 Pages 1-307

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

\+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

\+ + + + +

SUBCOMMITTEE ON DIGITAL INSTRUMENTATION

AND CONTROL SYSTEMS

\+ + + + +

WEDNESDAY,

APRIL 18, 2007

\+ + + + +

ROCKVILLE, MARYLAND

\+ + + + +

The meeting was convened in Room T-2B3 of Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Dr. George E. Apostolakis, Chairman, presiding.

MEMBERS PRESENT:

GEORGE E. APOSTOLAKIS Chairman
THOMAS KRESS ACRS Member
OTTO L. MAYNARD ACRS Member
SAID ABDEL-KHALIK ACRS Member

NRC STAFF PRESENT:

STEVE ARNDT
ALLEN BRADLEY
CLIFF DOUTT
GENE EAGLE
ALAN HOWE
IAN JUNG
MICHAEL JUNGE
BILL KEMPER
ALAN KURITZKY
PAUL LOESSER
MIKE MAYFIELD
MIKE WATERMAN

ALSO PRESENT:

TUNC ALDEMIR
BOB ENZINNA
SERGIO GUARRO
KIMBERLY KEITHLINE
ALEX MARION
GERARDO MARTINEZ-GURIDI
RICK ROTA
JEFF STONE
RAY TORRECK
RICHARD WOOD

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

(8:30 a.m.)

CHAIRMAN APOSTOLAKIS: The meeting will now come to order. This is a meeting of the Digital Instrumentation and Control Systems Subcommittee. I'm George Apostolakis, Chairman of the Subcommittee.

ACRS members in attendance are Said Abdel-Khalik, Tom Kress, and Otto Maynard. Gary Hammer of the ACRS staff is the Designated Federal Official for this meeting.

The purpose of this meeting is to discuss NRC staff and industry activities for digital instrumentation and control systems. We will hear presentations from the NRC's Offices of Nuclear Regulatory Research and Nuclear Reactor Regulation. We will also hear a presentation from the Nuclear Energy Institute.

The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee.

The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in the Federal Register. We have received no written comments or requests for time to make oral statements from members of the public regarding today's meeting.

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

We will now proceed with the meeting and I call upon Mr. Mayfield of the Office of New Reactors to begin.

MR. MAYFIELD: Thank you, Mr. Chairman.

We just wanted to spend a couple of minutes to start this off and provide the Subcommittee a little bit of information about how we got where we are and what we are trying to accomplish.

There was a November 8th, 2006 meeting where the staff made a presentation to the Commission -- the staff as well as the industry. Coming out of that Commission meeting was a Staff's Requirements Memorandum directing the staff to establish an NRC project plan with specific milestones and deliverables with both short- and long-term milestones. And to address the critical path short-term actions.

The staff established the NRC Digital I&C Steering Committee. The Executive Director for Operations issued a memorandum in January of this year. Jack Grobe from NRR chairs the Steering Committee. Unfortunately Mr. Grobe could not be with us this morning so he asked me to sit in for him. I'm much better looking than he is so we went that direction rather than to some of my colleagues who are also on the Steering Committee.

CHAIR APOSTOLAKIS: And who are also good looking.

MR. MAYFIELD: Pardon me?

CHAIR APOSTOLAKIS: And are also good looking.

MR. MAYFIELD: Well, I won't go that far. But the other members of the Steering Committee are Mark Cunningham, representing the Office of Research, Joe Gitter, representing NMSS, and Scott Morris, representing INSR.

We have had three public meetings with our industry counterparts. The first was December 21st of 2006. We met again in January. And then again in March of this year.

We have had multiple internal Steering

Committee meetings and have evolved into six task working groups that represent cyber-security, diversity and defense-in-depth, highly integrated control rooms in terms of human factors, highly integrated control rooms in terms of communications within the control room, risk-informed issues for digital I&C, and the digital I&C licensing process.

We have drafted some project plans and problem statements for each of those task working groups. Those have been shared with the industry and publicly to solicit industry comment and feedback. We will finalize those problem statements and the associated work plans in the near future.

We will be briefing the Commission on the status of this program in June. And we are also hosting an IAEA technical meeting in June on diversity and defense-in-depth. This promises to be a fairly large meeting.

Mark Cunningham and Bill Kemper are the leads on it. And so if any of you are interested, we would certainly invite you to participate. We've had good support from NEI, EPRI, as well as DOE in organizing that meeting.

MEMBER KRESS: Do you know the dates?

MR. MAYFIELD: Well I should but I don't.

MR. KEMPER: Sorry, this is Bill Kemper. June the 19th through the 21st here in the D.C. Metro area. I believe out in Rockville actually -- in Bethesda, excuse me.

MR. MAYFIELD: Okay. With that, Mr. Chairman, I would, I guess, turn it back to you.

CHAIR APOSTOLAKIS: Yes, our next presentation is from NEI, Mr. Alex Marion, who is a new presenter for the Committee.

MR. MARION: Good morning. My name is Alex Marion. I'm the Executive Director of Nuclear Operations and Engineering at NEI. With me is Kimberly Keithline, Senior Project Manager in the Engineering Group at NEI.

I just want to make a couple of comments with regard to what Mike Mayfield said about the establishment of the Steering Committee and development of the project plan for licensing digital I&C applications. We're really pleased with the effort thus far.

We would have liked to have the project plan in place six months ago but the industry and the NRC is working very effectively. And we're hoping that we can use this as a protocol for future interactions on some of the more challenging regulatory issues that both the industry and the NRC have to deal with.

With regard to the project plan that was recently made public, we intend to provide comments to the NRC next week.

MS. KEITHLINE: This is Kimberly Keithline. By the 25th, April 25th.

MR. MARION: Okay. And we have industry participation on each of the task working groups that Mike Mayfield identified. And those activities are going well.

There are two groups -- two of the task working groups that aren't as developed or haven't gone as far as the others. And they are in human factors and digital PRA. And we'll have some comments about digital PRA this afternoon. The human factors group is meeting today so hopefully they will better define the problem statements and milestones and near-term deliverables.

CHAIR APOSTOLAKIS: Excuse me, Alex. The Steering Committee consists of NRC people only, right?

MR. MARION: Yes.

CHAIR APOSTOLAKIS: And they have a --

MR. MARION: And they have public meeting with the industry -- there have been three meetings thus far.

With regard to diversity and defense-in-depth, the task working group is using a deterministic approach in addressing the issues with regard to those concepts. We're okay with that in terms of a process and how to address the issues that need to be identified so that we are confident with the appropriate level of diversity and defense-in-depth in the design of digital systems.

We need to stay focused and we are working on a screening approach but it is very important that this set of issues regarding diversity and defense-in-depth be resolved as soon as possible because it is fundamental to the design of these systems and we go forward. And it is extremely important for both new plants as well as the current operating fleet.

Branch technical position was recently revised. And we recognize the staff was on a highly expeditious schedule to finalize that document and release it to the public.

There are additional comments that we have on that document and we intend to work very closely with the task working group to address those comment. And hopefully make some additional changes to that branch technical position.

The problem statements that have been identified by this particular working group are adequate and sufficient from the industry position and we are prepared to work with the staff in addressing and completing the milestones that have been identified.

There are two items that need to be addressed as we go forward on resolving diversity and defense-in-depth issues. One is where do you need it? And how much of it do you need? And by the latter point, how much diversity and defense-in-depth is necessary to meet the standard of reasonable assurance? And that is something that we are going to focus on in our interactions with the staff going forward.

Hopefully as the result of the presentations this morning with regard to diversity and defense-in-depth, we'll get a reasonably good idea of where the staff is focused.

We intend to develop technical papers on the issues that have been developed. We have already agreed to develop one on manual operator actions and the timing aspect. And we are also going to be developing one on digital components and their susceptibility to common-cause failures.

We are continuing to look for opportunities to collaborate with the Office of Research. We are focused clearly on collaborating in those areas where there is a practical value-added proposition to the results of the research in terms of advancing the state of knowledge of the technology or addressing issues that need to be addressed so that the licensing of these systems can go forward for new plants as well as current plants.

We have also agreed to do pilot applications of some of the fundamental design concepts. One of the plants has agreed to work closely with the NRC on the reactor protector system digital upgrade. And we're looking forward to the interactions. We're looking forward to the briefings that you will hear from the staff today.

We may have a comment or two at the end of the morning session so if time allows, I'd like to have the opportunity to comment on the subject matter that the NRC staff presents. And that is all we have to say about that first topic.

CHAIR APOSTOLAKIS: The technical papers that you mentioned, these will propose specific ways of checking for the need for defense-in-depth and diversity or what will they do?

MS. KEITHLINE: This is --

CHAIR APOSTOLAKIS: Yes, okay, go ahead.

MS. KEITHLINE: This is Kimberly Keithline. One of the papers that we have specifically discussed is related to developing a process by which you could determine what to assume. What would be a reasonable assumption for operator response times just as they relate to your diversity and defense-in-depth evaluation.

We recognize that the NRC staff has a lot of work and they are in the process now of trying to hire people so that we felt that if there are recommendations that we can make or proposals for approaches to resolve some of these issues, that may help the resolution along.

It will be, of course, up to them to decide whether they want to accept any of our recommendations. But that is one specific one would be to recommend a process by which we could determine acceptable operator response -- acceptable from the standpoint of are they reasonable? Are they best estimate? Can they really be used in the diversity and defense-in-depth evaluation?

CHAIR APOSTOLAKIS: Well, it is my impression that branch technical position as it is now is fairly general. One could do a lot of things under it to demonstrate adequacy. And also it's using an approach that was described in a NUREG from 1994.

I'm wondering whether the industry is planning to propose specific methods that have been developed more recently in the last 13 years or so to actually address the two questions that Mr. Marion raised.

And I was -- you know after I saw this 1994, I just went to a website or a couple of journals. And my goodness, I mean there are so many papers that have come out. I mean there is a lot of work going on in Taiwan using simulators, evaluating the -- in fact, their first reference is the BTP. So the NRC says this. Let's do it. And they went to simulators and they evaluated the potential for various common-cause failures.

So I'm wondering whether there is anything in those methods -- not necessarily this particular one but people have done a lot of thinking that could be used.

MS. KEITHLINE: Right. And I think Mike Waterman will probably tell you that as part of the current research that NRC is doing, they are looking at what has been done, what is being done outside --

well, outside of our U.S. nuclear industry and outside maybe of the nuclear industry to try to build on what has been done in this area.

CHAIR APOSTOLAKIS: But the industry is not planning to do anything along these lines. So you don't know yet.

MR. MARION: Well, no -- yes, this is Alex Marion. As Kimberly indicated, the NRC is doing some work in this area and I believe we'll hear details from Mike today.

We have international participation in EPRI. And EPRI is doing a lot of technical work for us in this particular area. And they are receiving input from some of those international members in terms of what they have done in implementing this technology.

I don't know if Ray wants to add any further detail. This is Ray Torreck.

MR. TORRECK: I'm Ray Torreck from EPRI. Yes, we've been working in this area for a number of years now for both deterministic approaches and risk-informed approaches. And we will -- we are applying some of that in working with NEI now. So we're continuing to incorporate insights from that work as appropriate.

CHAIR APOSTOLAKIS: Incorporating insights into where?

MR. TORRECK: Into like the white papers that Kimberly mentioned that we will be preparing for NEI and so on. So we will factor that in.

MS. KEITHLINE: Ray, I should probably point out there are also two aspects or we could divide the diversity and defense-in-depth issue into two parts. One would be the as purely-deterministic-as-one-can-be approach, which is the subject of this morning's discussions. And then another would be applying risk insights or risk informing even to take it to maybe an extreme the diversity and defense-in-depth evaluation process.

EPRI has done some work that may be very applicable, especially in that second category with using risk insights and risk informing. And that will be more related to this afternoon's discussion.

MEMBER KRESS: When you say deterministic system, you are referring to the application strictly in design basis accidents and using the well-known concepts of conservatisms and specifications.

MS. KEITHLINE: Right.

MEMBER KRESS: That's what you mean by deterministic?

MS. KEITHLINE: Yes. With the caveat or

the further explanation that the diversity and defense-in-depth evaluation described in BTP-19 has a different design basis that the regular loss of coolant analysis.

In other words, when you assume the common-cause failure and evaluate the systems that way per BTP-19, you don't evaluate to the acceptance criteria in 10 CFR 50.46. You can use 10 CFR 100 dose criteria.

So it is a --

MEMBER KRESS: But it is still strictly deterministic.

MS. KEITHLINE: But it is still deterministic, yes, it is.

CHAIR APOSTOLAKIS: That is why it is called deterministic without the benefit of probabilities. That's what it is.

Somebody want to comment?

MR. ARNDT: I was just going to highlight the fact that we are going to talk about some of these issues in our presentation --

CHAIR APOSTOLAKIS: I understand that, Steve. But what I'm trying to understand is is BTP is going to be influenced by all this work that we will be presenting this afternoon? Or is it going to stay the way I saw it?

MR. ARNDT: The purpose of the task working groups are to develop potentially new staff positions through our interactions with the industry and Research.

CHAIR APOSTOLAKIS: So it is the job of this Steering group to oversee all this effort? And the branch technical position that we have now is subject to change? Is that the correct understanding?

MR. ARNDT: That is correct.

MR. MAYFIELD: Mr. Chairman, let me -- from a non-I&C person's perspective, I just keep getting drug in the middle of this, the way I see this is that the branch technical position, the review guidance that exists today could lead to licensing an I&C system. However, that would not allow the designers, the industry to take advantage of all the features and capabilities that are available today.

So there has been a lot of dialogue with the industry as well as among the staff on how far can we go to change the approaches that the staff has had for a number of years. And at the same time, not give up critical pieces of safety. And the safety structure that we have.

So we're very interested in pushing this forward. The industry obviously has both the safety and an economic interest in pursuing these areas. Our primary role is to assure that safety isn't compromised and at the same time to facilitate moving forward as far as we can reasonably go.

So that is what we're looking at. And yes, all of these -- the SRP section, the branch technical positions, the associated regulatory guides have the potential of being revised.

CHAIR APOSTOLAKIS: So today's meeting, the purpose of today's meeting is to actually discuss ideas as to how to proceed to do these things?

MR. MAYFIELD: I think it is to inform the Subcommittee about where the staff is going and to seek input from you if you see a flaw or a better way to go at it.

MR. ARNDT: And to provide you information to support your letter to the Commission in this area.

MR. MARION: Which, of course, will be highly supportive of the staff's effort.

CHAIR APOSTOLAKIS: As it usually is.

MR. MARION: As it usually is.

MEMBER MAYNARD: A couple of questions. Back on the technical papers, George asked a question a while ago and I'm not sure it was clearly answered.

These papers will be based on today's current standing of the technology not based on 1994's understanding the situation, right?

MS. KEITHLINE: That's correct, yes.

MEMBER MAYNARD: And do you have a schedule or milestones? Or when would you planning to issue the paper? What time frame?

MS. KEITHLINE: All right. We're currently in the processing of developing those details. NRC has given us a draft project plan with milestones and deliverables. But the dates need to be filled in. And then specifically for each item when we will submit things.

So we don't have a final detailed, dated schedule yet. Probably by sometime --

MR. MARION: Yes, this is Alex Marion. I'm hoping within the next month or so, we can have an agreement on the schedule. We have a meeting of our working group tomorrow. We're going to review the project plan and do what Kimberly just suggested in terms of putting in our thoughts on the schedule. And then we will convey that to the NRC in our letter next week.

CHAIR APOSTOLAKIS: So things are still in a state of flux, right?

MS. KEITHLINE: Being developed.

MR. MARION: I wouldn't characterize -- this is Alex Marion again -- I wouldn't characterize it as a state of flux. I think we are working very, very hard in the same direction, making sure we understand what the expectations are relative to milestones and deliverables and schedules.

CHAIR APOSTOLAKIS: Just to make clear though where I come from because I don't want you to think that I am a crazy academic who wants the latest paper implemented, I realize, I fully realize that a lot of these methods are just academic exercises or work in progress.

But I do think, though, there is a lot of good stuff there that we can take and implement and go beyond the 1994 report, especially in the area of identification of potential failure modes of the system that involves digital I&C.

When it comes to probabilities, yes, I'll be the first one to say that we shouldn't really touch it at this point. But the failure mode part, it seems to me, there have been some pretty good ideas and applications and so on. So what I'm asking is really somebody ought to look and decide, you know, if A, B, F, and G are good, we can use them. The other stuff is still in development. We can wait. That's really my position.

Thank you very much.

MR. MARION: Thank you.

CHAIR APOSTOLAKIS: Unless you have something else to say?

MR. MARION: No, that's fine.

CHAIR APOSTOLAKIS: No? Thank you very much.

MEMBER KRESS: You could still be a crazy academic.

CHAIR APOSTOLAKIS: I could.

(Laughter.)

CHAIR APOSTOLAKIS: The next presentation is from the NRC on the current regulatory position on diversity and defense-in-depth by Mr. Loesser.

MR. LOESSER: Loesser.

CHAIR APOSTOLAKIS: Loesser.

MR. MARION: Mr. Chairman, if I could, just before Paul get started, we have got a number of presenters before the Subcommittee today. And I know in the past you've asked some questions about just who are these people and why are they standing up in front of you.

So we wanted to share with you. I would

tell you we brought the A Team but I really don't have a B Team. We've been very fortunate in hiring some very talented people. And several of them are going to be talking to you today.

I'll start with Paul. He's got a fairly diverse background in design. And he's been with the NRC since 1990 doing technical reviews. He has a diverse background in the design of computer systems and control systems.

Gene Eagle has also a nearly 30-year background in the nuclear industry as well as in significant design activities. He's only been with us about a year.

Mike Waterman has been talked about a number of times. And I think he has presented before the Subcommittee as well as the full Committee in the past. He also brings about a 30-year background coming to us from the Idaho National Engineering Laboratory.

Cliff Doutt is going to be talking to you this afternoon. He is a member of the Risk Informed Task Group. He's been involved in a wide extent of both digital I&C as well as PRA activities.

Steve Arndt I won't bother to introduce to you. He's presented before the Committee a number of times.

And Alan Kuritzky has 25 years' experience in the PRA area. And he is going to be talking to you this afternoon.

So that's sort of -- I think Richard Wood is also here. He's from Oak Ridge and is going to be supporting us as we go along.

So we've brought a fairly broad range of folks with a lot of years of experience and diverse experience. So with that, we'll turn it over to Paul.

CHAIR APOSTOLAKIS: Thank you.

MR. MARION: Paul?

MR. LOESSER: My intended presentation here is to explain what the current position on diversity and defense-in-depth is. That is the position from which the working groups and all that are starting. What we have done to date.

The safety concern that we were worried about is that an error in common software could cause all the different channels in the protection system where the software is used to malfunction at the same time. And the fact that a number of safety functions are being handled by the same four-channel system has increased this concern.

We feel that high quality design is still the most important method to defend against common mode failure or, for that matter, any kind of failure. And high quality hardware and software will reduce the failure probability.

However, despite high quality software, this only reduces the probability. It does not totally eliminate it. And as such, software errors may still defeat the safety functions in redundant safety-related channels.

This idea was confirmed by the 1997 National Academy of Science Report on I&C Systems in Nuclear Power Plants. Their conclusion was that the NRC position of assuming that a common mode failure could occur was credible, that it conforms to engineering practice and it should be retained, and their recommendations echo this, that the position is credible and that we should maintain our position regarding the need for diversity in digital I&C systems.

The basis for our policy of diversity and defense-in-depth stems from a number of places. Intense CFR 50.55a(h) protections and safety systems --

CHAIR APOSTOLAKIS: What do you mean by basis?

MR. LOESSER: This is the legal reason why we think that we can require this.

CHAIR APOSTOLAKIS: Is there also a reason somewhere that says we looked at past experience and this is what we have found? And yes, there is a problem with common-cause failures?

MR. LOESSER: There have been a number of studies -- I don't think I mention any of them here -- where we have looked at past studies. Research has done some work where they have looked at failures in power plants in the past and have found quite a few which could have been -- had the potential for causing a common mode failure.

CHAIR APOSTOLAKIS: That's the thing. I think we need a good discussion of the operating experience because this is really what gives you insights, not the legal documents.

MR. LOESSER: Okay, well --

CHAIR APOSTOLAKIS: Are they real common cause failures? Were they -- did they have the potential of becoming common-cause failures? I went back to a presentation from Brookhaven, I believe, last time we met here. And I remember the number of -- 11 common cause -- potential common-cause failures.

MR. KEMPER: Yes, this is Bill Kemper. L

Yes, George, you are right. Absolutely. We discussed that at one of our previous meetings with you all. Mike Waterman has prepared a table of many of those.

CHAIR APOSTOLAKIS: Will we have a discussion this afternoon on this?

MR. KEMPER: Unfortunately, we hadn't planned to do that. But we can talk maybe extemporaneously about it.

CHAIR APOSTOLAKIS: Yes, isn't this --

MR. KEMPER: Okay, maybe we can get a slide quickly, you know, and talk about it later on after the break maybe.

CHAIR APOSTOLAKIS: I think the Subcommittee would benefit a lot from actually seeing real data as to what we mean by common-cause failure in this new domain. And I remember was it you Steve or Dr. Chi who made the presentation?

MR. ARNDT: It was Dr. Chi. But the data has been analyzed by a number of people --

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: -- including us. And what we can do -- we've intentionally included a short section at the end of the D3 on general discussion.

CHAIR APOSTOLAKIS: Yes?

MR. ARNDT: And we'll get some information and we'll --

CHAIR APOSTOLAKIS: That would be great --

MR. ARNDT: -- shoe horn it in.

CHAIR APOSTOLAKIS: -- because I think it is going to provide tremendous insight to the members. Remember this is a data-driven Committee.

MR. ARNDT: Yes, I understand. Just a quick logistical issue before we go on, what we have here is Paul is going to talk about the current position and how we got there. Gene is going to talk about our activities going forward. And then Mike is going to talk about the research. Then we've got a short general discussion where we can talk about these things.

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: One other issue, the primary purpose here is the D3 stuff. So if we have to slip the afternoon a little bit, that's fine.

CHAIR APOSTOLAKIS: And I agree with that. I think the diversity issue and defense-in-depth is extremely important.

MR. ARNDT: Okay.

CHAIR APOSTOLAKIS: That's why I really want the discussion of the experience as well.

MR. ARNDT: Okay.

CHAIR APOSTOLAKIS: Sorry to interrupt.

MR. LOESSER: Unfortunately, I am --

CHAIR APOSTOLAKIS: Actually I'm not sorry.

MR. LOESSER: -- I am not prepared at this moment to discuss the experience.

CHAIR APOSTOLAKIS: I understand.

MR. LOESSER: But I think we can be at a later time.

CHAIR APOSTOLAKIS: But I think it is important also to express the view of the Subcommittee I believe. I see my colleagues are nodding.

MR. LOESSER: The policy also derives from a SECY paper, 93-087, where a four-point position on the common mode failure for I&C was given. And this was modified somewhat by the Commission's Staff's Requirements Memorandum dated July 21st, `93.

And it basically says that the applicant needs to assess the diversity and defense-in-depth, demonstrate that the vulnerabilities to common-cause failure have been addressed, that while performing this assessment, they should analyze each postulated common mode failure in conjunction with each event evaluated in the accident analysis using best estimate methods. And the vendor can then demonstrate adequate diversity exists.

CHAIR APOSTOLAKIS: I guess the key here is to postulate the appropriate common-cause failures, right?

MR. LOESSER: Yes.

CHAIR APOSTOLAKIS: Which is what Mr. Marion meant I think by saying where.

MR. LOESSER: In general the way it has been done to date is just to assume failure of the software. And that whatever protective function is supposed to be wouldn't occur.

There are other ways where you could assume certain types of failure but those are significantly more difficult to do. And the licensees, I don't think, have chosen that route so far. When they do, we will, of course, evaluate what they have and tell them if we believe that their analysis was adequate and correct or if it was not.

CHAIR APOSTOLAKIS: But I suspect though that in postulating common-cause failures people are heavily influenced by the corresponding work on hardware where essentially you look at similar components in the same system and you say yes, if I have two trains and they are nominally identical, and we have their pumps, I may have a common-cause failure of the pumps or of the valves and so on. For example, we don't look at -- or we rarely look at similar components in different systems and so on.

But these are hardware failures. I wonder whether there are unique features here with software where, you know, we have a broader set of potential failures.

MR. LOESSER: I think there certainly is.

CHAIR APOSTOLAKIS: That's why operating experience really helps.

MR. LOESSER: I think there certainly is a difference. First of all, when we are talking about a particular I&C system, the hardware has often been used many times before and has a fairly definitive history behind it.

For example, if you use a Pentium chip, there's what -- a 50-, 100-million of them used throughout the world, possibly more. And there are known failures but -- there are known problems with the Pentium but they are known. There might be some unknown ones but that's based on history.

However, if you write new software for a plant for a particular functions and this is the first time the software has operated, you don't have a history on it. So you have to approach it a little bit differently.

There are some differences between hardware and software. And that is part of what the diversity and defense-in-depth group is trying to look at. What do we need to consider? How do we need to consider it? What are the issues involved? And frankly, I don't have a total answer at this point. I have personal opinions but I can't prove a lot of what I believe.

CHAIR APOSTOLAKIS: But your personal opinions would be useful, too.

MR. LOESSER: Well, in my opinion, something that is being used for the first time has a higher probability of having a problem with it than something that has been used many times. That is one issue.

Second of all, I believe that sufficiently complex software will have a problem in it somewhere. I don't know what that problem is yet but if you are running to a half a million lines of code, it is very difficult to find all the issues. We can find most of them.

I think virtually every digital system we have approved in the past, despite the high quality, has later on been found to have some sort of issue.

In some cases, it is a trivial one. In some cases it is a more important one. But some sort of problems have slipped by the entire quality control, the entire V&V teams, all of this. And I think we need to continue with that assumption that sufficiently complex software will have an issue.

It is the same with hardware. Sufficiently complex hardware will have an issue. And the experiences, for example, of the Pentium show this. However, as you have a whole bunch of operating experience, you get to know what those issues are, can fix them, can work around them or something like that.

So those are just a few of them. I have many more which I will be happy to get to as we go in here.

CHAIR APOSTOLAKIS: Let's go on. But the point of this and the point of all the report and the current BTPs, somebody has to postulate a potential common-cause failure and then you verify that you have adequate protection using 10 CFR 100 and so on. And there isn't --

MR. LOESSER: Back to the third point here --

CHAIR APOSTOLAKIS: -- there isn't a requirement to have a methodology for searching for potential common-cause failures. That is my understanding from reading the document and our discussion this morning.

MR. LOESSER: Well, actually the entire quality control process we use or we require licensees or vendors to use during the design, the V&V, the testing, the quality control, the configuration management, all of those are intended to find and fix errors before the software is fielded.

The problem is this system is not perfect. And problems work their way through it anyway. We do have a method for trying to find and fix errors. Otherwise we could use -- I don't know -- Windows straight off the shelf.

CHAIR APOSTOLAKIS: What method is that?

MR. LOESSER: That is high-quality design, thorough test, V&V, independent to some degree. And I think all of those do a reasonably good job of producing high quality software. But high quality is not the same as perfect.

The third position, that if a postulated common mode failure could disable a function, then a diverse means needs to be provided to take care of the same kind of thing. The diverse function, however, could be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated conditions.

And the fourth position is that despite all of this, a set of displays and controls in the main control room will be provided from manual system level actuation of the critical safety functions. And these displays or controls will be independent and diverse from the computer systems identified in Items 1 and 3 that I just spoke about.

MEMBER ABDEL-KHALIK: How would you verify this word sufficient?

MR. LOESSER: In which --

MEMBER ABDEL-KHALIK: In the first bullet -- Bullet No. 3 -- one, two, three, four, fifth line?

MR. LOESSER: You are talking about sufficient quality?

MEMBER ABDEL-KHALIK: Right.

MR. LOESSER: That is an issue. We, to tell you the truth, haven't done it yet because we haven't gotten to that phase where someone has presented us the diverse system.

However, what I would expect is that while it would not be safety related, it would be a deliberate and careful design effort, good quality testing, and this type of thing, very similar to what we required of the ATWS systems, which is documented in General Letter 85-06.

I expect that some time in the future, we will have to promulgate this in some way saying this is what we really mean by high quality or sufficient quality. But so far we don't have an official statement on what that means. I think this is one of the things that is lacking and one of the things we need to do in the next few months or as soon as we can get around to it.

MR. KEMPER: This is Bill Kemper. If I could just offer something from my experience in the industry, typically -- well, many times, not necessarily the process but many times this is handled in an augmented quality-type of analysis where critical characteristics would be established or identified for the requirements or the performance of the system.

And then those requirements would be institutionalized and preserved in terms of the quality requirements for that piece of equipment even though it is not safety related, if you will. And licensees often refer to that as augmented quality. That is the way it is characterized and labeled within their system. And those are the critical characteristics that they will preserve for the life of the equipment if that helps.

MEMBER ABDEL-KHALIK: Thank you.

CHAIR APOSTOLAKIS: So sufficient quality does not refer to any digital I&C that is in that diverse system. Sufficient quality means that, for example, if it is a cooling system, it can actually cool the core?

MR. LOESSER: No, actually where we are talking about the I&C system that we could use as the diverse system, which would be credited in the event of a common-cause failure.

CHAIR APOSTOLAKIS: So someone then has done to that system what the three points -- or the four points require. I mean --

MR. KEMPER: So, for example, if I could, say we want this to have a reliable power supply, that would be a critical characteristic that is identified for this non-safety equipment. Typically in a non-safety world, we don't address those things, right? If it fails, it fails.

So the designer would then take it upon him or herself to put in a reliable power source for this non-safety piece of equipment. It could be a UPS, you know, something like that.

CHAIR APOSTOLAKIS: But that's not I&C. Is it I&C?

MR. KEMPER: Well, no, that is specifically to power the I&C system. That is just one example.

CHAIR APOSTOLAKIS: Well, it's not entirely clear to me.

MEMBER MAYNARD: Yes but there has been a lot of experience dealing with it. It would be better if there was a little more clarity as to really what constitutes it. But there has been many other things that we have in the industry between the regulator and the user of things that aren't safety related but they are important to safety or they are augmented quality or there are other ways to do it.

But they kind of almost have to be discussed and negotiated on a case-by-case basis rather than have them --

MR. LOESSER: That's why I mentioned the ATWS system where something has been written down in the past and has been applied. And we could do -- either use the same criteria or after discussion with EPRI and NEI and other industry representatives, modify this somewhat.

What I was saying is that this has not yet been done and is something that is going to be required in the future.

Just as some background, the way we got to this area, when we were thinking about the existing operating plants back in the early `90s, we assumed that digital system would replace analog systems pretty much one function at a time. And the digital systems would perform only one safety function.

That is, in fact, the kind of replacements we were getting in `95, `98. And that other analog systems would still be available. And that the D3 analysis for operating plants would be comparatively simple.

We would show that if one safety function didn't mitigate the accident that another one would. That is if you didn't trip on the level in the reactor vessel, you could trip on the pressure for a particular accident or occurrence.

The current digital upgrades, however, use many safety functions and in some cases all of them in one four-channel digital system. The diverse analog systems are no longer available. The D3 analysis does often show that some diversity is required.

And this now leads to the question of exactly how diverse must the diverse system be? What kind of quality do we need? And those are the reasons why we have all these issues today.

MEMBER MAYNARD: But with the current digital upgrades, aren't they still required to have like the AMSAC or the ATWS --

MR. LOESSER: Yes, they are still required to have --

MEMBER MAYNARD: So there is still some -- it has not taken away all of the current diversity.

MR. LOESSER: No, I said it was the safety functions. The ATWS systems are generally no safety functions. But, for example, we have had an applicant who wanted to put all the ESF and all the RPS functions together into one four-channel system where one common mode failure would take out the whole lot.

So if you did have a software failure which stopped the system as an example, froze it, none of these functions would be available. The question is what does the plant do now? And that is what the diversity and defense-in-depth analysis is supposed to show.

The primary difference between the SECY paper that originally went up in `93 and the SRM deals with the common cause software failures. The SRM says that common-cause failures are beyond design basis.

And as such, the analysis needs to be on a best estimate basis.

The result of this is that the diverse or different functions may be performed by a non-safety system and that the analysis can be done on a best estimate basis and that the displays and controls required by the fourth point, the independent displays and controls, do not need to be safety grade.

The current policy is that the applicants need to perform a diversity and defense-in-depth assessment. They need to analyze design basis events as identified in the SAR.

If a postulated common-cause failure could disable these functions, required to respond to a design basis event, then a diverse means of response needs to be present with a documented basis. And that the diverse means could be non-safety. And once again, we have the if the sufficient quality to perform the necessary function is there.

NUREG-6303 from December `94, as you pointed out, which is now 13 years old, does show an approved method for performing the diversity and defense-in-depth analysis.

CHAIR APOSTOLAKIS: But that -- I mean there are methods and methods.

MR. LOESSER: Yes.

CHAIR APOSTOLAKIS: And my opinion is that it is a very high-level method. I mean you can do anything you want under it. Essentially it says look up a block diagram and try to figure out what interactions are. I mean unless I'm missing something, it's a fairly general --

MR. LOESSER: No, you are absolutely correct. Like any other NUREG, this is one method we have looked at and approved. Certainly if the licensees have a different way of doing a diversity and defense-in-depth analysis, they can propose it. And if they do a good job of it and it actually accomplishes what is needed, that is to show that diversity is there or diversity is not there, we would review it and accept their methodology.

If they don't have a reasonable argument as to why this is the case, then we would then reject it. I think that is pretty much what we're required to do.

CHAIR APOSTOLAKIS: And my hope is that as a result of the research that the Office of Research has undertaken and perhaps the efforts of EPRI and NEI, we will be able sometime in the near future to be more specific as to what methods could help and how and so on.

MR. LOESSER: I mean to be honest, when it comes to a diversity and defense-in-depth analysis, when you are trying to decide if two different systems are diverse, I think an awful lot of the stuff in 6303 goes to a level that is not really needed.

If you were looking at two different systems, and they really are different, they have different microprocessors, come from different companies, are programmed in different languages, you can be fairly sure they are different. Granted they may buy their resistors and capacitors from the same vendor but this doesn't effect software and wouldn't effect the software common mode failure.

I think in most cases, the question is not are two different systems diverse. The real question is do we need a diverse system. And that's something different than what 6303 discusses.

MEMBER ABDEL-KHALIK: The National Academy study, one of their conclusions stated that there appears to be no generally applicable effective way to evaluate diversity between two pieces of software performing the same function.

Now so whether this second system is safety or non-safety, there still has to be the determination that these two sets of software are diverse.

MR. LOESSER: Yes. There is a couple --

MEMBER ABDEL-KHALIK: Is this statement still applicable?

MR. LOESSER: I think there are ways of determining if it is diverse. There may be some issues deep down such as those that Nancy Levinson's studies have talked about.

But if you are talking about two different pieces of software, if they are derived from different specifications and we know that specification failure is one of the major problems with software, so if they both use the same specification and there is a specification error, they would both have the same thing, assuming that they are correct and that specification is implemented.

But if they have two different specifications, if they have two different coding teams, if there is human diversity between the people performing the functions, if the hardware that it is being run on, if, for example, the compiler and the software, if they are programmed in different languages, if there is a method made to avoid the same kind of logic, I think you can be fairly certain that they are diverse.

Granted Nancy Levinson is of the opinion that even if all this is done, since universities tend to teach the same programming techniques, the same techniques will be used throughout and there will be a degree of commonality but I don't think you can ever get a perfect determination. But I think you can certainly get a reasonable determination that this is unlikely to be subject to the same common-cause failure.

CHAIR APOSTOLAKIS: So ultimately you have to risk inform this one way or another, somehow.

MR. LOESSER: I wouldn't say risk inform -- 10 CFR, by its very nature uses words like it is unlikely or highly -- that the function is highly probably or something like this. And this was used long before the concept of PRA or risk-informed was introduced.

And I think there is always a value judgment that has to be made. There is always a certain amount of judgment. And in my opinion, that judgment needs to be documented to the point where a reasonably competent engineer would understand if they read this why you made the decision you did.

I will grant you that in engineering, as in many other fields, there are very few absolutes. It is very difficult to say this is absolutely different from this in every respect. Virtually all semiconductors use silicon. But it is not a software issue. And what we are worried about is primarily software common-cause failure.

I would look at the various diversity aspects, which will be on the next slide, and say which --

CHAIR APOSTOLAKIS: Okay, let's move on then to the next slide.

MR. LOESSER: In the diversity analysis, it says the two systems should be compared for each of the diversity attributes. And those are listed here: design diversity, equipment functional/human, and by human we mean the life cycle processes, not operator action, signal diversity, and software diversity.

Then once you have considered all of this, the combined assessment should be used to present an argument that either the system is diverse or it is not diverse. And the basis for claiming these needs to be documents. I think those are all fairly reasonable.

I will grant that two different engineers looking at the same two systems might come up with somewhat different answers but as long as the methodology and thoughts are documented, I think they are understandable and a decision can be made and an agreement can be reached.

The acceptance criteria in BTP-19, as it currently is, says that for each anticipated operational occurrence for each postulated common mode failure, you do an analysis using best estimate methods. And that the resulting radiation release should not exceed ten percent of Part 100 guidelines or violate the primary coolant pressure boundary.

We do the same thing for each postulated accident in the design basis, use best estimate methods, once again, not allowed to exceed ten percent of the Part 100 guidelines, violate the integrity of the primary coolant, or violate the integrity of the containment.

That if a common element or signal source is shared between the control systems and the trip system, and failure of this is postulated where it can create a situation where you need a reactor trip and at the same time impair that reactor trip, then a diverse function needs to be provided to perform the safety function.

And the same basis not exceeding ten

percent of the Part 100 guidelines or violating the integrity of the primary coolant boundary.

Also it says that no failure of the monitoring or display systems, that is the non-safety systems, should influence the functioning of the trip system or the ESFAS. And that adequate diversity -- the adequacy of the diversity provided needs to be justified.

That is actually my final slide. Are there any other questions I could --

CHAIR APOSTOLAKIS: Yes, there is a question that maybe we should discuss in more detail later but maybe you can give us your opinion. Shouldn't we apply the principle of diversity to the review as well? The review itself should use perhaps diverse ways of doing all these things rather than relying on the judgment of one or two guys?

MR. LOESSER: Well, in fact, I believe it is. While, for example, if I do the review, I read all the stuff, I write up my opinion but certainly I'm not the guy who signs it. This is then looked at by my boss. And then very often his boss to see if I made a reasonable argument, if I took things into consideration.

To be honest, there have been times when

I have been overridden or my opinion has been -- how do I put it -- modified. There is some diversity in review.

Now if you mean we should have two entirely separate reviewers come to the -- look at all this --

CHAIR APOSTOLAKIS: That could be one way.

MR. LOESSER: That could be one way.

CHAIR APOSTOLAKIS: Or two different ways of checking the thing, that could be another way.

MR. LOESSER: Any of our significant issues get what we call a peer review. If I do a review, it is read by other reviewers. And they question my logic and my thought pattern. I know I have done it to others. I have had others do it to me.

And I have to convince them that I was right. Or the two opinions go up for arbitration to the next level in management.

We don't have just one person deciding these things. There is a group or at least more than one person looking at it. So there is a degree of diversity.

CHAIR APOSTOLAKIS: Okay.

MR. LOESSER: But as far as having two

reviewers look at exactly the same thing, to be honest, right now I don't think we have the people to do it. We might in five years. But this all takes time and we have to apportion our time with what is most critical and what is most important to industry to some degree.

CHAIR APOSTOLAKIS: Any questions from the members?

(No response.)

CHAIR APOSTOLAKIS: Thank you very much.

We are moving on to the next presentation from the New Reactor Office. Mr. Eagle?

MR. ARNDT: While he is getting set up, some of the questions with respect to looking at different diverse attributes and finding more specific ways of doing this are going to be covered by Mike in his discussion of the ongoing research. It is the second presentation on the right.

MR. EAGLE: Yes, hello. I'm Gene Eagle with the NRO, Division of Engineering, in Instrument Control, my supervisor being Ian Jung.

Our topic today is the NRC activities to address -- our topic today will be looking at the diversity and defense-in-depth issues that we have been working with our task working group.

To start with, we'll look at an overview. We'll look at the problem statements that have been worked together through both the NRC and the industry. We'll take a look at some of the deliverables we are expecting or we will be working on. And then our conclusions.

CHAIR APOSTOLAKIS: Just press the arrow.

MR. EAGLE: Okay. Our diversity and defense-in-depth working group is made up of representatives from both the NRR office, the NRO office, that is the New Reactor Office, and also from Research. We have links with the NMSS group.

We have a very strong group from industry that is backing us up as somewhat like consultants or we've been able to meet with these. And we've met with them several times and we have a good working relationship, as you have already seen, from the talks we had from the people just a few minutes ago.

Paul has already presented two of our main things here that we see in the next two bullets -- the basis for diversity and defense-in-depth presentation in regulatory requirements and the guidance that is in place for helping the reviewers. Paul has done an excellent job giving us the background, what is being done right now. And the main point here is that this has already been used for the certification of new designs.

For example, the design of the AP 1000 from Westinghouse, the GE's ABWR, the CE ABBs, System 80+ are examples of where this certification has been used. And used successfully.

Also, it is being used in some of the special I&C-type systems for safety. For example, the Eagle 21 with the Westinghouse area. You've had the NUMAC with GE. You've had the Common Q, which is going to be in the AP 1000. You have the B&W Star. You have the new TELEPERM for the EPR-type reactors. So we have had experience with this.

The key here, I think, at this point is that the advances in technology now are pushing the industry and the NRC to design clear and more detailed guidance and being able to use these and being able to provide diversity and defense-in-depth in case we do have common mode failures.

What we have done here is to develop a series of problem statements. The overall issue, of course, is that the guidance does not explicitly identify what constitutes acceptable diversity and defense-in-depth in the nuclear facilities and safety system designs. This was pointed out very clearly by

Mr. Loesser in his talks.

So what we did was to take a look and bring together, you know, first our groups and talk about what are some of the problems, what are some of the things we are facing? Kind of a round-robin, barn-storming-type effort. And the result was a list of eight problem statements that need to be looked at, that we have examined in more depth.

The first one, of course, adequate diversity is the key overall. Additionally, we clarify what constitutes adequate diversity and defense-in-depth for the various systems. However, going further, we're looking at some of the details from the other problems is the manual operator action. We will need to clarify just where can we use and how much can we use the operator to depend on him for a second level or even a primary backup or third level backup in case -- and also what time period do we need to have for him to be able to respond.

Now probably the industry mentioned they were going to try to produce a white paper on this. And I think from all our standpoints, we would say this is probably one of those logical -- where do you get the most experienced information from reactor operations is from the people actually operating the reactors.

So this is a major area and we look forward to the information to help from the NEI and the other industry group people

Another area is the credit for leak detection. One of the most famous items in accidents is where we assume that the largest pipe in the reactor suddenly disappears, a guillotine break, just suddenly vanishes and water starts pouring out. And the emergency systems turn on and start pumping it all in.

Basically one of the comments is is this realistic? Can we back down from this? This is a conservative way of looking at it. Can we back down a little bit and look at it? Maybe there is leakage first. And can we take an credit for that? And in looking at that, this is an area that has been --

CHAIR APOSTOLAKIS: Hold on.

MR. EAGLE: Yes?

CHAIR APOSTOLAKIS: In number two --

MR. EAGLE: Yes?

CHAIR APOSTOLAKIS: -- I guess the intent there is to see how operators can save the day. But, again, if you look at operating experience, there was, in particular, a common-cause failure that occurred in

-

MR. EAGLE: Three Mile Island?

CHAIR APOSTOLAKIS: No, no, no, it was a combustion engineering plant where the computer technicians inserted an incorrect dataset to all four channels.

MR. KEMPER: Palo Verde in the core protection calculator.

CHAIR APOSTOLAKIS: Yes. Is that kind of common-cause failure -- this is really not a cause, right, it is a common cause, part of all this?

MR. EAGLE: Yes.

CHAIR APOSTOLAKIS: We do worry about all this? The humans and how they can do things that are -- okay -- and this will be addressed somewhere? Or is it being addressed?

MR. EAGLE: This is definitely one of the things that would have to be considered. It is one of the areas, particularly if you have what you call a live-type situation in which the operator, for example, has to insert something.

It is a little bit different if you have engineers that are developing something and maybe getting ready to go through a new cycle and they actually have to insert new constants into the system to get ready for the new cycle. There you are off line. You are getting ready for it. It's not like an instantaneous thing. Whereas if you have -- where an operator has to put something in and then within a few seconds or a few minutes it is having an effect on the plant, so there are two different looking-type things.

CHAIR APOSTOLAKIS: But does the current branch technical position allow for this? Does it guide the reviewer to look for things like that? Or is part of postulating the common-cause failure?

MR. ARNDT: It is part of postulating the common mode failure. You can get common mode failure be it software or hardware or integrated hardware/software system, in any of a number of ways. The BTP is an evaluation criteria of do you have sufficient diversity given that you have a failure? What you are talking about is how you get that failure.

CHAIR APOSTOLAKIS: Right. So in postulating the failures, people do take these possibilities into account? Or I don't know.

MR. LOESSER: We actually don't take --

CHAIR APOSTOLAKIS: Please, come. You have to identify yourself again. I'm sorry.

MR. LOESSER: Paul Loesser from I&C and

NRR. When we postulate the common mode failure, we don't really consider where it comes from. We just assume there is one.

The kind of thing you are talking about is taken care of in Appendix B, which requires high quality and the way Appendix B is implemented. There are a number of things that are done to make sure, for example, if a software code is modified, that regression testing is done, that a number of other tests -- that it goes through the same level of quality control, V&V testing, and this kind of thing to minimize this kind of failure.

But once again, while we think high quality can minimize it, it can't totally eliminate these failures. And when you do the diversity and defense-in-depth analysis, it doesn't really matter where the failure came from.

Whether it came from the original specification, whether it came from coding error, or whether it came from maintenance error after the system is fielded, it is there. And it is going to cause a problem.

CHAIR APOSTOLAKIS: Well, I understand that part. What worries me is when we say postulate a common-cause failure. So I'm wondering how they are postulated because it is the issue of completeness in other words. If you miss something, you missed it period.

MR. LOESSER: It's, as I said, so far no one has tried to talk about individual types of failure. They postulate overall failure of the system. People haven't gone in and said well, if we have a failure due to coding error in this particular block, this is going to happen. Or if we have a failure in maintenance in putting in new software, this kind of thing will happen.

So far the method has just been to postulate the overall the system will fail. This software will fail. What do we do about it? If a more complex analysis was used, we would certainly look at it and do our best to evaluate it.

MEMBER MAYNARD: I believe this Item 2 here, manual operator actions, what we're talking about is what all operators are trained for is if a limit is exceeded but the reactor protection system didn't do its job, that they are trained to take certain actions, manually tripping the reactor, trip the turbine, or whatever.

And I think we're looking for methodology for the time and how much credit can we take for the manual operator actions --

MR. EAGLE: Yes.

MEMBER MAYNARD: -- in the event that the digital I&C system failed.

CHAIR APOSTOLAKIS: Right. Which is similar to what we are doing in fires, right?

MEMBER KRESS: With respect to the third item up there, I usually view credit for leak detection as a reduction in defense-in-depth and the way to reduce it. And so I don't quite understand what your problem statement means there as it is worded.

Are you looking to say eliminate large break LOCAs from the design basis accidents when you talk about diversity and defense-in-depth? I mean just what -- would you expand on Item 3?

MR. EAGLE: Well, that's a possibility. In other words, the conservative way that is presently being looked at in the analysis for these new plants is that -- or in older plants was the fact that you assume the largest pipe suddenly just disappeared and then what the resulting loss of coolant that results from that was supposed to be considered one of the worst possible accidents.

So then you design your defensive

mechanisms, your engineering safeguards to try to overcome that.

One of the things being questioned is -- and, again, this might be getting into probabilities, the probability of risk assessment, is this an absolute -- a way of looking at it? Is there ways that perhaps by being able to detect leakage we can start to say that maybe this significantly conservative approach, maybe we could back away from it a little bit and yet still have the safety factors. So this is something that is being looked at.

MEMBER KRESS: Okay, you are saying that doesn't -- I think the postulation is that assuming a large break LOCA doesn't add much to defense-in-depth and diversity.

MR. EAGLE: Right. Well, see, as far as the -- yes, defense-in-depth here we're talking about that's the physical thing. The thing that probably would be more in concern with the instrument control people would be can you detect that leak.

MEMBER KRESS: Oh.

MR. EAGLE: And then the instrumentation that doesn't fail --

MEMBER KRESS: That would be the issue.

MEMBER MAYNARD: But this does not

eliminate large break LOCA. It eliminates particularly the guillotine-type break. But you still have to be able to defend against a large break.

MR. WATERMAN: This is Mike Waterman. With regard to diversity and defense-in-depth, the credit for leakage detection is really a subset of manual operator actions in which licensees have wanted to credit the ability to detect the onset of a large break LOCA and respond quickly enough in the event of a common-cause failure of the emergency core cooling system to actually manually initiate it within the design basis of the plant.

And the credit for leakage detection arose out of the existing Branch Technical Position-19 in which we gave, as an example, a justification for crediting operator action. And that example was the leakage detection in a nuclear power plant. In that case, although not stated in the position, it was a System 80+ advanced reactor design in which they had extensive leakage detection devices planned for that reactor.

And so when I put in that example, guilty as charged, I just put in for example, you could credit leakage detection in a nuclear power plant. And I should have been either much more specific or just not used that example.

So what industry has proposed is they have said well, you know, you have given us leak before break, if you will, leakage detection on pipe lip restraints and jet impingement barriers and so why can't we use that analysis to justify operator response times as a diverse approach for mitigating a large break LOCA. And, therefore, not have to put in a diverse low pressure injection system.

And so that is where that problem statement arose. Personally, I consider Problem Statement No. 3 to be wrapped up into manual operator actions. When can you consider a manual operator action as a diversity strategy for certain classes of accidents?

MEMBER ABDEL-KHALIK: The discussion regarding manual operator action, in my mind, affirms the need for Point 4 in your list in BTP where it says a set of displays and controls located in the main control room should be provided for manual system level actuation of critical safety functions and for monitoring of parameters that support safety functions.

The displays and controls should be independent and diverse from the computer-based safety systems identified in the earlier points. Is that true that if you are going to rely on manual operator action, you must have this Point 4 as part of your criteria?

MR. KEMPER: Yes, this is Bill Kemper. Yes, I'm sorry Paul, I didn't mean to cut you off there but yes, that is true. Yes, manual actions have to -- it is assumed that in order to take manual actions that the indicators and the controls that the operators will respond by and with must not be subject to the same common-cause failure.

MEMBER ABDEL-KHALIK: Thank you.

MR. EAGLE: Another factor in there is if you talk to the operators themselves, they want the ability to be able to if they feel that everything is falling apart around them, they feel much more comfortable if they have some way that they can come back and do something.

So I think you will see the operations people when they go into these advanced designs and the operations people in these various plants that are running 103 active nuclear plants now, when they are using advisors, they will be putting some strong emphasis on being able to have operator being able to be -- if everything else fails, be able to be a dependable backup somewhere in there. Because we have gone a long ways in human factors and operations since our Three Mile Island days.

MEMBER ABDEL-KHALIK: If you couple that statement with the statement I made earlier coming from the conclusions of the National Academy study that there appears to be no generally applicable effective way to evaluate diversity between two pieces of software performing the same function, does that imply that this redundant system that would be available for manual operator action can't be digital? Has to be analog?

MR. KEMPER: Again, Bill Kemper here. No, that does not conclude that the system must be analog. It simply means that their backup system must be diverse. So it cannot be operating on the same computer system. It cannot be driven by the same software.

An analog backup system is certainly an acceptable alternative. But not necessarily a directive, if you will, of ours.

MEMBER MAYNARD: But what we are talking about are things that wouldn't even necessarily have to have a computer program. You're talking about being able to push a button that will trip the reactor or start a pump. So you are not necessarily looking at doing something that then takes another reactor protection system . It's taking manual action to push a button to cause a breaker to open or a pump to start.

MEMBER KRESS: But that did open the question of what you mean by diversity. You know it is different computers, different software put together by different people. And so at some point, you'll give us a definition of what you mean by diversity?

MR. ARNDT: We'll talk to you about where we are going on that and how we are trying to get smarter about that.

MR. EAGLE: That's literally part of the whole process that we are working on now. That is one of the key areas that we are looking at.

MEMBER MAYNARD: One of the other, just for clarity in reading the branch technical position and other things, sometime we're not real disciplined on our use of terms as to reactor protection system versus reactor trip. And when we're talking the bigger picture and the smaller picture and different other components here. So that is just something else you have to watch out for when you are reading some of this, too.

MR. JUNG: This is Ian Jung. I'm the Chief of the I&C Branch in NRO. I started about seven months ago.

Just one thing to add about the manual operation and many of these problems statement related to diversity and defense-in-depth, they are very interrelated with human factors engineering and even communications and software development life cycle processes.

So this particular set of statements, problem statements, are not intended to address all the other areas. We are sort of focusing these problem statements from a pure perspective of diversity and defense-in-depth perspectives. So if there are other concerns sort of related to it, that will probably be addressed whereby in coordination with other branches.

For example, manual actions, operator actions, clearly we're going to work with the human factors group as we resolve that issue.

CHAIR APOSTOLAKIS: Possibly use ATHEANA?

(Laughter.)

CHAIR APOSTOLAKIS: Please go on.

MR. EAGLE: Okay. In our Problem

Statement No. 4, BTP-19 Position 4 challenges, this is a case, again, we just read that where they set displays and controls located in the main control room shall be provided for manual system-level activation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified as above. And we've already mentioned that.

One thing here is I've been right pleased in noticing the various designs that we're seeing and work coming in from the AP 1000, the SBWR, EPR, they are showing the four channels and then showing not only inside the four channels, they are actually starting to show subdivisions within these channels to even have a redundancy so what I assume a component even inside a subdivision would not take the whole division down.

So this has been an interesting thing. Going back into this area, if they have credit for taking components because of this, it allows maybe some more diversity in being able to what components can be turned on or used. And this is a question that needs to be looked at a little bit more in detail.

Number five, effects of common-cause

failures, additional clarity is desired regarding the effects that should be considered. Generally we think of just -- as Paul spoke of not long ago, with failure is all of a sudden, it just doesn't work any longer. But also there may be other ways and other types of failures.

For example, a failure to activate but also a failure to -- it actually causes a spurious activation, particularly in some of the engineering safeguards, the actual starting of the pumps or starting the pump items would not be good. So this is something that has to be taken into consideration.

CHAIR APOSTOLAKIS: I think this is related to something we discussed with the Office of Research some time ago, namely classification of the systems that utilize digital I&C somewhat, just actuation systems there may be feedback and control systems and so on. The methods are different and I think several of these points, in fact, are related to that. So you may want to think about rephrasing some of this. And that applicability, too.

MR. EAGLE: Right. This is a -- point six is a clarification of identification design attributes. Could there be sets of attributes that can be used, maybe expanded on, that help us get a much more simplified or clearer picture, a more direct of being able to present and understand this diversity and what kind of depths we would need.

One example might be simplicity. For example, we think of these process computers being quite large and complex. But also we're now seeing the breakdown into such things as the field-programmable gator rays, things like that that are logic devices that could be brought down and maybe used in small chunks or groups that are much more simplified and much easier to thoroughly test. Also, it's easier to predict failures within these.

Echelons of defense, additional clarification is desired regarding the echelons of defense. These echelons, for example the ones that I talked about that control the reactor trip system, the engineered safeguard systems, and the monitoring and indication post the diverse and one depending on being able to take over if the other one fails, therefore, BTP-19 and some of the documents indicate these should be separated.

One idea is that really necessary? Is there some places where there might be some maybe commonality but still to be able to carry the defense-in-depth and the diversity. And actually may be able to achieve greater safety with certain types of this combining certain things. But this is an area that does need more look-see.

Number Eight problem statement is the single failure. At this point in time, the failure of all four of the computers, all of the software, or all four computer systems within the four channels is looked at as beyond a credible accident at this point in some of the statements and some of the documents.

However, there have been others who say really we should need to consider this as a single failure. And the things Paul pointed out in accident analysis, you have to just about assume a single failure, common-cause failure, or common mode failure. And this is another area to be looked at from the group.

As far as deliverables, the idea is to take a look very carefully at the various problem statements, what we have, and to come up with some consensus and then provide this in some type of guidance that can come back. For example, a regulatory issue summary might be achieved, be able to provide this information, and to be able to use it in reviews and also in development and design.

The goal here is to deliver an additional guidance to enhance efficiency and effectiveness in handling safety issues and schedules for simulators. Actually I kind of looked at it is we're all in one great big football game.

And, of course, you know football is one of the greatest pageantry system that we have in this country. And the NRC represent the referees. But you have all these other groups. But the whole objective is to complete the game. And to complete it safety and fairly.

We also have long-term things that will be done. That will be referred to in a moment here, more that will be talked about. And this is where the recommendations, the things we've learned about from research, from the various talks, discussions, developments, conferences, will come and result finally in updating, for instance, the standard review plan. Maybe, for instance, updating the 10 CFR or other things.

CHAIR APOSTOLAKIS: Now the goal in the near term I find a little interesting. Schedules for simulators. Did you elaborate on that? Maybe I missed it.

MR. EAGLE: Yes. One of the most important parts of developing the new reactors and getting ready to operate these is that you have to train your personnel. So you have to have the simulators for this. And to be able to order the simulators, the simulator obviously has to represent almost a completed system.

So you start asking yourself when do we need to know that. And you start backing the times table back. One of the areas I think has been talked about is maybe somewhere in the late part of 2007 they would need to have a guidance that would help be able to facilitate the ordering of the simulators. That the information that would be sufficiently intact so that the designs could be completed and approved, that would help us be able to get those simulators ordered.

CHAIR APOSTOLAKIS: The reason why I raised the issue is because I saw a few papers in the literature where they -- I fully agree with what you said, by the way -- where the simulators are used to actually do a safety analysis.

In other words, when we do all these evaluations and do son and, for example, I have one paper in front of me, it says the standard techniques like failure modes and effects analysis, fault tree analysis, and so on are static.

And they cannot perform dynamic analysis and identify the interactions among systems. So they use simulators to actually do these things and try to see what the consequences of common-cause failures are and so on. So that could be another way of performing this evaluation.

MR. MAYFIELD: Mr. Chairman, if I could, this is Mike Mayfield from NRO. And I agree, given the adequate fidelity in the simulators you could use them for that purpose.

CHAIR APOSTOLAKIS: Yes.

MR. MAYFIELD: The driver here, as Gene said, is training for the in-plant staff. I think we didn't fully appreciate that schedule constraint when we got started on this. We've had some ongoing dialogue with the industry about timing for delivering some of this interim guidance.

And it has been fairly clear that being able to order the simulators to facilitate the fairly lengthy training schedules becomes the long pole in the tent. And so we're working hard to achieve -- to try to achieve the schedule that they need to be on.

We got short-cycled a bit in the last couple of months, which is creating some challenges, some prioritization of the various activities which we are interested in the industry input, where to put the resources first. But the schedule for the simulators has proven to be the more challenging issue.

CHAIR APOSTOLAKIS: I think you would benefit from the experience of these people but maybe the use of the simulators they way I just described can be part of the long term.

MR. MAYFIELD: I think it could very definitely be part of the long term. The near term thing is to give people enough assurance in these criteria so that they can move forward, finish up the design to the degree they need to move forward on ordering the simulators.

CHAIR APOSTOLAKIS: I think it would be useful for you guys to look at some of these papers. I'm not saying you should do what they are describing. But it would be useful. Where should I send it?

MR. MAYFIELD: Why don't you send them to Steve --

CHAIR APOSTOLAKIS: Okay.

MR. MAYFIELD: -- as the initial point of contact.

CHAIR APOSTOLAKIS: Right.

MR. MAYFIELD: And he will share them among the working groups.

CHAIR APOSTOLAKIS: Just look at them and see what these guys are doing and what kind of insights they are gaining.

MR. MAYFIELD: Yes.

CHAIR APOSTOLAKIS: And take it from there.

MR. MAYFIELD: Yes.

MR. ARNDT: The point of this bullet, Doug, just to put a point on it is some of the design decisions are going to be driven by what our interim guidance is on diversity and defense-in-depth. How they design things.

Those need to be made so they can do their complete design, get it reviewed, get their simulators ordered, et cetera. So that the point here is that the interim guidance is being driven by that design decision which is being driven by their need to order the simulators.

CHAIR APOSTOLAKIS: Good.

MR. EAGLE: There are two key areas here concerning simulators that I'd like to point out. We have already put out very clearly the importance of the simulator to the nuclear plant for training the operators. There is also a simulator for the vendor. And I would like to make a personal recommendation to the Committee that they visit these vendors' simulators because in looking at these modern systems, it is nothing like you have seen before. It is more like walking into "Star Wars" now.

And we've had the pleasure of visiting at least one of these and it is an interesting experience sitting down where everything is being run by computers and try it. So the Committee I think would find a very good learning experience by doing that.

CHAIR APOSTOLAKIS: Yes. Meeting R2-D2.

(Laughter.)

CHAIR APOSTOLAKIS: Okay. And what's number nine?

MR. EAGLE: Our final is the conclusions, the regulatory basis for staffing guidance on diversity and defense-in-depth are in place for the new reactor submittals. Additional details, flexibility, clarifications are needed in some areas as technology has advanced.

The staff, in principle, is in agreement with industry in advocating the use of digital computer-based I&C with the potential of providing greater safety. The challenge is in the details.

The NRC and nuclear industry continue to work closely to resolve identified problems. Once again, we repeat, the goal is to deliver additional guidance to enhance efficiency, effectiveness in handling safety issues and schedules for the simulators.

Is there any questions?

(No response.)

CHAIR APOSTOLAKIS: Okay. Well, thank you very much.

MR. EAGLE: Thank you.

CHAIR APOSTOLAKIS: So we'll take a break now.

MR. MAYFIELD: George, if I could --

CHAIR APOSTOLAKIS: Yes?

MR. MAYFIELD: -- just a question you had asked early on about is the Steering Committee made up only of NRC people and I wanted to provide the Subcommittee a little bit of perspective on the structure that has been put in place.

At the Commission meeting where this all got started, the industry representatives described the Steering Committee that they had in place. And that seemed like such a good idea the Commission said we probably should go do a similar thing.

So there actually is an industry Steering Committee and a parallel NRC Steering Committee. There are then parallel structures down at the task working groups. There is active information exchange, idea exchange, in a public meeting setting between the industry groups and the NRC groups.

But it is not a joint Steering Committee or a joint task working group. These are parallel groups. And they each have their own working activities and things to go do. But there is very active information flow between them.

CHAIR APOSTOLAKIS: How big is the NRC Steering Committee?

MR. MAYFIELD: Pardon me?

CHAIR APOSTOLAKIS: Who are the members of your Committee?

MR. MAYFIELD: The Steering Committee, Jack Grobe chairs it. I'm on it. Mark Cunningham from Research, Joe Gitter from NMSS, on the fuel cycle facilities is where that one really comes in. And then Scott Morris from INSR. So that --

CHAIR APOSTOLAKIS: Those are senior level people.

MR. MAYFIELD: Senior level -- Division Director and higher.

CHAIR APOSTOLAKIS: Okay. Go ahead.

MR. ARNDT: It was intended to be similar to the PRA Steering Committee. Sorry, Steve Arndt, the other thing you might want to mention is all these interactions are done in a public environment to elicit additional comments from other stakeholders. It is not just the industry that we are working with.

CHAIR APOSTOLAKIS: All right. Shall we break until 10:20?

(Whereupon, the foregoing matter went off the record at 10:02 a.m. and went back on the record at 10:22 a.m.)

CHAIR APOSTOLAKIS: We are back in session. Our next presentation is by Mr. Waterman on Diversity and Defense-in-Depth Research.

MR. WATERMAN: If Dr. Wood could come on up here.

CHAIR APOSTOLAKIS: That is different, I guess, from what it says here. It says long-term activities. But it is the same thing?

MR. WATERMAN: That is correct, Dr. Apostolakis.

CHAIR APOSTOLAKIS: Okay.

MR. WATERMAN: My name is Mike Waterman. I'm in the Office of Research. I was formerly in the Office of Nuclear Reactor Regulation as an I&C Engineer over there for about I don't know 14 or 15 years and came over to Research, I think, in 2003 or 2004, something like that. Time flies.

With me today is Dr. Wood from the Oak Ridge National Laboratory. Dr. Wood has extensive experience in the area of instrumentation and controls and he is my principle investigator in the research that I'm going to describe today.

The research I will describe in this presentation really addresses the fundamental question of how much diversity is enough in the nuclear industry. This research was initiated last October and is still in progress. And consequently any conclusions I describe today are with regard to the ongoing research and should be considered preliminary.

Now in this presentation, I will summarize the diversity and defense-in-depth issue we are addressing with the current diversity research project. I will then provide background information on diversity and defense-in-depth NRC policy, a little bit of history.

I will then describe the research project and schedule and conclude with some preliminary results of that research.

Now adding diverse systems and defense-in-depth is a worthwhile strategy for assuring public health and safety. And obviously a diverse system for every safety system and extensive defense-in-depth could be used to mitigate common-cause failures. However, from a practical standpoint, this solution may be technically unfeasible.

Given this conclusions then, the question is not whether diversity and defense-in-depth should be employed but rather how much diversity and defense-in-depth are enough to provide reasonable assurance of adequate safety. And supporting questions include are there precedents for good engineering practices? For example, what is being done in other countries, industries, and agencies with regard to diversity and defense-in-depth?

Can sets of attributes provide adequate diversity? For example, are there subsets of attributes identified in NUREG/CR-6303 that can provide sufficient diversity?

And finally are there standards or other guidance that can be endorsed? For example, does ANSI ANS 58.8, which is the time response design criteria for nuclear safety-related operator actions, which is referenced by IEEE Standard 6013, provide acceptable guidance for determining operator response times.

MEMBER ABDEL-KHALIK: You know posing the question in the form of how much implies that diversity can be quantified. And the issue then in my mind is is that true? Can you actually assign a quantifiable measure to measure diversity?

MR. WATERMAN: I don't think that was what I was meaning. I mean you could provide some amount of diversity that is just overwhelming. Different microprocessors, different systems, different operators who do the same function, things like that. And you can just literally overwhelm a system with so much diversity that you are sure is that really as much as you need?

But I don't know about quantification. We're not attempting to do any quantification.

CHAIR APOSTOLAKIS: This is the question that was asked I don't know 15 -- 10, 15 years ago when we were debating Regulatory Guide 1.174. And there we were not asking the diversity question because, you know, the problem with a traditional regulatory system is that the question -- the statement was that it doesn't guide you as to how much defense-in-depth is sufficient.

And by quantifying risk or some metric that is related to risk, you can actually say yes, this is enough because I have reached an unavailability level that is acceptable.

So what I would say -- I think strictly speaking, the answer to your question, Said, really does not exist. But you can have metrics that give you some indication.

But I would say that these are good questions also for the Research group. One, as you know, one of the major efforts there is to develop risk methods that involve digital I&C. And here is a set of practical questions that the Agency is interested in that maybe those guys should have in the back of their mind when they develop their tools. Say can I answer this question? Can I give some guidance to Mike or whoever else is using this?

Steve?

MR. ARNDT: Yes, and that is one of the things we'll talk about a little bit this afternoon. Not in a lot of detail but some.

What Mike is, and correct me if I'm wrong, Mike also works at our Office of Research, the Research Program, to answer some of the long-term questions we talked about before the break, is looking at qualitative strategies to answer this question.

CHAIR APOSTOLAKIS: Yes.

MR. WATERMAN: And these questions, we

here in the NRC, we didn't invent these questions. These are really questions that have risen out of the industry when we've told the industry employ diversity and defense-in-depth and they come back and say well, how much do you need?

CHAIR APOSTOLAKIS: Because as far as they are concerned --

MR. WATERMAN: And we're trying to answer that.

CHAIR APOSTOLAKIS: -- you can keep adding diversity to systems.

MR. WATERMAN: That's right.

CHAIR APOSTOLAKIS: To make them safer and safer and safer.

MR. WATERMAN: Of course, as you get more and more diverse, you become more and more complex and so the reliability starts suffering.

CHAIR APOSTOLAKIS: That's why there is a period of public comment.

MR. WATERMAN: Now some background here is our policy was established really in the early to mid-1990s as a means to address common-cause failures in digital safety systems. However, our knowledge of digital technology has increased significantly since that time, mostly by experience. And the technology itself has evolved considerably since the Agency's policy was established.

Now as recognized by the nuclear industry and others, common-cause failures in digital systems are difficult to predict. And consequently, just as difficult to prevent. Generally the perceived solution has been to design and build systems that will not fail.

Indeed, for production- class systems, that is an overlying objective of the quality assurance processes and other contractual obligations of the system supplier.

Historically, however, designing systems that will not fail has been difficult to achieve not just in the nuclear industry. You name it, you know, any industry, pick any industry, and they have all had that same problem. And that objective becomes more difficult as the size and complexity of the systems being developed have increased.

Before I settle into a discussion on ongoing NRC research, I think it would be helpful to provide just a brief definition of what diversity is and what defense-in-depth are because often in conversations you hear people use those two terms interchangeably. Sometimes they say defense-in-depth, sometimes they say diversity. And you're not really sure what they are talking about.

So let's just do a brief illustration here. Now this slide illustrates the difference between diversity and defense-in-depth.

Now the slide is for illustration purposes only in that reactor trip systems and engineered safety feature systems are often complementary and not hierarchical in structure. In other words, ESF doesn't always depend upon a reactor trip system to operate in order for it to be called up to operate.

In this illustration, however, four echelons of defense-in-depth are arranged concentrically such that when the control system fails, the reactor trip system reduces reactivity when both the control system, a control system such as main feedwater, turbine generated, governor controlled, chemical volume control systems won't effect, when both the control system and the reactor trip system fail, the engineered safety features continue to support the physical barriers to radioactivity release by maintaining cooling to the core and allowing time for other measures to be taken by reactor operators to bring the plant to a safe state.

Now monitoring and indications, that last echelon down there, allow the operators to monitor plant conditions and to take control of the plant in the event the other three echelons of defense-in-depth cannot. And often operators are directed to take control of the plant even when the engineered safety features are running. For example, terminate high-pressure safety injection under certain conditions.

Now diversity is used to provide added assurance that the reactor trip systems in this case and the ESF systems will function as required. So summarizing, defense-in-depth is a strategy that uses different functional barriers, if you will, to compensate for failures in other barriers -- reactor trip systems, compensating for failures in the control system barrier for example.

Diversity is a strategy that uses different means within the functional barrier to compensate for failures within that same functional barrier. And that is given by the little trapezoid here versus the ellipse, right, those are both reactor trip systems but they are diverse functions such that if a hazardous condition is not handled by one of the diverse means, it may be handled by the other one right here.

So that is what diversity is and that is what defense-in-depth are. So that is sort of in response to your question earlier, I believe, Dr. Apostolakis, you know how do we define these things.

CHAIR APOSTOLAKIS: This is the swiss cheese model, right?

MR. WATERMAN: This is the swiss cheese model, yes.

CHAIR APOSTOLAKIS: Because Jim Reason has proposed it in human performance.

MR. WATERMAN: Generally there are two approaches you use in diversity and defense-in-depth strategy. And these approaches are not exclusive approaches. They are used generally as complementary approaches.

The first approach is avoidance, produce high-quality error-free systems. Build a system that will not fail. Minimize common elements in the system so you can avoid a common-cause failure. Or just limit the fault propagation to a specific system so that it doesn't propagate over and cause a common-cause failure.

In addition to avoidance is the mitigation strategy where you acknowledge you may have a common-cause failure. How do you mitigate it as quickly as possible or as effectively as possible so you can continue to accomplish your function. And by mitigation, you add defense-in-depth to compensate for failure in other functional barriers or systems. And you can provide diverse systems that will not fail at the same time within a functional barrier. So those are the two general approaches.

The current process for confirming adequate diversity and defense-in-depth has been incorporated in safety system design is fairly complex. Current regulatory guidance identifies six categories of diversity attributes that can be used in design of systems.

What we want to know is how can you combine those diversity attributes such that you can come up with sets of diversity strategies. In a research approach for identifying what would constitute the components of the diversity strategy is we want to go out to academia, scientific organizations, other countries' industries and agencies, and find out what the rest of the world is doing with regard to diversity and defense-in-depth.

We also want to use the information that was provided in NUREG/CF-6303 on diversity strategies, combine those and try to develop -- this is the core of the program -- develop sets of D3 strategies that use the attributes and associated diversity criteria out of NUREG/CR-6303.

Once we develop those sets of strategies, we need to know whether or not we need to develop guidance and acceptance criteria for each of those strategies. And, of course, that will feed through the D3 -- the diversity and defense-in-depth task working group that you heard about earlier today, and along with public interaction.

Once we have that guidance, we really need to validate is the guidance applicable? Okay, you've got guidance. Can you actually apply that guidance to license a system?

With that, we will be working with current and new plant designs, licensees, applicants, what have you, to validate our guidance against real systems to find out -- and that was what Alex Marion described early as this cooperative research effort, if you will, to find out is our guidance applicable in a licensing environment? As opposed to just having guidance there that nobody can apply.

And finally to integrate our licensing guidance and acceptance criteria into our regulatory practices. So that is kind of the basic outline of what we are intending to do. Of course there will be public interaction in some parts of that and there will be licensee interaction in other parts.

CHAIR APOSTOLAKIS: Excuse me, Mike, we have our consultant, Dr. Guarro on line.

MR. WATERMAN: Good.

CHAIR APOSTOLAKIS: So I'd like everybody to know that there is somebody listening in and participating.

Sergio, are you there?

(No response.)

CHAIR APOSTOLAKIS: I take it back. We don't have anyone. Okay, he'll come back, I'm sure.

MR. WATERMAN: As described in the above slides, the research project objectives are to supplement and augment existing guidance, acceptance criteria, and licensing processes by evaluating processes used in other countries, agencies, and industries, coupled with recommendations from academia, crazy and otherwise, and scientific organizations.

CHAIR APOSTOLAKIS: Yes, Dr. Kress just pointed out to me that the way you have it there, they appear to be mutually exclusive.

(Laughter.)

CHAIR APOSTOLAKIS: That's okay, keep

going.

MR. WATERMAN: That's right past me.

The results of this research will be integrated into the development of D3 strategies that are based upon the guidance developed in NUREG/CR-6303, as I described earlier. And this phase of the research project is scheduled to be completed in the May time frame of this year.

A follow-on research effort will solicit industry support to validate the licensing process developed by the research to improve clarity and consistency of the licensing process. And this effort is tentatively scheduled to be completed by the end of this year. That is the validation of results, August 2007 time frame, maybe September. It depends on how we schedule things with the licensees and who steps forward.

CHAIR APOSTOLAKIS: So this is what the staff is doing in response to the SRM that the staff should establish an NRC project plan with specific milestones and deliverables? Is that what you are doing here?

MR. ARNDT: No, sir.

CHAIR APOSTOLAKIS: Yes?

MR. ARNDT: The project -- no.

CHAIR APOSTOLAKIS: No?

MR. ARNDT: This is the milestones for a specific research program that is addressing a specific issue within the overall I&C project plan. The project plan is what Alex was talking about earlier. And Mike was talking about earlier. The SRM directed us to put together a project plan to answer the short- and long-term issues that have been identified.

CHAIR APOSTOLAKIS: Right.

MR. ARNDT: So for each of the six areas, D3 is one, risk is one, cyber is one, there is going to be a piece of the project plan. And in each of those project pieces, there are going to problem statements like the ones you heard earlier. And under each of those problem statements, there is going to be actions associated with it. So this is one piece of that problem.

MR. WATERMAN: And this research -- well, this research will be integrated into that task project. But it doesn't encompass the whole project.

MR. KEMPER: George, let me try. I think your question can be answered in two parts here.

CHAIR APOSTOLAKIS: Who is speaking? I'm sorry.

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

Number one, as you know, we presented the digital safety system research plan and program to you all. It is a five-year plan. This research project is a component of that plan. It has been in there for a long time.

CHAIR APOSTOLAKIS: The one we have seen?

MR. KEMPER: Yes, the one you have seen and commented on, as a matter fact, to the Commission.

CHAIR APOSTOLAKIS: All right.

MR. KEMPER: Now it just so happens that when we kicked this off, we also formed these TWGs at the same time. So everything kind of came together quite nicely from a schedule perspective, if you will.

And we've also got other projects, too, like in the communications for highly-integrated control rooms, digital system risk, which we will talk about this afternoon as well. So the research, because we are in a point where it is producing results in a timely fashion, is being integrated as part of the information that is being reviewed by these task working groups. If that clears it up.

CHAIR APOSTOLAKIS: So the specific answer to the SRM, the SRM addressed to you because we also have one as well, is listing those six items or questions?

MR. ARNDT: Six specific areas.

CHAIR APOSTOLAKIS: Areas -- and then say what you will plan to do under each one?

MR. ARNDT: Correct.

CHAIR APOSTOLAKIS: That's really what this requires.

MR. ARNDT: That is correct.

CHAIR APOSTOLAKIS: And it requires also a schedule and so on which you are giving us here as well for this particular piece.

MR. ARNDT: This is for the Research.

MR. WATERMAN: This is just this Research project.

CHAIR APOSTOLAKIS: Yes. But Research feeds into --

MR. ARNDT: Yes.

MR. WATERMAN: Yes.

CHAIR APOSTOLAKIS: Yes, it is not a different agency.

MR. ARNDT: No, it's not a different agency.

CHAIR APOSTOLAKIS: No, I'm trying to get the big picture.

MR. ARNDT: Yes.

MR. WATERMAN: But, for example, this particular research project will not answer the question of what are acceptable manual operator action types.

CHAIR APOSTOLAKIS: I understand that. And the Research plan we have reviewed did not include operators, as I recall, operator actions.

MR. ARNDT: No, that is actually in the HF part of the work. So it wasn't included in the research plan.

CHAIR APOSTOLAKIS: It was not. But now there will be a piece of it?

MR. ARNDT: There will be a piece of it in the project plan which is the Agency plan to deal with these specific issues.

CHAIR APOSTOLAKIS: But who is going to do it is open?

MR. ARNDT: No, it is going to be dealt with by the TWG on human factors. And it is also going to feed into this particular project plan.

CHAIR APOSTOLAKIS: By human factors, you mean they can come back to the Office of Research --

MR. ARNDT: Well, Research at NRR.

CHAIR APOSTOLAKIS: At NRR, okay.

MR. ARNDT: They've got it. We're just

looking at those specific issues.

CHAIR APOSTOLAKIS: Is that research plan that we have seen being modified in any way as a result of this new activity with the group?

MR. ARNDT: It is not specifically being modified. We're going to update it. And this will obviously have an impact on it. But it is not being modified specifically to address these.

MR. WATERMAN: And actually this research here was called out in the existing research plan as something to do. So this was a planned research project.

MR. KEMPER: Yes, excuse me, yes, I'm sorry, Mike, I didn't mean to talk over you. Bill Kemper, again.

Yes, this has always been one of our desires is to clarify what diversity attributes should exist in a system because the guidance right now, as we've said to the Commission, it is sometimes difficult for licensees to understand and decipher and figure out how much diversity they should build into their systems. So that is what we are attempting to accomplish here is to clarify that.

CHAIR APOSTOLAKIS: But it seems to me coming to my earlier -- now bear in mind I'm still trying to understand what is going on -- my earlier comment that the work that your group has been doing on the data should be a critical input here.

MR. KEMPER: Data, you mean failure data?

CHAIR APOSTOLAKIS: Yes, common-cause failures and all that. What has happened in the past? And what did we learn from it? How are the answers to -- or how is the formulation of diversity strategies effected by what we have learned? I think that would be a very valuable thing.

My impression from last time we had a presentation and the data was that it was primarily done for us to understand what had happened and see how that could effect the risk part of the plan. But it seems to me that there is a broader perspective there that can be gained.

And you have already done a lot of it. But I mean, again, I come back to the Brookhaven presentation. And also John Bickling, the paper that I just sent you, looked at the combustion engineering experience.

So I would say that that should be an important resource here. This is what happened. And if we had this strategy, we would have handled it this way. Or whatever else -- lessons.

MR. MAYFIELD: This is Mike Mayfield, if I could suggest, I kind of like your idea, which is unusual in and of itself. But if I could offer the proposal, let us take this back and chew on it. Obviously, it hasn't -- what you are suggesting isn't something that we have thought through carefully in terms of expanding the use of the data to this application.

I kind of like the suggestion. Why don't you let us take it back and work it both at the Steering Committee -- you know, on the staff Steering Committee as well as with the task working groups on the industry side as well as staff. And let's see where we can go.

I'm sure this won't be the last time we're talking to the Subcommittee or the full Committee. And let us come back to you with a strategy.

CHAIR APOSTOLAKIS: Are you scheduled to address the full Committee next time? In May?

MR. ARNDT: We've got an hour and a half to talk about D3 issues. We had not decided yet how much you are going to report and how much we are going to present.

CHAIR APOSTOLAKIS: I understand that.

MR. ARNDT: So that is something we need

to talk about later.

CHAIR APOSTOLAKIS: Right. But, Mike, do you think you may have some preliminary thoughts along these lines in two weeks?

MR. MAYFIELD: Well, I think this is something that -- when are we supposed to be back?

CHAIR APOSTOLAKIS: In two weeks or so.

MR. MAYFIELD: I would think this is something -- preliminary thoughts but nothing definitive. I think that would be unrealistic.

CHAIR APOSTOLAKIS: That would be great, yes.

MR. MAYFIELD: But let us -- and this is something where we can reach out to Kimberly Keithline from NEI --

CHAIR APOSTOLAKIS: Good.

MR. MAYFIELD: -- motivate some discussion. And at least give you some initial thoughts on it.

CHAIR APOSTOLAKIS: Very good. Yes, that should be sufficient. Yes, we'll come back to you.

MR. WATERMAN: Now in that vein from a historical perspective, a lot of research has already been done. And some of the conclusions are is that a lot of the common-cause failures arose because of inappropriate specifications. And we are seeing a lot of common-cause failures arise as a function of maintaining a system once it is installed.

Somebody does a modification. The modification didn't go through the same process and caused the common-cause failure.

Within the vein of specification, you could -- we could come up and insist that all specifications be sent through a formal methods process. As the systems get more complex, that becomes a much less tenable approach.

With regard to maintaining a system, putting in a software patch, if you will, or something like that, what else can you do? You tell people do a good job and somebody misses something, it causes a failure. There is not a lot of diversity strategy that you can apply toward telling somebody to do a good job.

The software processes that are used for safety-critical systems are all Appendix B-type processes, independent verification and validation, configuration management, software quality assurance, all of those are rolled into it. But it is the practice. It is the actual application of that.

And a diversity strategy that says well, you've got to do a better job of independent verification and validation is not a very good strategy because the people who are doing it are already doing the best job they can.

It is when that process breaks down. And what my experience has been, the process breaks down during the mod -- you know, somebody needs to do a patch. The Palo Verde core protection calculator example, that was a system modification. And the error was introduced into the system after it was in there.

And incidently, that wasn't really a common-cause failure. I just want to clarify that. It was a potential common-cause failure. It required a hardware failure in each channel before the common-cause failure would manifest itself. So just to clear the air on that. I don't want the industry to be defensive because it was a potential. It was a precursor to a common-cause failure.

So with that in mind, if I can move on now to talking about what our sources of information are that we have gone with. We've looked at from the academia and the scientific disciplines, we've looked at, of course, the National Academy of Sciences, the National Science Foundation.

We've looked at various papers that were produced by universities. Some of those papers were sponsored by agencies such as the Federal Aviation Administration and things like that.

With regard to engineering disciplines, the science organizations, if you will, we've looked at IEEE, the standards organization, to see what they are doing, the IEC, we've looked at their standards organization.

We've looked at Controls Engineering, the American Society of Chemical Engineers, and the Society of Automotive Engineers.

With regard to foreign reactors, we looked at the French, British, Korean, and Finnish designers and researchers and regulators. As a matter of fact, Dr. Wood and I are planning a trip, as directed by the Commission, but we had already anticipated the trip over to Europe next month to talk to the French regulators, the Finnish regulators, and the UK regulators about what they are doing for diversity and defense-in-depth to get a regulatory perspective.

I mean we could talk to the plant designers, too, but what we're really after is what is the regulatory perspective. Why does France, for example, impose one type of diversity? What was the basis for that? Try to gather some of that information together.

In the chemical processing industry, we've looked at the Center for Chemical Process Safety. In mission-critical defense systems, we've looking in the area of battlefield management.

There was a suggestion that we take a look at nuclear submarine power plant-type stuff. But a lot of that stuff is classified. And we are trying to get something out that you can actually put out to the public. And so we really haven't looked at the classified stuff as much as we've looked at battlefield management systems.

With regard to avionics, we've looked at the Federal Aviation Administration and the Radial Technical Commission for Aeronautics and NASA. And within transportation, we've looked at the Motor Industry Software Reliability Association information and Federal Railway Administration.

So why are we looking at all of this? Well, we're trying to develop some specific strategies that can be used to evaluate system diversity recommendations from academia scientific community. And we want to use those recommendations and approaches to develop specific diversity attribute criteria strategies.

Now what do I mean by diversity attribute criteria? Well, for those of you who have seen NUREG/F-6303, which was written by Lawrence Livermore, a National Labs -- under contract to the NRC back in like 1994 -- Gary Prekshaw was the head engineer on that -- they developed a set of diversity attributes -- six of them -- design, equipment, function, human, diversity, which is really life cycle process diversity signal, and software because software is unique.

And within each of those attributes, those six attributes, they developed certain criteria that could be applied, diversity criteria that could be applied within that attribute. For example, in signal diversity, you could have diverse driven equipment or diverse parameter sensor types or diverse parameters.

And we already employ some of that diversity in the existing analog systems, right? I mean we trip the reactor on high temperature and we trip the reactor on high flux. Both of them are designed to protect the fuel. Or we trip the reactor on low pressure or low flow or whenever we usually have a DNBR-type trip function.

Those are diverse functional trips using often different signals -- high temperature signal versus a flux signal. So some of that is already employed.

Within the digital area, we have other types of diversity. We could have diverse software languages, Pascal and C, for example, or Assembly language and Pascal. Different operating systems, maybe we run a Motorola operating system on Motorola chip versus a risk-based system on an Intel chip. We could use different algorithms.

Within the life cycle process, we've seen a lot of this diverse approach like independent verification or validation, if you will, is a diversity strategy in the life cycle process. When I say life cycle process, I mean the software development life cycle process.

Typically we may use different management teams to assure that there is some diversity in the approaches followed. Or we might use different designers, engineers, and programmers. And, of course, that is the inversion approach that, you know, has been shown to have some flaws.

Dave Parness says there is nothing wrong with inversion as long as you impose diversity on the two different parties who are doing the program. In other words, they are not totally independent. You have a referee in there that tells somebody you have to use rectangular coordinates. And you have to use polar coordinates, for example, if you are doing slope of a line or something like that.

So these are the -- the colored areas in there are what we call the diversity attribute criteria. And what we are attempting to do with this research project is to develop diversity strategies, to identify diversity strategies that use various diversity attribute criteria. We are trying to determine, you know, are there collections of these criteria that if they are put together as a diversity strategy, that provides enough diversity.

Now this is just an example diversity strategy. Don't follow the arrows. Don't think there was a lot of thought that went into the arrows. There was a little bit but not total.

The idea is to develop say, I don't know, five or six diversity approaches, diversity strategies, the licensee could look at their system and determine well, Strategy A is good for my system. I'll follow that. And he would know exactly what diversity approaches he could follow that would be found acceptable here at the NRC. It would be our job, of course, to ensure that they were applied correctly and appropriately.

Right now the licensee has no guidance like that. When they come up with a diversity approach, they don't know whether it is going to be approved by the NRC or rejected. And they really don't know what the criteria is for either one.

And so what this is intended to do is to provide much more licensing certainty to the industry and much more licensing guidance to the NRC staff so that everybody knows what the rules are on diversity and defense-in-depth, especially diversity.

So that is basically the approach that this research is trying to do is to find out what the rest of the world is doing, identify specific diversity strategies that seem to be working such as like what is being done on the Boeing 777, you know what are they doing for diversity and defense-in-depth?

And then to take those and try to bring them into the nuclear industry in a coherent set of diversity strategies that people can follow.

So what have we learned to date? Well, with regard to other industries, this slide describes the results of our diversity research with regard to strategies being used by other agencies and industry such as NASA, the FAA, the aircraft industry, et cetera. The industry strategies are not necessarily used throughout an industry.

What we have done is we've looked at specific applications, identified diversity. But that does not necessarily mean the whole industry follows that strategy. But they are examples of what was found in selected applications within an industry.

The next step in the research project is to develop these diversity attribute strategies to determine specific diversity attribute criteria strategies within each.

For example, in the space shuttle where they are using functional diversity, what type of functional diversity are they using? Where's my wheel? Okay, when we say functional diversity, are they using different functions or are they using different mechanisms? Different response times? Diverse response times? Or what? So, you know, we're trying to -- that's the next step in doing that.

But you will notice interestingly something I noticed here is the signal diversity. Do you notice that? It seems like nobody is using diverse signals like RTDs versus thermocouples.

Nobody is following that approach. They all seem to acknowledge that signals are pretty immune to common mode failure, I guess, although you could argue that the Rosemont certainly would disprove that, the Rosemont pressure transmitter.

But it seems like nobody is really using signal diversity as one of their diversity --

CHAIR APOSTOLAKIS: In the chemical industry, you don't quite have assorted green but --

MR. WATERMAN: Yes, this right here is an indication of this thing about it is not an industry-wide approach. This was just one application. But I wanted to caveat the rest of them with that same comment.

DR. WOOD: If I may interject, this is Richard Wood, the chemical industry, part of the reason those are shaded is because you have recommended practices that acknowledge some virtue to different kinds of diversity. And in the case of the chemical industry signal diversity, using different measurement technologies can have some value and provide some additional means of protection against the potential for common-cause failure.

In some of the other cases, for example the NASA cases or the FAA, they are limited in what they can do because of size, weight, and power consumption considerations. So they don't tend to look at -- and the other thing is they tend to want the same signals going into the same software giving the same results for points of comparison. That is a philosophy that you will see in some of those applications that is distinct from what the nuclear industry does.

MR. WATERMAN: And we can provide additional detail on, for example, space shuttle or anything like that. I've got that in a -- I can reference that fairly quickly.

With regard to the foreign reactors, we've looked at Sizewell, Temeline, well, you can read the list there all the way down to Lungmen, and to determine what they are doing. And this is preliminary information. There may be some corrections that come out, for example, Dukovany or something like that.

Sizewell B does use diverse signals. But none of the rest of them use that. But you'll notice that functional diversity seems to be a common thread throughout all of the plants.

And software diversity, interestingly, is not something that is embraced by all the plants. For example, Sizewell, Dukovany, and Beznau and Paks for that matter, don't really push the software diversity attribute that hard.

So that's basically a summary of where we are at right now is we've narrowed it down to what are the attributes that are being used. And the next step is to go into each of those attributes for each of these diversity examples and determine what criteria in each attribute are being used so we can synthesize some diversity strategies.

MEMBER MAYNARD: What is the expected output of this? Will it be like a NUREG? Will it be a --

MR. WATERMAN: A NUREG is proposed right now. To do that. Long-term, I guess that is what that is really, long-term I'd like to see all of this rolled into the SRP, standard review plans for the various nuclear facilities.

While we are focusing on nuclear reactors right here, Advisory Committee on Reactor Safety, I foresee that this could also be applicable to nuclear facilities in general such as mixed oxide fuel facilities or advance centrifuge facility or the American Centrifuge Project and things like that to also address safety over in those areas. Even though the risk from those facilities is not as high, they still have safety systems. And safety is safety.

MEMBER MAYNARD: Well, it just looks like there is a lot of good information and interesting information that would come out of this that I would hate -- it would be nice if it was in some consolidated document.

MR. WATERMAN: Well, the NUREG is the project deliverable on this. But we need to move beyond the NUREG space into regulatory acceptance criteria space, too. I agree with that totally. And I'm sorry -- I'm kind of from two perspectives here. One is interesting information I'd like to see captured.

But yes, that may not -- you know the more timely thing is what is needed to be factored into the guidance. And the information that is actually going to be used in the regulatory process.

DR. WOOD: If I could make a couple of observations, this is Richard Wood, again. On the previous viewgraph dealing with other industries and agencies, there are some -- one point that I think we should be aware of is none of these industries has an objective set of criteria for how much diversity is enough. We haven't found it. If it is there, it is well hidden.

But in many cases, the amount -- or the need for diversity or, I think as FAA calls it dissimilarity, depends on the consequence of the hazard. And there is some risk impact considered in that as well.

And engineering judgment is very important in the determination of have you got enough diversity. And a great deal of analyses, hazard analyses up front. Some of the other applications like the Department of Defense rely very heavily on the up front analyses and very rigorous processes for the development of the system of systems. And not so much on intentional diversity introduced into the system of systems.

One interesting point is on the Boeing 777. As they went into the development process, there was an intention to use design diversity. And then a decision during the process not to pursue that because of concerns of the complexity it would add in the development of the system. And then the maintenance of the system.

And we found in looking at some of the NASA examples that it is the upgrades that happen that have created the common-cause failures that have caused some problems. The International Space Station is one example where they a multi-tiered control system for the International Space Station. They loaded some upgrades into their top tier. And subsequently had a loss of all the computers on the top tier.

And they had, by design, implemented a reduced functionality fail-safe that resided in the second tier, which was then uploaded to the top tier that kind of saved them on that one. So complexity -- balancing diversity versus the complexity it adds is the challenge in all of these industries.

And what we are hoping to do is -- what we are working to do is to take these examples, translate them into the nuclear context because the applications are different and the needs are different, and use those as the bases.

But we're also taking a different, a diverse approach to developing some diversity strategies as well is looking at more systematic ways of assessing what are the kinds of common-cause failures you have to mitigate.

And what are the diversity strategies that are effective against those? So hopefully we can supplement what is developed from what we have learned from the other industries with the underlying technical basis that says this set of attributes gives equivalent coverage to this set of attributes.

And so we're working multiple paths to try to come to an effective answer that the industry and the NRC can make use of.

MEMBER MAYNARD: I'm glad to see that you are factoring in the consequences of too much diversity or making it too complicated. Just like on the Boeing 777 there, in the industry, we've got to be careful we don't just think about the operators because we also have to maintain these systems.

And you do reach a point of complexity and the number of different things people have to be trained on and knowledgeable about and parts for and everything that we can make it where it is so complicated it becomes less safe than if we had less diversity or less defense-in-depth sometimes. So we have to find that right balance.

MR. WATERMAN: Yes, that's the trick.

DR. WOOD: And one other observation I wanted to make. It was discussed earlier whether or not there were measures that could be used.

And some universities in the United Kingdom have been working on mathematical methods for assessing diversity among software. And we're hoping to -- we've accumulated a lot of reports and articles from those sources. And we are also hoping to have discussions when we visit the United Kingdom to talk about how that is being used there. And what is their actual status.

CHAIR APOSTOLAKIS: That's it?

MR. WATERMAN: That's it.

CHAIR APOSTOLAKIS: Okay. Thank you.

So now we can move on to the general discussion. Do you gentlemen want to come up front here?

MR. ARNDT: What we thought we'd do is Mike has a very brief discussion on operational history.

CHAIR APOSTOLAKIS: Oh, good.

MR. ARNDT: And we'll use that as a segue to the general discussion.

CHAIR APOSTOLAKIS: Very good.

MR. WATERMAN: Now before I bring this slide up, I want to preface this next slide -- it is a historical perspective, if you will, of potential common-cause failures that have been reported in the nuclear industry since 1987 or something like that -- 1987, 1988 through 2006.

They are not necessarily common-cause failures but they were events that were reported to our Operating Experience Report database. And the reports that go into that database are reports of things that could potentially effect accomplishment of a safety function.

And so many, many of the failures we see here -- the reason I did this research -- I wasn't paid to do it, I did it on my own time -- is I was curious about the question about everybody claims that digital systems are very highly reliable.

And I wanted to know well they performed, you know, over the history here in the nuclear industry. And are we getting better at implementing digital systems in the nuclear industry. I mean you would expect to curve the tail down as we get smarter and smarter and learn more and more lessons.

And so I did a histogram, if you will. There we go. Thank you, Steve. And these are some of the things I found. And like I said, I want to preface this. They are not all common-cause failures. But they are events that happened in a digital system that potentially could have been common-cause failures.

And they go back to 1987. You'll notice

no numbers up there. I guess I can give you a number. Represented here -- and it is only on a single screening -- are 340 events over a 20-year period of time.

MEMBER KRESS: What this doesn't show is the denominator -- how many digital systems are out there.

MR. WATERMAN: That's correct. And the reason why is that to tell you the truth, I didn't put in that kind of review to determine how many digital systems were actually in place in a given year because it was like on my own time.

MEMBER KRESS: Well, this could actually be telling then.

MR. WATERMAN: Yes, that would be telling from a faction of total number of systems implemented, yes. But what I was really wondering is well, absolute failure-wise, are they going down? Or staying constant?

MEMBER KRESS: That would tell you something. That's for sure, yes.

MR. WATERMAN: Plus general trends.

MR. KEMPER: Do you have handouts of this?

MR. WATERMAN: Yes, I do. I have handouts of this.

MR. KEMPER: Good.

MR. WATERMAN: Okay, well, I thought we weren't going to but --

MR. KEMPER: No, no, just that.

MR. WATERMAN: Yes, okay.

MEMBER ABDEL-KHALIK: So when you say relative number of events, what does the word relative mean?

MR. WATERMAN: Well, this was on a poster. And I didn't want to put in how many events per year. So I just put relative number of events. A high tower is a lot of events and a low tower is a few events.

CHAIR APOSTOLAKIS: So this is the actual number?

MR. WATERMAN: Yes, the actual numbers went into actually building this. And I just took off the left axis, if you will, and called it relative number of events.

And then across the bottom down in here, I put in certain events that occurred during different years. I could have put more arrows in but it gets kind of noisy after a while. Yikes, you guys are sort of in the way.

But the color slide is coming around here. We had low sequencer events in `95 at Turkey Point.

That was an Allen Bradley PLC load sequencer. That truly was a common-cause failure.

Feedwater control system events, not a safety system, but it was a digital feedwater control system. And mind you this went into the operating event report and I was just trying to determine how are digital systems in the nuclear industry going.

And you can be assured that a licensee does not put in junk for a digital feedwater control system. It costs a lot of money to shut a plant down because their feedwater goes down. So they do a good job of building these systems.

We some oscillator power range monitoring issues from `99 to `03 as they were shaking out various oscillation power range monitor systems that were being put into the plant. One and -- oh, which one was it -- `99, that was actually a microprocessor common-cause failure.

It was kind of interesting. They used -- the company that built that OPRM selected the Intel 286 microprocessor. And the reason why they selected it was because that company had been building mission-critical weapons delivery systems for the Department of Defense for years with that chip. And they knew that chip intimately.

And that's why they went with that instead of something like a 386 or at that time SX or something like that. It turned out that had never used that microprocessor in that system architecture.

In that system architecture, there was a master computer that was calculating oscillation power range functions. And it was synching a slave computer that was supposed to use the same data, calculate, come up with the same answer. And as long as the answer came out to be the same, that channel was assumed to be operable.

And what happened is on the Intel 286 chip, they have a priority baton passing glitch on that chip. It is well advertised on the site. I know I learned to start looking at the site when I'm reviewing these systems.

And when the master would synch the slave processor, depending upon what that slave processor was doing, it might have been doing some self-testing function on memory, when it got synched, the priority baton would be taken away from the maintenance program and given to the safety function program.

The safety function program would do the calculation as it was supposed to. But because of a problem with the Intel 286 chip, sometimes that priority baton did not get passed back down to the routine that had been interrupted. And a watchdog timer would notice that the routine didn't complete on time. And it would reset the slave processor.

And when the slave processor reset, the operator assumed this channel was nonfunctional. So that is a case there of, you know, it wasn't software, it was really the darn chip. Self-testing routine, right, that's -- self-testing, it has been my experience in most of these, self-testing is really -- it has some benefits but it can cause some real problems.

The load sequencer issue was caused by self-testing functions. It wasn't the safety function itself. It was all the self-testing to make sure the safety function would operate correctly.

The main feedwater systems, we had a recirc pump variable frequency drive, that was actually -- that happened just last year at Browns Ferry Unit 3 -- where is Alan at -- Unit 3, right, Alan?

MR. HOWE: Yes, Unit 3.

MR. WATERMAN: Yes, in which that was a datastorm issue that locked up the variable frequency drives on the recirc pumps. So there are all kinds of different things that have been going on in the industry. And most of these are precursors -- as a matter of fact, I'd say a preponderance of all these events are probably safety parameter display systems-related events.

We've got a lot of SBDSs out there. Every plant has got one. And any time the SBDS goes down, they have to report it because the SBDS is used by the operators to accomplish the safety function that is reportable. So we have a lot of SBDS problems here.

We've got some plant security systems -- you know, that is access control for, you know, the protected areas and things like that. We've had some security problems with computers.

Emergency response data systems that are, you know, sound the sirens. Some of those systems have crashed.

And interestingly in the Operating Events Report database, it describes the symptom, it describes the system that was effected. And then it provides the cause. In a lot of those causes, there are no cause reported. System reset, no cause reported. Restart it and keep on moving.

So anyway, across the top, D3 policy and guidance, sort of a timeline of how we've put our policy together -- 91-292 out there, that was sort of the first show at diversity and defense-in-depth. Updated the SRP in `97. And then, you know, for about ten years there we didn't do anything to the SRP. So we're just starting to update it again here in 2006, 2007 time frame.

So anyway that kind of gives you an overall perspective of digital equipment in the nuclear industry. But I want to caution, not all of those events are common-cause failures. They are just events that happened in digital systems that show that digital systems aren't as bulletproof as some people might like you to believe.

Oh, well, we're going to replace our obsolete analog stuff because digital is so much more reliable, right. And when I heard that, it just spurred me to go in and I didn't just do a keyword search where I say I looked at computer and anything that was computer popped up and I just did a count, I had to read those things.

So if there are 340 events here, you can imagine how many events I read because, you know, when somebody took an SBDS down for routine maintenance, that's not on that chart. That is not a failure of a digital system. That's just doing business, you know.

MR. ARNDT: Mr. Chairman, another issue that you raised earlier was this concept of the fact that common mode failure in hardware and software is different because the systems are inherently different, the recirc pump datastorm is a good example of that.

That was a failure of a system not because of the component itself or the software in that component but because of data being provided in a very rapid fashion across a communication bus which is a different kind of failure mode and can lead to a different kind of common-cause failures.

CHAIR APOSTOLAKIS: Well, that was a common-cause failure, rights?

MR. WATERMAN: That one was, yes. That was common-cause failure there.

MR. HOWE: Both of the variable frequency drives failed. Excuse me, this is Alan Howe. I'm the Chief of the Instrumentation and Controls Branch in NRR.

And just for your information, we have a draft of an information notice on that event that is in process right now. It should be fairly close to being issued. So that will provide a little bit of additional background as to what happened in that event.

MR. WATERMAN: That's just a little historical perspective in answer to your question, Dr. Apostolakis.

CHAIR APOSTOLAKIS: Okay.

MEMBER ABDEL-KHALIK: Is there an apples-to-apples comparison with analog systems?

MR. WATERMAN: I haven't done that. It's probably a good idea to say well, maybe digital is more reliable. And it may be.

MR. ARNDT: There have been some studies in the literature associated with apparent reliability after a change-out. There was a paper done -- help me -- I think it was Korea -- after one of their analog to digital change-outs and what their immediate reliability was in terms of very gross availability numbers.

But there has been very little specific detailed analysis of diversity or reliability or availability between the systems to my knowledge.

MR. WATERMAN: And I guess the other thing I'd like to say is despite all of these failures, our nuclear power plants have been safe in every case. They have systems that would trip the plant, or they would take control of the plant, or whatever, none of these are, you know, precursors to TMI.

The operators have always been on top of it. In the case of the load sequencers at Turkey Point, they identified the problem with that particular malfunction like in less than a day, they knew exactly what caused it.

So I'm not saying look at all the ways we could have killed the public or anything like that. That's not what I'm saying. The plants remain safe but there is a potential precursor out there if everybody doesn't do their job right. So far, people seem to be doing their job right. But if everybody doesn't do their job right, well, we have issues coming down the road.

CHAIR APOSTOLAKIS: Good. So shall we go on now with the discussion?

MR. ARNDT: At this point we basically just wanted to give the Subcommittee an opportunity to have a dialogue associated with what they have learned and additional open questions to hope them gain our insights on what the current position is and what you might want to put forth to the Commission on your opinions. So this is your opportunity to get what information you need from us.

MEMBER MAYNARD: What I haven't heard --

I've heard a lot about what our plans are and what we are planning to do and the various groups and committees and things but I haven't heard are we to a point yet of identifying what we are really looking at proposing in the way of new change?

I understand the branch technical position here but on more diversity or less diversity? More defense-in-depth? Less defense-in-depth? Or where are we going with it? I haven't heard too much about that.

MR. WATERMAN: Well, until our research gets completed, I really -- I don't want to force fit a diversity strategy on the industry that just isn't a very good strategy.

MR. KEMPER: Yes. I think we really need to interact with the industry more and be sure that we understand what their issues are primarily so we can digest those and consider them all in conjunction with the research results that we are obtaining right now. So we're probably a couple -- two, three, four months away from being at that point yet.

MR. HOWE: This is Alan Howe again. I'll just add a little bit to this is that the existing Commission policy and the branch technical position right now provide an overall framework. It is a workable framework but as you have seen from the discussion and presentation today, there are questions that are coming up in terms of how do you apply this? How do you answer that question?

I think there was a question early on about what constitutes sufficient quality. So we're now trying to fill in, if you will, and address some of those questions. So one of the outputs would be to identify what are the key questions out of the problem statements? And go forward with addressing them with clarifying what the position would be.

With regard to that, as you've seen right now the policy, as we are going forward with implementing it, is that diversity is an important aspect in terms of overall safety at the plants. But it is now just really answering these questions how do you identify what is the adequate level of diversity and defense-in-depth and how do you address the solutions to that problem.

CHAIR APOSTOLAKIS: So if I look at the SRM again, it says the short-term milestones should address critical path actions. The critical path actions are related to the eight statements -- problem statements? These are --

MR. MAYFIELD: This is Mike Mayfield.

There are near-term and longer-term actions and deliverables for each of those areas.

CHAIR APOSTOLAKIS: For each of these.

MR. MAYFIELD: Not so much for the -- in diversity, it is not that they are broken out by each of the eight. But for each of the six task working group activities, there are near-term and long-term activities.

CHAIR APOSTOLAKIS: Is it six or eight?

MR. MAYFIELD: There are six -- for diversity and defense-in-depth, there are eight pieces to the problem statement. There are six task working groups.

CHAIR APOSTOLAKIS: Oh, I see.

MR. MAYFIELD: Of which diversity and defense-in-depth is one of the six. Does that help? No?

MR. HOWE: Part of what we are doing is we are interacting with the industry to identify -- you talked about the critical path items -- which ones are the -- you know, from the industry's perspective, what are the critical path issues that need to go out there? That way it gives us -- informs us in terms of how to apply the right resources in addressing those issues earlier whereas some of the other ones could be longer-term-type of issues.

That's part of what we have asked for feedback on the problem statements.

CHAIR APOSTOLAKIS: Well, let's clarify. The six groups --

MR. MAYFIELD: Yes.

CHAIR APOSTOLAKIS: -- they were presented earlier?

MR. MAYFIELD: We talked about them and listed them for you.

MR. HOWE: If I could, I'll just give you a little bit of perspective on that. When we briefed the Commission back in November, they issued the Staff's Requirements Memorandum. Subsequent to that, a charter was issued by the EDO to form a Steering Committee and also develop a project plan.

As we have developed in that process, what we did is we looked at the key areas. And we identified six key areas that we then further -- under the oversight of the Steering Committee, we further broke down into what we call our task working groups to deal with the individual issues.

And I'll try to give you the list here off the top of my head. Cyber-security is one of them. Diversity and defense-in-depth is a second key area.

Integrated control rooms communications, integrated control rooms human factors, risk informed, and last area is licensing issues.

CHAIR APOSTOLAKIS: Well, you did a good job.

MR. HOWE: So we tried to chop apart the big problem and establish what we call these task working groups to focus on the individual areas. There is also going to be interactions with the external stakeholders on that as well as interactions both at the working group level and at the Steering group level to ensure that we do go forward with a coherent approach here.

Because what we don't want to do is to have the different parts getting out of synch and we have recommendations coming from one group that are at odds with recommendations from another group.

MR. KEMPER: Yes, if I could add just one more segue onto what Alan said and primarily we didn't just think of these things from thin air, we drew this from industry. We have been interacting with industry for quite some time on this.

And I think our first meeting was back in March of last year where we started talking about some of these issues. And then we had another comprehensive meeting I think it was in October.

MR. HOWE: October 19th.

MR. KEMPER: And that is really where most of the issues were bubbled up, if you will, to us from the industry. And so from that, that is where we put together the picture of what you see now as far as the critical issues that have to be addressed to address the short-term critical path items.

CHAIR APOSTOLAKIS: So when the Commission says critical paths, these six are the critical paths?

MR. HOWE: These are the key issues that we have identified. And now what we are working on is subsets from those broad issues, what are the critical issues --

CHAIR APOSTOLAKIS: Within each of the areas.

MR. HOWE: -- that we need to focus on immediately. And which ones will be dealt with in the longer term.

CHAIR APOSTOLAKIS: Okay. That makes it clear.

So today then we heard only -- well, we focused on Key Area B, diversity and defense-in-depth. That's correct?

MR. ARNDT: So we'll talk about risk-informed this afternoon.

CHAIR APOSTOLAKIS: This afternoon, okay.

MR. ARNDT: Now, if I could --

CHAIR APOSTOLAKIS: We are asked to comment on this? Then we have an SRM that says the Committee should provide its view to the Commission on staff's effort related to digital instrumentation control. The Committee should consider potential means for providing reasonable backup if appropriate. Are we writing two letters, Gary? One on the staff's efforts? And one on --

MR. JUNGE: No, we're just writing --

CHAIR APOSTOLAKIS: One letter.

MR. JUNGE: Yes, we're writing one on the SRM.

CHAIR APOSTOLAKIS: This was Mike Junge.

MR. ARNDT: Yes, George. The reason we structured this presentation the way we did is you need to write a letter on generally what we are doing but also specifically the back-up issue which --

CHAIR APOSTOLAKIS: That's correct.

MR. ARNDT: -- goes to this issue and other issues associated with D3.

CHAIR APOSTOLAKIS: But we cannot really say anything on the four key areas that we are not discussing today.

MR. ARNDT: That's correct.

CHAIR APOSTOLAKIS: Unless we go back to the research plan which I don't think would be the appropriate thing to do.

MR. MAYFIELD: Well, if you wanted to do that what we would need to do is get you the task plan, the project plans for each of these six areas.

CHAIR APOSTOLAKIS: These areas.

MR. MAYFIELD: And I think it would -- to get you that information in a timely fashion so that you could review it and we could engage with you in this setting or the full Committee, I think that would be probably useful but challenging in time.

CHAIR APOSTOLAKIS: What do my colleagues think? I mean the Commission's charge is very clear. The staff's effort related to digital I&C. And then specifically on backups. So we know about that.

So with the afternoon's presentation, we can address also the key area on risk-informed digital I&C. But we will not have any plans for how to handle cyber-security, highly integrated control rooms, and the licensing process.

Should we then agree that maybe at the full Committee meeting we'll have a briefing on your plans in these areas?

MR. MAYFIELD: Why don't we take as an action and work it back with the ACRS staff and come back to you with a proposal as to what we could do in two weeks to give you the broad picture about all six working groups. Obviously it can't be at this level of detail.

CHAIR APOSTOLAKIS: Right. But what do you --

MEMBER MAYNARD: I'm not sure that we -- well, first of all, I think that would probably be good, the big picture view. I'm not sure that we have to evaluate or review each specific area.

I think probably of bigger value would be are these the right areas. You know is there something else that is not there or whatever. But are there -- do they have a plan in the right areas or is there some big part of the picture that is missing here.

CHAIR APOSTOLAKIS: To answer this, we'd would definitely need what Mike said. We'd need this overall view. So we can address this question and then maybe focus more on the D3.

MEMBER KRESS: Well, I think we need the overall picture. But two weeks is not a lot of time.

CHAIR APOSTOLAKIS: It is not a lot of time but they can get it done in that time.

MR. MAYFIELD: Given the amount of time we are likely to get on a full Committee agenda to give you a snapshot of the six areas --

MEMBER KRESS: This one of those cases where I think we need to have the written invitation far ahead time to read because we're not going to be able to get enough --

MR. MAYFIELD: We can certainly provide you the draft information that has been shared publicly, recognizing it is draft.

MEMBER KRESS: That's all right. We do that all the time.

MR. MAYFIELD: And we have been specifically asking for comment and frankly to have comment back from the Committee would be very useful at this time. Six months from now, it is going to be a whole lot less useful simply because we're going to be moving.

MEMBER KRESS: So I think we ought to comment on the whole plan --

CHAIR APOSTOLAKIS: I think so, too.

MEMBER KRESS: -- because I think we're asked to.

CHAIR APOSTOLAKIS: That's what the Commission wants.

MEMBER KRESS: Yes. And the only way to do it is to get the written information at least a week before the meeting.

CHAIR APOSTOLAKIS: Yes. And this should go to the full Committee.

MR. ARNDT: We will get that to you late this week.

MEMBER KRESS: Okay. That would be good.

CHAIR APOSTOLAKIS: I think you can have a shorter presentation than what was presented today. A lot of it, I think, the members are more or less familiar with.

MEMBER KRESS: Yes.

CHAIR APOSTOLAKIS: So a discussion of each of the six areas and then saying for diversity and defense-in-depth, here is a little more detail. For risk informing, here is a little more detail it. That should do it. We have an hour-and-a-half?

PARTICIPANT: Yes.

MEMBER KRESS: Now we had a full meeting on the risk informed some time ago. I don't know if that's --

CHAIR APOSTOLAKIS: More than a year ago

I believe.

MEMBER KRESS: Yes, I don't know if that has changed a lot.

MR. MAYFIELD: One of the other points that I guess I had wanted to make with you gentlemen is that there is a disconnect or a potential disconnect in schedule interest for new reactors versus the operating fleet. And where the fuel cycle facility interests fit in in that schedule is something I guess I'm still interested in learning about.

The approach we are taking, when you see these plans, you will see some discussion about interim guidance and then longer-term where we would fix up the SRP, fix up the reg guides and so have you. The intent is that we will provide interim guidance to support the first schedule need, which is almost always going to be the new reactor interests.

I think when we first got into this, that wasn't quite as clear as it has become. Where the pacing issues appear to be the COL applications as well as some of the design certification reviews for new reactors. So we are looking at interim guidance to make sure we are actively moving to support the rate-limiting licensing activity.

Mike talked about the longer-term research that will -- as systems continue to evolve, as interests continue to evolve, then I think the research fits in further adjustments downstream. But our interest -- and I think the industry's interest is to provide guidance in a timely manner, recognizing that may evolve a little bit for future systems, future applications. But that's -- I'm sorry?

CHAIR APOSTOLAKIS: This memo from Mr. Grobe says that there are six attachments. Are these relatively short attachments? I mean maybe we can get those. I mean it is up to you.

MR. MAYFIELD: What letter are you looking at?

CHAIR APOSTOLAKIS: It says in order to -- from Grobe -- Digital I&C Project Plan.

MR. MAYFIELD: Yes. We can provide those. It's not hundreds of pages.

CHAIR APOSTOLAKIS: Good.

MR. MAYFIELD: It's 20, 25 pages.

CHAIR APOSTOLAKIS: All together?

MR. MAYFIELD: Yes.

CHAIR APOSTOLAKIS: Yes, that's fine.

MR. MAYFIELD: So it is probably --

CHAIR APOSTOLAKIS: That probably would be a good think to have.

MR. MAYFIELD: It is just a matter of setting somebody in front of a computer, hitting the print key and getting them in front of a copier to get copies over to Gary.

CHAIR APOSTOLAKIS: Very good.

MR. HOWE: Just one other thing I would offer up is that in the Commission's SRM back in December, they also had staff set up a digital instrumentation control website. And that website was established I think in January as a kind of Phase I process.

But that is also information that is readily available right now in terms of background. Some of these subjects that we have talked about in detail today and some of the topics of the working groups are also described in the different pages in the website.

CHAIR APOSTOLAKIS: And that is at the nrc.gov?

MR. HOWE: It is an NRC public website.

MR. ARNDT: But we will give you the specific address in the transmittal.

CHAIR APOSTOLAKIS: Good. Good.

DR. GUARRO: George, this is Sergio. Can

you hear me now?

CHAIR APOSTOLAKIS: Yes.

DR. GUARRO: Oh, okay. I have a question with respect to the research in the diversity and defense-in-depth. Is there anything specifically in your research plan that looks at whether one can go beyond the block approach, so to speak?

In other words, if I understand correctly now a common-case failure is assumed to occur in one of these blocks. And everything proceeds from there. Wouldn't, you know, a path would be perhaps a little bit less conservative if possible to look beyond that level? And try to see if there are ways of being able to classify types of common-cause failures within a block?

And also from the point of view of the remedies, prove that the remedy indeed addresses with sufficient diversity a particular type of common-cause failure?

CHAIR APOSTOLAKIS: The blocks you are referring to are the ones in the old NUREG, right?

DR. GUARRO: Right, right, well, yes, I'm referring to the current approach. So, you know, is there some attempt to look beyond that level of -- well, I think is pretty top level in terms of the assumption made.

MR. KEMPER: Sergio, this is Bill Kemper, let me start it out, Mike, and you just jump in here. We really hadn't talked about it from the perspective yet. Your point is well made. The block strategy of trying to diagnose the portions of a digital processing system that is subject to a common-cause failure is difficult to decipher.

And so generally speaking what the industry inventors have done, they have just assumed the whole platform fails, right, because to provide an analysis with finer granularity would mean you would actually be looking at circuit boards, you would be looking at microprocessors, semiconductors, that sort of thing. And it has generally been my experience in talking with many folks over the years on this, it is just not cost effective to do that type of analysis. That is why they don't generally get into it in that detail.

DR. GUARRO: Well, I wasn't referring to much to the, you know, circuit board level. I mean the block approach is taken -- isn't it taken also at the functional level so for other types, isn't it also assumed? And the same way for software? Or, you know, any of these major functional components?

MR. LOESSER: On the analysis we've seen so far, no one has even gone to the block level yet because of the increased level of complexity that this would offer. If, however, a licensee did go down to the block level or even went further, we would have no objection. It might be a little more difficult to review but we'd certainly take a look at it.

DR. GUARRO: No, I guess what I'm asking, I understand that currently that is what is done because nobody is able to do better or thinks that it is not possible to do better but as part of your research, if one wants to try to see how one can be a little bit less, you know, broad-brush conservative, so to speak, shouldn't the research try to determine if there has been a circumstance that permits to go to a lower level in some areas?

I'm not saying -- obviously I intuitively agree that in certain areas, probably we haven't made any progress. But maybe in some of the areas in which the present approach is applied, one could go a little deeper and save themself some conservatism.

CHAIR APOSTOLAKIS: Well, that would be a longer term issue, right?

DR. GUARRO: Right, right. I'm talking about longer-term research. But I mean since in the discussion I haven't heard anything that goes in that direction, that is why I was asking the question.

MR. KEMPER: No, this is Bill Kemper again, clearly we're trying to focus on a set of suitable diversity attributes because right now 6303 just mentions them in general. And it doesn't really give you any guidance on how to deploy or implement that guidance. So that is what we are trying to do now is refine that guidance from how do you build in diversity into your design.

What we're seeing pretty much now is what is being submitted to us is here is our design. Now let's see how that matches up with 6303 criteria. And then find ways of coping with the lack of diversity, in many cases, that exists with a given design.

But it is certainly something that we can look at in the long term, I believe, as we work through this research. We just haven't talked about it in detail. It doesn't mean that we are not thinking about it or going to do that. That is probably the next phase.

DR. GUARRO: You know it would seem that in order to answer the question of how much diversity is enough, one has to understand a little bit more about, you know, the nature of the problem that effects the common cause issue. And so that, you know, you can decide what type of diversity works for what, so to speak. So anyhow, that's just a thought.

CHAIR APOSTOLAKIS: Thank you.

Okay, so it seems like we are beginning to formulate the presentation to the full Committee.

MR. ARNDT: Let me reiterate. I think what I heard was the general overview of what we are doing and why we are doing it. And what the structure is. I'm sorry -- a general overview of what we're doing, why we are doing it, what the plan is about, how we are getting there. A short review of what we talked about this morning. Did you also want a short review of this afternoon's presentation?

CHAIR APOSTOLAKIS: I think that would be useful, yes.

MR. ARNDT: Okay.

CHAIR APOSTOLAKIS: Although the Committee is probably more familiar with the afternoon. But so you use your judgment.

MEMBER KRESS: Since the last time we had this meeting, there have been a lot of new members added.

CHAIR APOSTOLAKIS: And we have a lot of new members, you are right.

MEMBER KRESS: So it might be worthwhile.

MR. ARNDT: Okay. We will have to manage this because of the timing issues. But we will get with you. And we will start with that as a start and work through that.

MR. MAYFIELD: Well, let me add -- this is Mike Mayfield -- let me add that I think it would useful for the full Committee to hear it because I think the risk area is one where there is probably the greatest disconnect with the industry based on what I heard. So I think that would be useful for the Committee to hear. Where we are and why we think we are going where we are going.

CHAIR APOSTOLAKIS: And I'm not sure now will the industry have time at the Committee meeting?

PARTICIPANT: Yes.

CHAIR APOSTOLAKIS: About 15 minutes or so?

PARTICIPANT: Yes, we will be providing that time.

CHAIR APOSTOLAKIS: Yes. So we should take that into account.

MR. ARNDT: We will work it out, yes.

CHAIR APOSTOLAKIS: Okay.

MR. WATERMAN: This is Mike Waterman.

Just one comment.

CHAIR APOSTOLAKIS: Yes.

MR. WATERMAN: The purpose of the research stems from if an applicant came to the NRC today and said we have a diverse system. We have used different microprocessors and different channels. We have used two different management teams and development teams to develop the software.

We have rearranged the software so there is a different order of software processing in each channel, and we think that is enough diversity -- it sounds good -- but we don't have any guidance at the NRC right now that says that is good enough or not good enough or any basis for saying why it is not good enough.

So the licensees and the applicants out in the industry haven't got a clue of what to do for diversity and defense-in-depth because frankly I don't think we've got a clue on how to handle it. And that is what the focus of this research was is to try to nail that down so that when a licensee comes in here, they know what the answer is before they come in. And we know what the answer is when we take a look at something.

CHAIR APOSTOLAKIS: Now one other point,

we've heard the words short-term, long-term. Mr. Mayfield said earlier that under the eight problem statements that refer to defense-in-depth, there are long-term and short-term issues.

Can we make that a little more explicit at the full Committee meeting? What is short term? What is long term?

MR. MAYFIELD: Yes, the challenge is that, as several folks have suggested, we are looking to prioritize, looking for interest from the industry on priorities for the various activities. Specific dates, when you get this information, you are going to see a lot of open slots in the table.

CHAIR APOSTOLAKIS: Right.

MR. MAYFIELD: And the reason is we are waiting on that priority information to finalize the specific schedules. But relatively we can give you a sense of what --

CHAIR APOSTOLAKIS: That's what I mean.

MR. MAYFIELD: -- short- and long-term mean.

CHAIR APOSTOLAKIS: Yes, like Mike Waterman just said, you know, we really need these because we don't know and the industry doesn't know. That's a short-term need.

MR. MAYFIELD: I look at it as short term

CHAIR APOSTOLAKIS: Yes, it is short term.

MR. MAYFIELD: Yes.

CHAIR APOSTOLAKIS: But you don't have to tell us, you know, by May such and such, no. That would be useful.

MR. MAYFIELD: We will give you some insight on that.

CHAIR APOSTOLAKIS: Anything else?

(No response.)

CHAIR APOSTOLAKIS: This is a happy meeting. We'll break for lunch and be back at one o'clock.

(Whereupon, the foregoing matter went off the record at 11:47 a.m. to be reconvened in the afternoon.)

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

1:00 p.m.

CHAIR APOSTOLAKIS: Okay. We can start again.

And the first presentation is from NEI.

MR. MARION: Good afternoon. My name is Alex Marion with NEI. And with me is Kimberly Keithline.

I just would like to make a couple of comments regarding the staff activity relative to modeling, if you will, digital systems. Our basic needs are rather straightforward. One is we want to ensure we have quality PRAs, probabilistic risk assessments, and we minimize requests for additional information that the NRC may call for.

And we want to be able to use risk insights to allow us to focus on the risk-significant aspects, if you will, of digital system performance. And, of course, in order to do that, operating experience is extremely important in developing a database so you can make some reasonable estimation of failures, et cetera, and get a better understanding of the performance of these systems.

So we agree that that is a very important area. And we are going to look into that. And also work with the NRC staff to make sure we are not duplicating efforts unnecessarily.

But I do want to make it very clear that we think the -- we don't support the detailed modeling aspect that the staff is going to talk about this afternoon or any research related to advancing the state of the art. We don't think that that is needed relative to digital system applications in nuclear power plants.

And the reason for that is very fundamental. Every industry in this country has applied digital technology except the nuclear industry. And a lot of the utilities are hesitant in doing that because of the uncertainty in the regulatory process.

But what we have in place with the Steering Committee and these task working groups will provide some structure to what the issues are so that we can stabilize the regulatory process going forward. But we need to keep a focus on research that will accommodate or support that activity in the near term. And that's basically where we are coming from.

We also believe that the existing PRA methods are adequate and sufficient to model digital technology. And we haven't seen any work indicating that there are gaps, if you will, in the use of PRA technology today.

I'm trying to recall if the NRC had done any work to identify gaps or vulnerabilities in PRA models that are being used today. I don't recall.

MS. KEITHLINE: There was -- and help me out here, guys, if you need to -- I think there was a NUREG-6901 that had a list of reasons why you might need to do more detailed or dynamic-type modeling. And our industry folks who are knowledgeable in this area think that those tend to be things that people wouldn't use in safety systems.

And, Jeff, you may want to -- Jeff Stone from Constellation probably has a better, more detailed answer. I'm pretty new to the PRA part of this.

MR. STONE: We have looked at -- oh, I'm sorry, Jeff Stone from Constellation -- we have looked at the 6901 and the newer research that we reviewed in December that hasn't come out yet, I don't believe that has a number that I know of yet -- at this point we haven't seen any quantitative evaluations that show dynamic modeling will have a significant impact on overall core damage frequency or a significant impact on the probability of failure of a system.

And what will be driving it is probably the software probabilities we use or potentially a hardware common cause failure probability between computers. We do encourage the research to go forward if that is the intention.

But before we implement something as complicated and as costly as dynamic modeling, we feel that there should be some sort of cost benefit to show that there is a significant change to our models to require this sort of expense.

And I think I've gone over my time but that's my opinion.

CHAIR APOSTOLAKIS: Thank you.

MR. MARION: Yes, with regard to dynamic modeling, we are concerned with the added complexity it is going to provide. And then quite frankly the practicality of it all. We feel reasonably confident in the techniques currently available.

We think that in the near term, as an alternative to dynamic modeling, we need to do some work to better define software failure probabilities, focus a little bit of effort on failure modes and effects, and as we said earlier, start collecting and evaluating operating experience with the existing systems.

And we think that from a design perspective, we can deal with the recognized set, if you will, of common cause failures such that we can provide reasonable assurance that these systems will function properly and maintain safety at the plants. And that completes my comments. I don't know if you want to elaborate on that.

MS. KEITHLINE: We've -- this is Kimberly Keithline -- the part that we are most concerned about is what you will see as the third problem statement within this task work group on risk related to developing or implementing state-of-the-art techniques and the dynamic modeling as an example.

There are two other problem statements that we are more on board with, the first dealing with more life refining techniques to be used for design certification and COL applications, how we would use them near term to support using digital I&C in the new plants.

And then the second would be more like a simplified approach to be applied to existing plants and maybe new plants -- existing plant upgrades -- we think that may be a useful thing that would help support and even improve diversity and defense-in-depth evaluation process.

And the NRC staff, I think they are planning to describe what they are doing in all three of those areas. So we are more aligned on the first two and it is really the third area that we have the most concern with.

CHAIR APOSTOLAKIS: Are you opposed to this particular approach? Or attempts to develop models for risk evaluation in general? The risk evaluation with a digital I&C obviously. In other words to bring the digital I&C into the PRA.

Now you may say that you don't see any value to this dynamic modeling. Or this is a subject we shouldn't worry about at all.

MR. MARION: It is the value aspect of the dynamic modeling. We just think it provides unnecessary complexity and really don't think it is needed because of everyone we have talked to within the industry from the standpoint of PRA practitioners are indicating to us that the PRA methodology today should be adequate and sufficient to effectively model digital systems and determine the risk significance of any problems you can have with those system designs.

CHAIR APOSTOLAKIS: Well, I see it as the problem having two parts. The first part is identifying potential failure modes. Maybe additional minimal cut-sets or whatever. That will be a combination of the traditional events that we have in the PRA plus a contribution from digital systems. And that is extremely important also as we said earlier to discuss diversity, and defense-in-depth, and all that stuff.

And then you have the issue of quantification, which is much tougher in my view and much more difficult to achieve. It seems to me that for the first part, my view is that it is a necessary thing to do and we should try to identify and to develop those methods to understand because the failure modes of software are not understood as well as the failure modes of analog systems or hardware obviously so the issue is there, you know, are we missing anything and so on.

When it comes to probabilities, I think it is a much longer-term issue. And, you know, there are certainly many ideas how to approach the issue. Is the dynamics of the situation an essential part of it? Or can we do it somewhere else? As you probably know, there have been fault trees in the past that have been applied to digital systems.

So the issue -- especially because a lot of the failure are due to specification errors which are the equivalent of design errors and we really don't know how to handle those.

But the first part, I guess, is really more urgent, the identification of the failure modes it seems to me.

MR. MARION: Yes, we also feel that from the standpoint of software performance, that the software development process can address a lot of the issues to provide some level of reasonable assurance. The question becomes one how much is enough.

You know you are not looking at an environment where you have one individual cranking out lines of code anymore. That is the way it was 15, 20 years ago. Software development has changed significantly in that time.

So we think there are adequate techniques out there now that can be credited in assuring some sense of reliability in the performance of the software.

CHAIR APOSTOLAKIS: But the words reasonable assurance, of course, are part of the traditional way of doing business.

MR. MARION: Right.

CHAIR APOSTOLAKIS: We want to quantify -- and I remember I believe it was the AP 1000 and maybe others where they just assumed that, you know, all the software went down, see what happens, it was more of a sensitivity kind of analysis rather than quantifying what is going on.

Okay, any questions?

(No response.)

MR. MARION: Thank you.

CHAIR APOSTOLAKIS: Thank you very much.

And now we move on to Mr. Doutt, NRC short-term activities associated with risk-informing digital system reviews.

MR. ARNDT: Let me give a brief introduction. This afternoon's presentation is going to be a series of presentations talking about where we are in the terms of digital system research as well as the shorter-term activities.

Cliff is going to give a presentation basically on the current status associated with what the TWG, task working group for risk is, what the problem statements are, and how they align with our current work.

After we go through that, I'm going to give a short update of where we are in the dynamic reliability modeling.

And then we're going to have a longer

presentation on the traditional reliability modeling, which is the parallel program that you have heard about but not as much detail as the dynamic reliability modeling.

Then I'm going to give you a real short presentation on where we are in regulatory guidance. It will become obvious as we go that since we have been more directed toward short-term guidance, the longer-term formal regulatory guidance in this area has been put back. But I'll give you just basically a five-minute version of that 30-second statement at the end of the day.

CHAIR APOSTOLAKIS: Okay.

MR. DOUTT: We'll try this again. Good afternoon. My name is Cliff Doutt. I'm with the PRA Licensing Branch in the Division of Research.

CHAIR APOSTOLAKIS: PRA Licensing Branch, are you licensing PRAs?

MR. DOUTT: No, licensing as in licensing actions.

CHAIR APOSTOLAKIS: Oh, I see.

MR. DOUTT: And don't I wish. In the Office of Nuclear Reactor Regulation. Basically I think Steve kind of did the beginning here but what we're basically trying to do here is do a presentation on what the working group has come up with in the way of project plans, tasks, problem statements, and whatever on how we try to incorporate risk insights into methods to review digital I&C systems.

I'll tend to use digital I&C systems a little more than other people have done. It is simply because I think it is a little wider subject that just defense-in-depth and diversity. That is keeping with our project goals in long-term work.

We have had a couple of meetings of the working group so far. The first one was in February, on the 23rd. And we had a second one April 11th and 12th. That's with industry, public meeting, to try to hash out, again, the problem statements and project plan. We've issued -- well, we'll get into that but we've issued a draft of the project plant.

Based on this, there are future meetings planned. One for hopefully the end of May. And so everything we are doing here is pretty preliminary. Keep that in mind on this regard to ongoing work.

This gets us to more introduction. We'll do a background which is just a quick review of where we think we are right now. We'll go through the problem statements, what we think the goals of the TWG should be and maybe what we think they are going to be, project plan, what we think the deliverables will look like, a very general approach, I would think, will address the problem.

And, again, we'll do a little bit of discussion on application of PRA so far in digital systems and where we think this has occurred. And what has happened. And out of that, I'll give you a real brief insight as to what we've seen so far.

And, again, I'll make a list of challenges that we would think we will need to look at, resolve, or address in order to implement PRA in a -- digital system in a PRA. We'll discuss briefly on schedule and then there will be a conclusion.

And this is a refresher from this morning really. You've seen the presentations on deterministic defense-and-depth and how to deal with that. That's the current way of doing it. Specific digital I&C system development, design, testing, maintenance, and staff review processes are basically deterministic. That is how it is being done.

The process is to ensure adequate quality, reliability, and diversity and defense-in-depth when implementing a digital I&C system. Why we're doing what we are doing now, one of the reasons is is within the staff requirements dated December 6th, there was an item in there to address risk-informing as a topic for deployment of digital I&C.

So one of the things in deterministic space as far as that staff requirements goes, licensing actions to date involve usually a significant amount of staff and licensing effort. So one of the things is to see how we can address that. And based on that SRM, the TWG was formed. And where we are at.

Current short-term tasks and what we believe currently is existing guidance does not provide us sufficient clarity on how to use current methods to properly model digital systems in PRAs for design certification applications or license applications under Part 52.

There is a second part to this, too, which is using current methods for PRAs. In that respect, the NRC has not determined how or if risk insights could be used to assist in the resolution of key specific digital system issues in operating reactor licensing action requests and specific defense-in-depth and diversity.

Just a little clarification, obviously the first one is Part 52. The second one which is operating plants, one of the reasons to divide those is just requirements of PRA in general. In Part 52 there is a PRA in operating plants. A little different perspective. So one of the reasons to split those.

This is the long-term tasks. I'm not discussing it except just to bring it up and that it exists and we are considering the work to try to develop a state-of-the-art method for a detailed modeling of those systems. And one of the things is to advance the state of the art in order to provide a comprehensive risk-informed decision-making framework. We don't believe we have that right now.

And this would include licensing reviews of digital systems for current and future reactors. So that is a fairly significant long-term task. And a wider scope than the short term as you'll see as we move forward.

MR. ARNDT: This is really what you heard the industries say. They are not in agreement with us in the fact that the staff currently does not believe that the state of the art is such that you can do detailed quantified digital system reliability models to a standard like 174. So the words here have been carefully chosen to not make any specific statement as to what the state of the art is. We refer to it as not been established from a regulatory standpoint to take into account that there is a disagreement on this level of the state of the art.

The first two tasks, number one in Part 52 space, on what is necessary for that particular licensing action and number two is short-term use of risk insights for things like D3 and other issues was the points that Kimberly was making earlier.

MR. DOUTT: Next slide. So from the risk task working group goals, we've set the up -- basically improve the NRC review process is obviously a goal.

We also thought if we could implement risk assessment in a D3 or import it in for digital systems that we could look at -- get a better insight into vulnerabilities including diversity and defense-in-depth. And it is a little different review structure than design basis and a strictly deterministic way of looking at it.

That may help improve some insights as to where -- that may improve on the question from this morning as to where and when and how much. I guess this is a place where we think there might be some benefit.

To do that -- and I split the task down --

is to provide some interim guidance on the use of current PRA methods in modeling digital systems. And we would do this in design certification and COL area.

The other part of this is provide some type of interim approach on use of risk insights in the licensing review. And, again, we split this. Let's see if there is anything else. Again, basically that was --

CHAIR APOSTOLAKIS: So why do you have the two sets separated?

MR. DOUTT: One of the reasons to separate them -- this was the request but part of it is, too, is how we think going forward the COL design certification has a PRA and a rule structure and different acceptance guidelines. Operating plants can come in risk-informed, non-risk-informed. And acceptance guidance we are not as clear on and it is different.

And that's how we -- we feel -- and the two tasks are just different. To look at how those models may be structured. Now -- and I see comments but one of the --

MR. STONE: Cliff, can I --

MR. DOUTT: Sure, go ahead.

MR. STONE: -- can I just comment one

point.

CHAIR APOSTOLAKIS: Give your name please.

MR. STONE: I'm sorry, Jeff Stone, Constellation. What we had considered the second for was BTP-19 right now is relatively deterministic. It does have the best estimates. We were looking for are there any ways we can use any risk screening risk insights into those in the BTP-19. If there is any way that the NRC would find acceptable or we could find acceptable between -- in the task working group and with the NRC?

MR. DOUTT: And we weren't quite that specific.

CHAIR APOSTOLAKIS: But all four are short term, right?

MR. DOUTT: Yes. That is the intent.

Now project plan, currently we are looking to receive a couple of industry technical papers. One is on PRA methods which applies to -- when we go into the problem statements you will see that, PRA methods of either a simplified or whatever -- there is also a document on lessons learned. We would like to incorporate those with staff PRA risk insights which we hope will look at key principles and methods and what we have done so far. We just need to go back and take a look and see what has happened. Most of that has got to be in design cert. space.

Operating reactors have not employed PRA in a digital system in the licensing. And the other thing is to look at research as what we've done to date. And this is a wide focus. Not just what we've done, completed, go out to industry, academia, the usual things, and see if we can pull some insights in and try to incorporate them in a short-term solution.

The other thing, which is relatively important -- I think it is very, very important actually -- is to integrate these results with the other two TWG recommendations. After you listened this morning, it is a very deterministic process with deterministic acceptance criteria.

If we are going to do this, it has to be consistent either with the SRM, regulations. We have to look at that way or we have to look at it as our policy issue. Right now we are leaning for short-term is to be consistent with current regulation and consistent with the other TWG recommendations.

In other words, we would be, like 174, it is complementary. We would provide complementary insight. But we wouldn't -- we'll get further into this as far risk-informing defense-in-depth goes. I'd like to avoid that.

Now for project deliverables, for Problem Statement 1, which was back -- issue interim guidance and address use of current methods, modeling of digital systems, and again, for COLs and/or design certification.

In the longer term, we would intend to update regulatory guidance as needed. And that is SRP, Reg Guides, and NUREG best practices, things like that. But we thought we need to pull those off into long term. It is not going to be a short-term resolution.

One thing I should mention, too, on this, and we did have a discussion last week on it, as the papers from industry, as to how those would be reviewed. To do a short-term project, we were looking at using that information and incorporating it in what we are doing. If it ends up being a formal review like a topical report or something like that, that can impact scheduling. So we are discussing how we want to handle that.

MEMBER MAYNARD: Cliff?

MR. DOUTT: Sure.

MEMBER MAYNARD: Just briefly for me on interim guidance versus a long-term change in the standard review plans, my understanding that somebody comes in with a COL application that they are tied to the SRP or whatever that was in place six months prior, how does the interim guidance play into this if we don't -- if we put as a longer-term item as updating the standard review plans and the reg guides, what are they bound to when they come in with a new COL application?

MR. ARNDT: Let me.

MR. DOUTT: Okay.

MR. ARNDT: They are bound to the regulations and guidance six months ahead of time, just like what -- what's the reg guide, I can't remember off the top of my head, that provides that guidance?

MR. DOUTT: 1.206.

MR. ARNDT: 1.206, thank you. This interim guidance is going to be specifically -- and this is true for most of the TWG actions regardless of area is going to provide clarification, additional information, and that kind of things.

There are specific rules on what we can do without doing a formal regulatory guide update or a formal SRP update. The idea here is to provide that additional information as to what we really mean, what the acceptance criteria really means, what the level of detail -- the word we are using is added clarity associated with this.

In Problem Statement 1, if you recall, the statement was we want to -- there is a concern that there is not enough clarity in the guidance associated with digital systems in terms of the design cert. in COL PRAs. So that is a specific regulatory decision. Accept the results of those PRAs.

And what we are trying to do is provide additional clarity in the guidance that is out there, which is very general, as you know, as to what is good enough to make that particular regulatory finding that we are comfortable with that.

MR. ROTA: This is Rick Rota from Research.

That is correct, Steve, but they are not bound to the SRPs and reg guides that are in place. But they need to explain how they meet them or why they don't meet them. So they would, you know, if we have guidance and they say we will meet this guidance, then obviously we found that as acceptable approach.

MR. DOUTT: And the goal in the sort term is to be consistent with current guidance and regulations. We are not foreseeing that that would be a change. In the long term, though, on a comprehensive look at this, that may, in fact, be required.

MR. ARNDT: And the reason we carry a long-term outcome of the short-term goals is we want the guidance to be as clear and concise and usable as possible. But the process of putting it into a reg guide or an SRP update is a two- or three-year process.

MEMBER MAYNARD: And I don't want to belabor it but it seems to me like we are kind of heading down a path where we are going to end up with is this really clarification? Or is this new requirements and everything? I can see a lot of that coming down the pike with this approach.

MR. ARNDT: We understand that. And that is also a concern of our industry colleagues. But we also have a concern that we don't get ourselves into a box where we do something for expedience that we later have to do redo. So we don't want to go down that path either.

MR. DOUTT: For Problem Statement 2, this has the catch phrase in it -- it is to develop, if possible, an acceptable approach using risk insights and licensing reviews of digital systems, including consideration of proposed industry methods. If we agree on that, then if an acceptable approach can be established, we will issue the interim guidance and acceptance criteria for use of risk insights in licensing reviews of digital systems.

And, again, we have a longer term task there. I don't know if I need to -- one thing we have acceptance criteria here which is somewhat inconsistent with Reg Guide 174, which would be acceptance guidelines. In other places in it we have said acceptance guidelines. We had to do the problem statement as stated. So I think there is some clarification there.

The reason we say if possible is in the short term, in risk informing, I think we were pretty leery that we could actually pull that off. Risk insights might be valuable. I think they would be -- personal opinion.

That this would provide some additional clarification or help as far as doing a risk insight from a -- if you did the defense-in-depth diversity analysis and came up with how much do I need or whatever, this might provide some insight as to how well you did.

Or, in fact, provide indication where you need to do more or maybe less actually. You never know.

But that is the idea here. And we are just -- on the short term here, we're a little bit leery of the success.

MR. ARNDT: I'm sorry. And this really goes to the point that you were making earlier, George. There are probably some insights -- and we use the term insights so it is not risk informed because that is a very specific process, in terms of failure modes, in terms of what is important and what is not important, in terms of what we can learn from the analysis either qualitatively or quantitatively.

And this is certainly something that the industry wants us to do. And they have got their ideas, which is why including consideration of proposed industry methods is in the problem statement, that's something we are going to work to in the short term.

As you heard, there are other disagreements associated with what the best modeling approach is. So this is specifically written in such a way that it is comprehensive but doesn't pin anyone down. We want to be able to use the insights that can be gathered but we're just not sure how we are going to do it and how much we can do in a relatively short time period.

CHAIR APOSTOLAKIS: And we will have some Subcommittee meetings on these things?

MR. ARNDT: We will have supplemental discussions on this.

CHAIR APOSTOLAKIS: The other thing, of course, that is different here from the traditional hardware analysis is that if you find any problems most likely people will fix them.

MR. DOUTT: Yes.

CHAIR APOSTOLAKIS: Whereas if you say, you know, a pump may fail in the future, you can't really fix that. I mean there is a failure rate. Because the problems here tend to be specification errors or some other design-type error, typically you go back and fix it.

Now if the fix though is very expensive and you believe that the circumstances or the context that will lead to this kind of behavior is extremely unlikely, you may tolerate that. But it is a very different approach here.

MR. ARNDT: It is. And there is, as you know, a lot of different work in the software reliability community, if you will excuse the terminology, associated with both identification of latent failures and the likelihood that you haven't identified latent failures. And the likelihood that they will occur. And there are a lot of things like that.

What Alex was mentioning earlier, there are other approaches associated with how you design your software and how you design your digital system to mitigate the consequence of design faults and things like that. And that is something we have to work out with industry. We have some things we agree with and some things we are not yet agreed to on.

CHAIR APOSTOLAKIS: Are you talking about a year from now to have answers to these things?

MR. ARNDT: We haven't put a date on it. Part of the issue is how important this effort is compared to D3, compared to cyber and things like that.

We would like this to be a relatively short-term activity. But the same resources, to some extent, that is going to be used in D3 or cyber or something else also impacts these resources both internally and in the industry.

CHAIR APOSTOLAKIS: But the first bullet certainly would effect any decisions on diversity, wouldn't it though?

MR. DOUTT: Right. I mean --

MR. ARNDT: It could, yes.

MR. DOUTT: -- one of the things here is that we have to work in concert. And if we come up with some insights or methodologies, there is an issue here of -- if there is -- that is a 1.0 type deal over there.

You run through your defense-in-depth and you come up and you don't have it added. We would come up with -- you could come up with the perspective that you added it, how did you do? Maybe that wasn't the most benefit or the least.

But again, from an acceptance guideline point of view, we are stuck with -- you know we don't know whether we can say well how does that relate to implementing the change or not. Or how does that work in current guidance for D3. That are the concerns that we have to try to fit that -- it has got to be a complementary-type -- well, as short term, I think it is complementary.

We have to look at it from like a 174 approach and apply principle to an idea. But --

CHAIR APOSTOLAKIS: 1.174?

MR. DOUTT: Well, from a standpoint of --

CHAIR APOSTOLAKIS: That's some issues.

MR. DOUTT: Well, we can't do it that way. What I'm saying is from a -- it has to be complementary to defense-in-depth, okay? Complementary to defense-in-depth.

DR. GUARRO: George, this is Sergio. Can you hear me?

CHAIR APOSTOLAKIS: Yes.

DR. GUARRO: One way in which, I think, a risk-informed approach can be useful in the area of software licensing is in evaluating the level of testing that software and the type of testing a software may have to undergo for different types of scenarios and functions for which it is used because as we have learned, often the failure of software is conditional upon the mode in which it is called to perform.

And so knowing in what type of likelihood scenario a certain function is performed is important to determine how to handle the software function from a risk perspective itself.

CHAIR APOSTOLAKIS: Yes, that could be.

MR. DOUTT: Back it up from the system back to the development, yes.

MR. ARNDT: And that, as Sergio has

pointed out, that has been used in other industries as a criteria associated with how do you really -- how much testing is necessary, what kind of testing is necessary, what your acceptance criteria for release of the software for practical applications and things like that.

So there are a lot of aspects of this that we might be able to use to improve the other deterministic analysis.

CHAIR APOSTOLAKIS: Good.

MR. ARNDT: That's really where we are trying to go from the staff's standpoint. The industry has got a couple of very specific decision criteria they want us to use this in but the problem statement is more general than that.

MR. DOUTT: And just a very general idea on approach. For the short term, we are trying to -- obviously guidance is the SRM to SECY 93-087 and the four points and the discussion here this morning, stay consistent with policy statements on PRA, encouraging the incorporation of it.

Commission safety goals, the thoughts are right now is to try to stay with current methodologies in the short term.

And the review process is -- I'm not clear on the review process and I don't think we are for sure. It could be a 174-type look and risk informed. We think that is probably tough on an insight point of view in trying to implement in digital.

We also have non-risk-informed applications and how we want to deal with that if they came in and had risk insights, but not risk-informed.

Let's see, I've got some other issues here. One of the things is in acceptance guidelines, which isn't here, how we would do that. Whether it is a delta CDF and it is, of course, LERF, is it, as in the SRM, which is Part 100, and so we have to look at how we want to do acceptance criteria here, too.

CHAIR APOSTOLAKIS: Again, I think the function classification that we have discussed in the past would be extremely useful here because fault trees event risk probably could be useful in situations where you just have to actuate something.

MR. DOUTT: Right.

CHAIR APOSTOLAKIS: If you have continuous feedback, that's a time-dependent problem, is it not? I mean you can't really force it to a fault tree kind of thing.

MR. DOUTT: Yes, we just --

CHAIR APOSTOLAKIS: So I think this

classification is really needed because it is the background to everything else.

MR. ARNDT: We will talk about that very briefly in the next presentation.

CHAIR APOSTOLAKIS: Good, good. Non-risk-informed applications -- non-risk-informed --

MR. ARNDT: Well, there is a --

CHAIR APOSTOLAKIS: Everything is non-risk-informed.

(Laughter.)

MR. DOUTT: Well, I put that there simply because if an effort was risk informing this but in licensing actions you have a choice. And whether we would incorporate this and how we would do that, that puts it in a little different perspective in how we would -- and whether we would or not review it.

And it really is -- if it comes in on risk perspective or risk insight, and we come up with that guidance, it isn't really in that category.

This is just quick on what we looked at from applications so far of PRA to digital systems. And this is reactor space. And operating reactors, to my knowledge anyway, to date risk insights have not been incorporated into a digital I&C submittal for upgrade or whatever by either staff or industry.

Some questions have been asked about whether it would be useful or not but we haven't actually seen it.

In new reactors, a brief look is that some have included digital systems, essentially software common cause failure, and/or performed uncertainly, importance, or sensitivity studies to look at digital systems and essential to evaluate the software.

So what we have seen so far is mostly uncertainty, sensitivity-type work, not a strict modeling of the system. You will find software, you'll find a common cause failure, but the software failure rates are not well document and well defined. Nor is the modeling tending -- you know, sometimes it is there. And in other cases, it is not. The software is ignored. And it is just the hardware.

There are other options, too. It is the hardware/software combined. If you knew the system had been working for a long time and you had the monitor, you have some operating history, you can combine that and assume that approach. Whether it is acceptable or not is unknown but that is the way it has been done.

The other part of his is strictly going out and looking at what other people are doing. We haven't -- we need to do that and try and incorporate this into the short term. Some research tasks are working on this. We can pull some of that from there. We need to look at some other industries. As you mentioned, there are other papers available and we have pulled some of those to see if we can get a little different perspective on this.

MR. ARNDT: As Cliff mentioned earlier in the presentation, and you may not have caught it because he went through it fairly quickly. On both the shorter term actions, what we are planning on doing is basically three parallel paths. We are going to look at what the industry provides us as input to the interim guidance. And they have told us they are going to provide those and they have given us some flavor of what those are going to look like.

We are going to look at what we have done in terms of past experience and review of the AP 1000 and other limited but significant experience we have had looking at these kinds of issues.

And the third path is where we stand on the research at the point where we are starting to put together the interim guidance.

So as you know, we have been working in research and have come up with some ideas and some guidance and some preliminary results both in terms of traditional modeling and dynamic modeling. So we're going to try to meld all three of those -- what is going on in the industry, what we've done, and what we've looked at in the research, which includes other areas.

MR. DOUTT: Okay. And this generally first bullet, general insight, and the strength, I guess, of it. In uncertainty, sensitivity, and importance studies have been used and essentially reduce the impact on uncertainties associated with digital systems and really software failure probability.

And in doing this, how you might impact the PRA conclusions or insight when implementing the digital I&C systems. In fact, if some of these failure modes would change your conclusions. That's mostly obviously in new reactor design certification work. That's a general, if not obvious, look at it.

There is a corollary to that though. It may, in fact, show that it didn't have an impact. Or this is not relatively insensitive in some cases.

What we have seen so far is basically a standard fault tree/event tree method. The level of detail in some cases is to the board level on failures identified to the board level.

Hardware failures were derived from proprietary general databases. There are numbers for that.

The common cause failure of hardware was there in boards and boards across systems. Software common cause failure, I mean it may have been considered in modules and across multiple modules, but what that really meant was and what the software failure probability was was pretty consistent through there and not well defined as to what that basis might be. So that is why the sensitivity studies were done is to give an idea of what the impact might be on software.

And that is where we are currently as far as general ideas go.

And we made up a list of what we think are challenges. What was pointed out last week, I think a kind of reasonable comment was is that this is very similar to an analog problem set, I think, except that when you add software to this, it becomes much more complex. And I don't know if the list is any order of priority but I put software reliability at the top.

If we are doing short term, we've got to deal with that somehow. And, again, how are we going to treat the common cause failure for that?

One issue is hardware/software interactions and dependency, if there is anything in that area that we need to consider. Again, we've got the modeling issues as to how well we need to do this.

I put failure modes in there and we added it as included unknown or unforeseen failure modes and that -- but the general method right now is to take a look at the failures, what you think they are, in deterministic and design basis and run those.

We may not know exactly what all those failure modes are. And some of the failures that have been pointed out, in fact, weren't what was expected. Failure data, we don't really have that. That is research work going on.

And any human reliability issues, a couple things. One is we won't really treat this but how you are looking in the software side it from updates and changes and things like that, whether we need to be concerned. And like obviously the interfaces, whether they will have the information available when this failure occurs. And what the manual actions are and how we are going to treat those.

And then the big question is we think we do conventional. And interfacing a digital system with PRA might be simpler.

The other concern is diagnostics and fault tolerance and coverage and how we might want to handle that. There is a desire to credit that in a PRA. And we will need to come up with a method or see how we want to handle that in short-term space.

That's the first list. There is another list here.

CHAIR APOSTOLAKIS: But I mean it seems to be now a given that we are taking the systems-centered point of view, right? Everything is system-oriented here which is good.

MR. ARNDT: Yes, how you actually define the models for the particular analysis methodology you want to use for the particular system you want to use may have the more --

CHAIR APOSTOLAKIS: Very good.

MR. ARNDT: -- software centric or hardware centric. But from a conceptual standpoint, it's --

MR. DOUTT: One of the things we did look at briefly is architecture and how that may impact some conclusions. And there could be some differences -- well, there are differences depending on how you did it.

In this one, I just did a low probability but credible event to point out in the deterministic, the SRM essentially made that conclusion by making it beyond design basis. But it also concludes that if you don't have something, while you said it could be non-safety and/or it can meet Part 100, but you still have to have something. You have to have some means.

In a PRA, there is a little different perspective on that. So we might want to -- how we want to be consistent with that approach.

Time dependency is in there just simply as you mentioned before, how we might want to handle in a fault tree/event tree space if we've got issues with time.

One thing that hasn't been talked about much is external events. And I just put fire in parenthesis. Digital systems and susceptibility to externals, whether that is different than analog and whether we need to consider it.

Again, the review process, that is a broad -- whether it is a Reg Guide 174, some other way, a simplified method, we need to look at -- we have some variety of ways to look at this. Along with that, then what acceptance guidelines would be acceptable. Also PRA quality here -- you know, it's going to come in here somewhere.

It may not in the short term. We might -- he have to consider that in the long-term. It is definitely is there.

CHAIR APOSTOLAKIS: PRA quality from what perspective?

MR. DOUTT: Well, from this point of view and on a license amendment, is the PRA adequate for the request? If I'm going to implement a digital system and I'm doing risk insights here, in fact is this adequate to make those conclusions? And we have to come up with some guideline for that.

There may be policy issues here, too, in the sort term. That is where we try to avoid that. But in the long term, there might be trying to blend this with a deterministic process, and risk-informing, if you will, defense-in-depth. We're trying to avoid that.

CHAIR APOSTOLAKIS: Is that how we do it now?

MR. DOUTT: No, it is not how we do it now.

CHAIR APOSTOLAKIS: Isn't 1.174 implementing this?

MR. DOUTT: When you -- in 1.174, there

are a couple of issues in there with defense-in-depth. One is it is deterministic and listed as, you know, there is another part in there that says you can also use the PRA to provide insights on your defense-in-depth. However, you don't want it to be circular, okay.

And that the uncertainty, you know, one of -- now, I don't want to say I have to put in a diverse system. It is a one based on deterministic. I come back and say well, but defense-in-depth is -- I don't want to -- that was what was limiting my uncertainty in software was that defense-in-depth. I don't know if I want to have a screening criteria that would remove it.

So I want it to be a complement to that defense-in-depth diversity analysis right now. Going forward, in the long term, that is something else.

CHAIR APOSTOLAKIS: I don't see what 1.174 does, I think because you have the defense-in-depth philosophy. Then you have the risk change.

MR. DOUTT: Right.

CHAIR APOSTOLAKIS: Make sure you don't overdo it.

MR. DOUTT: Right. Make sure you keep the two in synch. And that is what we are trying to maintain.

MR. ARNDT: The concern Cliff has is that if you are actually changing the defense-in-depth, then you have a potential issue with 1.174 because 174 says you can do a regulatory change so long as the risk criteria is met and you maintain defense-in-depth --

CHAIR APOSTOLAKIS: Philosophy.

MR. ARNDT: -- philosophy, correct.

CHAIR APOSTOLAKIS: So you can effect difference in there. In fact, if you didn't, there would be very, very few applications.

MR. DOUTT: But what happens is -- and where are we in this particular case, how much is enough, and where is it in acceptance? So we have to look at that.

CHAIR APOSTOLAKIS: Well, it is the same thing in 1.174.

MR. DOUTT: Well, that's the other thing.

CHAIR APOSTOLAKIS: I don't think this is new. This is the same.

MR. DOUTT: Okay. All right.

And then that puts us into consistent with current regulations guidance.

CHAIR APOSTOLAKIS: Well, improved

guidance. We want to effect the guidance.

MR. DOUTT: And the timeline is at this point relative simple. We need to determine that. Part of that is we provided the project plan to essentially public industry. We need those comments back as far as prioritization of what they think and what resolution and aggressive target dates are needed.

There are also going to be comments obviously on the problem statements and we will have to work on that.

So we have not determined that yet. But short term, as Steve said, is a relative term. And, again, long term is update regulatory guidance, SRPs, reg guides, and/or whatever else it looks like. But that should be a long-term task.

CHAIR APOSTOLAKIS: It is critical that industry include priorities for resolution and the dates?

MR. DOUTT: It depends on --

CHAIR APOSTOLAKIS: The dates will come from the industry?

MR. ARNDT: No, they will give us the priorities.

MR. DOUTT: The requested dates.

MR. ARNDT: The requested dates and priorities. This goes back to the issue we had this morning. There are some things -- if you go out to the transcript of the November 8th Commission meeting where the industry came in and said we need to finalize our designs so that we can do certain things like order simulators and things like that, what we specifically asked in our cover letter to the public was if there is some date that is driving your requirement, like we want to order simulators by such and so a date or we need this so we can resolve a particular technical issue so we can do our design, if there is some date that is driving that, then that will drive our prioritization to some extent.

So when we say that, the requested target dates for completion is basically input to us saying we want to have guidance in this or some other area by such and so a date so that they can take a particular action. And that will not necessarily be the date in the final problem plan but we will certainly consider that as part of our internal prioritization.

Clear?

CHAIR APOSTOLAKIS: Yes, I would take that comma out from --

(Laughter.)

CHAIR APOSTOLAKIS: It's confusing.

MR. ARNDT: We can do that. That can be done.

CHAIR APOSTOLAKIS: Okay.

MR. DOUTT: Some sort of conclusions as we just talked about.

CHAIR APOSTOLAKIS: Good.

Any questions?

(No response.)

CHAIR APOSTOLAKIS: Very good. Thank you, gentlemen.

MR. ARNDT: Thank you.

CHAIR APOSTOLAKIS: Although I guess Steve will stay up there.

Review of current status of dynamic digital reliability modeling research, so you are going to tell us why dynamic reliability modeling is important?

MR. ARNDT: That's part of what we are going to do.

For those of you who are not familiar, this is Professor Tunc Aldemir from Ohio State University who is one of our researchers in this area.

CHAIR APOSTOLAKIS: So this is now a color? Is that what it is? Yes? Okay.

MR. ARNDT: So what I'm going to talk about today is a quick background. And I want to do that because -- and it is going to be three or four slides -- I want to put this in perspective. The discussion by the industry this afternoon focused in on this particular project.

And although it is certainly one of the areas that we are looking at and we think shows a lot of promise and we have gained a lot of useful insights on it, it is not the only thing we're doing in terms of long-term research. So I want to put it in perspective.

And then we're going to talk a little bit about what we have done since the last time we came and talked to the Committee, particularly issues associated with the revision and update of the draft document that you looked at last summer. And then a couple of quick slides on the methodology and where we are on that.

One of the big issues that was found in the comments that we got -- and I'll talk about that more in a minute -- was there is a lot of issues associated with practicality. And we want to talk a little bit about --

CHAIR APOSTOLAKIS: As you know --

MR. ARNDT: -- how we are trying to resolve those.

CHAIR APOSTOLAKIS: -- especially Tunc knows very well, this issue of dynamic PRA, not just in the context of digital I&C has been around now for 10 years, 15 years?

MR. ALDEMIR: More than that.

CHAIR APOSTOLAKIS: More than 15 years. There were several groups that were involved from Maryland, from other places, American cities has worked from this, there have been workshops and so on, and the problem -- not the problem -- I mean the issue has always been really what NEI raised this morning or this afternoon. Where is the smoking gun? Where is the convincing argument that says you must go this way? And that the existing methods that are based on event trees and fault trees are inadequate in some sense?

And I must say I haven't heard that argument yet in the context of the broader PRA. There have been also effort from Italy and so on --

MR. ALDEMIR: Belgium.

CHAIR APOSTOLAKIS: What?

MR. ALDEMIR: Belgium.

CHAIR APOSTOLAKIS: Belgium -- and

although people were enthusiastic in the workshops and all this needs to be done, it is very exciting work, by the way, modeling and so on. But that has been the problem so far. That nobody doing work of consequence in the sense of decision-making and so on has seen a reason to go into this, which is considerably more complex than the existing methods.

So I guess NEI repeated this argument earlier today regarding this particular application and it seems to me --

MR. ARNDT: And I will try and address that in a very, very, very short --

CHAIR APOSTOLAKIS: Pascal-ful state.

MR. ARNDT: Hopefully.

(Laughter.)

MR. ARNDT: Because the -- well, both in terms of how we are focusing our research, which, I think, is somewhat misunderstood, and what the objectives of it is.

CHAIR APOSTOLAKIS: I just wanted to make it clear to people who are not from the PRA community --

MR. ARNDT: Sure.

CHAIR APOSTOLAKIS: -- that this is not new. And the argument that we heard against it is not new either.

MR. ARNDT: Right.

CHAIR APOSTOLAKIS: Okay? Not being new doesn't mean it is not valid.

MR. ARNDT: Right.

A couple quick things, the Office of Research has a program for evaluating and developing models needed to support risk-informed regulation. This is something that we have been doing for about three years now. It's not something that we started doing just because of the task working group. We have been doing this for a while trying to develop these.

The phraseology is specifically chosen. If we find something that we like, we don't have to develop something new. But we do want to understand what is out there, evaluate its capabilities and limitations, and look at how you can develop new things or relax the limitations that we find.

As you know, the NAS study recommended looking at this from a systems-centric standpoint and looking at hardware and software modeling, either as explicit hardware/software and then the interactions or the way we are doing it, the dynamic way, as a system-state-system type analysis. And we'll talk about that in a second.

So what we are doing is looking at these things. And for near-term applications -- and when I say near terms here, I mean the next ten years, not next year -- one of the other boundary conditions is that whatever structure we come up with, no matter how complicated, needs to eventually fit back into the broader plant PRA because that is what the acceptance criteria is written again.

So what we are doing is research to understand what can be done with traditional methods. Basically that's part of the research is looking at how far can we move what we currently know in terms of modeling digital systems and capturing the unique aspects of digital systems.

And then from the other side, in parallel, we are looking at what advanced methods can bring to the table. How much do you need to do? Where is it going to give you advantages and more power associated with that? And then how do you link it back to the event trees?

So --

CHAIR APOSTOLAKIS: Sergio, are you still on the line?

DR. GUARRO: Yes, I am.

CHAIR APOSTOLAKIS: Maybe for this part,

you should not participate.

DR. GUARRO: I'm not participating.

(Laughter.)

CHAIR APOSTOLAKIS: Let's make sure.

DR. GUARRO: If you want, I can cut off completely.

CHAIR APOSTOLAKIS: Sorry? What did you say?

DR. GUARRO: I said if you want, I can disconnect.

CHAIR APOSTOLAKIS: No, no, you can stay on line if you will but please don't participate in this part.

DR. GUARRO: I haven't made a sound have I?

(Laughter.)

CHAIR APOSTOLAKIS: Okay. Thank you.

DR. GUARRO: Okay.

MR. ARNDT: Okay. So the objective of the program is basically to identify or develop methods for regulatory guidance, et cetera, needed to support the problem statements that we just talked about.

The real quick overview of what we are doing, we've got a set of different tasks that have been assigned to different groups within the office.

I'll go through this quickly. The overall program coordination is with my group.

CHAIR APOSTOLAKIS: You group is --

MR. ARNDT: DEFERR.

CHAIR APOSTOLAKIS: DEFERR?

MR. ARNDT: DEFERR, Division of Fuels Engineering and Radiological Research.

CHAIR APOSTOLAKIS: That's where they are digitalizing the logs?

MR. ARNDT: The engineering part is where I&C is.

CHAIR APOSTOLAKIS: So it is DEFERR?

MR. ARNDT: Yes. And then the development of the regulatory guidance is also in our shop. And the interface with the Steering Committee.

The investigation or refinement of traditional modeling methods with traditional failure modes and effects analysis is with DRASP, the other division. The investigation and development of methods in dynamic models is with us.

And then development of the two benchmark cases that we will talk about -- one of the things we are trying to do is gain additional insights into the methods by actually trying them out on a couple of actual systems. And we will talk about those more.

But the first system is a system that is more likely to have dynamic interactions but has a potentially lower safety significance. The second system is one that is less likely to have dynamic interactions but has potentially more safety significance. So we are trying to choose a couple of example systems that will cover as much of the territory as possible.

MR. KEMPER: Steve, this is Bill Kemper. If I could just interject. Now that last bullet, we intend to benchmark -- use a benchmark to test both methodologies?

MR. ARNDT: Correct.

MR. KEMPER: The traditional methods using event tree/fault tree as well as the dynamic methods?

MR. ARNDT: Yes.

MR. KEMPER: Okay. So basically we're trying to validate both processes in parallel here. And see which one best suits the application?

MR. ARNDT: And that really gets back to the point that you mentioned earlier associated with understanding what systems need to be modeled at what level based on a set of characterizations.

CHAIR APOSTOLAKIS: I really think we need that, Steve. We need to see something along these lines.

MR. ARNDT: Okay. And we've started down that path looking at a three-axis model which is very, very preliminary at this point, looking at system complexity, system interaction, and system importance. Those are the orthogonal axis right now.

It is very preliminary at this point. If you'd like to discuss it offline or we can come and talk to you specifically about it.

CHAIR APOSTOLAKIS: I think we should discuss it. I know that it was even a problem within the group that put together the National Academy report.

MR. ARNDT: Yes.

CHAIR APOSTOLAKIS: There were strong disagreements within the group.

MR. ARNDT: Yes, it is a difficult issue.

CHAIR APOSTOLAKIS: Because, you know, somebody comes in with a failure that occurred in RER, a very complex feedback and control system, and says oh, you have to worry about it when you talk about describing the reactor. I mean it is not the same thing.

MR. ARNDT: Right. Yes.

CHAIR APOSTOLAKIS: It's just not.

MR. ARNDT: Right. And there are different issues --

CHAIR APOSTOLAKIS: We need that.

MR. ARNDT: -- associated with it.

CHAIR APOSTOLAKIS: Yes, exactly.

MR. ARNDT: And right now that is the approach we are looking at. We haven't vetted it with a lot of people yet. But we can come back and talk to you more about it.

So let me drop out of the general model now and talk about the specific dynamic model. We are going to have a longer presentation after I get done on the traditional modeling methods. And where we are going from that.

But the point here is these are parallel efforts. We are trying to learn as much as we can about both. And the principle idea is on the dynamic modeling methods, learn how powerful and how useful these can be under particular circumstances. And on the traditional side, look at how far can you push the traditional models before you run into issues. So it is looking at it from both sides.

CHAIR APOSTOLAKIS: Is there any reason why you have color copies here with green characters and blue background?

MR. ARNDT: The ones we provided this morning were all black and white.

MEMBER KRESS: To see if you are color blind.

CHAIR APOSTOLAKIS: That was your idea, too? Using the boilerplate?

(Laughter.)

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: Okay. So the basic structure is to investigate the capabilities and limitations. This is the 6901 that was talked about earlier. There is obviously some concern about that particular document although we thought it was a pretty good review of the models capabilities and limitations.

Look at what potential modeling methods would be the most practical for implementation in that we specifically looked at models that have had some level of implementation previous to this, which is why we came down on a Markov and a DFM modeling methodology, review past experience, review existing regulatory framework associated with the unique aspects of the digital system that need to be modeled, identify requirements -- and when I say requirements, I don't mean that in a regulatory sense, I mean that in a modeling capability sense, identify the methodologies, and then demonstrate the methodologies with the benchmarks.

Again, we're using two benchmarks. We will talk about the results of the first benchmark. That was a feedwater control system. The second benchmark is going to be a reactor trip system.

Current status, we've talked about this three times already. We put out 6901 which basically reviewed the methods. We identified two benchmark systems. We've looked at an example initiating event for integration of the dynamic models into the traditional fault tree/event tree.

That is one of the biggest challenges associated with non-event tree/fault tree-type models. How do you integrate them into this structure. Tunc will talk about that a little bit in a few slides. But we have identified a methodology that we think works well.

We have compiled this into a draft NUREG that is specifically designed to be a proof of concept. The title is there and it is in final review right now.

CHAIR APOSTOLAKIS: What is DFWCS?

MR. ALDEMIR: Digital Feedwater Control System.

CHAIR APOSTOLAKIS: Sorry.

MR. ARNDT: And then what we are doing is publishing a third document which will have the actual quantification, basically the numbers. One of the concerns that we got in the review of that document was well, where is the beef? What is the final numbers? And what does it tell you?

The point here is just to demonstrate that this kind of modeling methodology can be made practical. But certainly we would like to demonstrate that the quantification can be done. So we are going to have another document that will have the specific points.

CHAIR APOSTOLAKIS: Well, I guess there are two steps here. The first is do we get anything very useful that we cannot get with the traditional methods --

MR. ARNDT: Right.

CHAIR APOSTOLAKIS: -- which is the heart of the argument against this. And then second, can we make this practical.

MR. ARNDT: Right. And that is something you really have to do almost in parallel because you learn -- I mean theoretically there are a lot of things you could possibly learn from using these kinds of things. Identify new failure modes, identify new interactions that are dynamically based, identify new issues that might be there.

But the issue really is are you really going to see any of those in the practical implementation? Is there enough data? How do you parse the data? How do you aggregate the data? Is it going to be too computationally-intense to ever get any real insights?

So there is some synergism there. But yes, those are the questions that we need to answer. And we'll talk a little bit about that. Not in any great detail.

Because this has been a somewhat controversial issue, as you well know, we have had probably more peer review of this document than we have of a research document in a long time. We have had extensive internal reviews, including the comments you provided us last year. We've had internal reviews from the Research PRA group, the Research I&C group, the NRR PRA group, the NRR I&C group.

We have had external peer reviews from academia, from the labs, and from the industry. We had approximately 180 different succinct comments grouped in a number of different areas including regulatory issues, issues on the benchmark system both in terms of its applicability and the exact details, issues about data collection and generation. How do you feed the monster? Issues about the dynamic methodologies and their practicality. And issues associated with integration with the fault tree/event tree.

CHAIR APOSTOLAKIS: Are we going to see this before publication? Or this is it?

MR. ARNDT: It is in final publication now.

We prepared a comment resolution document that will be published in parallel with this which will basically have all 180 comments --

CHAIR APOSTOLAKIS: Yes, I'd like to see that.

MR. ARNDT: -- without attribution.

CHAIR APOSTOLAKIS: Without it?

MR. ARNDT: Well, what we've decided to protect the guilty is the reviewers will be listed but they will not be -- each individual comment will not be tied to an individual reviewer.

CHAIR APOSTOLAKIS: Can you give us some names?

MR. ARNDT: Internally, Nathan, and people like that. Externally, do you remember the academics?

MR. ALDEMIR: Enrico Zio.

CHAIR APOSTOLAKIS: Did you pay them?

MR. ALDEMIR: No.

MR. ARNDT: Curtis Smith.

MR. ALDEMIR: Curtis Smith.

CHAIR APOSTOLAKIS: Industry, who was from the industry?

MR. ARNDT: Mr. Stone who was just speaking.

PARTICIPANT: Bob Enzinna.

MR. ARNDT: Thank you. Bob Enzinna. Our friend from EDF, Tweat who has done a lot of the EPRI work in this area.

CHAIR APOSTOLAKIS: Oh, the gentleman who was here at the last meeting?

MR. ARNDT: Yes.

MR. ALDEMIR: Also from Norway --

MR. ARNDT: Oh, Altusa.

MR. ALDEMIR: Altusa Tunam.

MR. ARNDT: She's the lead software engineer at Halden. So pretty broad spectrum of both practitioners and theoreticians and others.

CHAIR APOSTOLAKIS: Was there anybody who was positive?

MR. ARNDT: Oh, yes. There were a lot of positive comments. There were a lot of negative comments, too.

CHAIR APOSTOLAKIS: I knew that.

MR. ARNDT: So it was --

MR. ALDEMIR: But even from the industry we had a few positive comments. Well, in different sections of it.

CHAIR APOSTOLAKIS: Good, good.

MR. ARNDT: So we will talk about a couple of the things that we did here in a second.

Just to give you a broad brush associated with it, it was not a super simple system. It was a real practical system. It was the digital feedwater control system. It had a high power mode and a lower power mode, a backup computer, and a main computer. And had different controllers.

We looked at the input devices. We looked at the output actuation devices. So it was not a trivial academic-type system.

MR. ALDEMIR: If I may say one word here.

CHAIR APOSTOLAKIS: What is this business trivial academic?

(Laughter.)

MR. ALDEMIR: One of the -- last time we

were presenting a similar presentation here, there was a whole bunch of equations on the screen. And --

CHAIR APOSTOLAKIS: And now it is clear.

(Laughter.)

MR. ALDEMIR: And, of course, a concern is how are we going to do it? What kind of expertise is needed to do that? That is one of the reasons why we developed the Simulink Model which, I think, is easier to generate from a process diagram because it looks pretty much like the process diagram as we incur it rather than dealing with a bunch of equations.

So the point I'm trying to make is that this is in response to the comments we received in terms of practicality.

CHAIR APOSTOLAKIS: You developed a simulation?

MR. ARNDT: Yes.

MR. ALDEMIR: Yes. A Simulink Model which you can interface with much more easily generically. Eventually we would like to come up with a shell that you plug in your own module. So rather than having the equations which are going to be user-unfriendly, we thought it would be a better idea to develop a Simulink Model which is much more well known.

And so if we designed the interface for a

Simulink interface, then it is easier on the part of the user if they wish to use it in the future to link up with it. That was our intention.

CHAIR APOSTOLAKIS: Clever idea. Clever idea.

MR. ARNDT: And the other point here is some of the comments we received basically was you really have to do a lot of work to do this. And in the NUREG, the original version of the NUREG, it had all the system equations and things like that.

And the point is you only need system equations or system simulation to the extent that the system is interfacing with the system. If it is a simple trip function, then this part is much simpler. It is a set of and/or type else systems.

CHAIR APOSTOLAKIS: Well, wouldn't the plant simulators --

MR. ARNDT: The plant --

CHAIR APOSTOLAKIS: -- simulate already a lot of these things?

MR. ARNDT: Yes, it could if you linked it with the PRA model. What you need to track the interactions is some mechanism, as you step through the time frame, to look at the interactions between whatever system you are modeling and the plant process as a whole.

In our case, since it was a feedwater control system, we were looking at steam generator level, steam generator pressure, temperature, pump flow, and things like that. In the case of an RPS, it would be the trip functions, whether or not the system had actually tripped or not, maybe --

CHAIR APOSTOLAKIS: Otto, wouldn't these things exist already?

MEMBER MAYNARD: You have to be a little careful with the simulator. As far as using a simulator for this, a simulator is designed to give you the same indications and views that you get in a plant but the programming may not be totally identical to every step that is going on in there.

And so you have to be careful. It really would depend on how the simulator computer system software was all put together and what it was simulating and stuff. But you do have to be careful in using the simulator for things such as this. It can be but not necessarily in all cases can it be.

CHAIR APOSTOLAKIS: This is the feedwater system control?

MR. ARNDT: This is the controller, yes.

CHAIR APOSTOLAKIS: Oh, the controller.

MR. ARNDT: There are equivalent type of things for the process input variables that we needed.

MR. ALDEMIR: This is pretty much directly from the process diagram. This does not have the full system dynamics in it. It doesn't have, for example, what we call the steam generator module that is going to be an additional input into this system.

That normally would have come -- this and the level change combined would have come from the plant simulator. But in our case, these are two separate modules. So it will feed -- because we had to test this module first with a simpler process model so that if there are problems, we can identify the problems rather than testing the whole complex thing in one shot.

MR. ARNDT: And this, like I say, this gets back to the issue we brought up earlier. Depending upon the functional classification, how much information you need to make the right decision, this might be this complicated or it might be much simpler depending upon the system.

The point here is we are modeling it to the level of detail that we think is necessary to capture the unique aspects of the digital system.

CHAIR APOSTOLAKIS: So if I were to do

then a complete PRA and I have things like high pressure injection, low pressure injection, recirculation, would I develop something like this for each of these systems? Or for the reactor as a whole with all the safety functions?

MR. ARNDT: You would develop a reactor model.

CHAIR APOSTOLAKIS: A reactor model?

MR. ARNDT: A model of the plant system, the plant process. And then --

CHAIR APOSTOLAKIS: Which is already in the simulator, right? I mean that --

MR. ARNDT: Again, that may not be exactly the case.

MEMBER MAYNARD: To give you some examples of the simulator, let's take the reactor protection system. You don't have a complete reactor protection system sitting there with your simulator. You will have that programmed into the software. But it is not identical to necessarily what is -- all the signals and the various things you'd be getting.

Again, the main idea is to get the same inputs, the same displays in the control rooms, and get the components, to, you know, get the reactor trip at the same point. But it is not going through the same logic, the same controllers, the same types of things that you would have going on inside the power plant or a reactor protection system.

CHAIR APOSTOLAKIS: Which you will have to do here though.

MR. ARNDT: For those systems that you want to model in detail, the issue would be you would make a determination, however you wanted to do it, as to what level of modeling detail you needed for each system --

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: -- like this. And then as you step through the initiating event --

CHAIR APOSTOLAKIS: I would say, Steve, that this helps with the question of practicality.

MR. ARNDT: Yes.

CHAIR APOSTOLAKIS: But it does not help with answering the question why do I have to do this.

MR. ARNDT: Okay.

CHAIR APOSTOLAKIS: Is that correct?

MR. ARNDT: That's correct. That is exactly correct.

CHAIR APOSTOLAKIS: So if you decide that you need to do it, then developing these simulators makes it practical because now an average user can do it.

MR. ARNDT: Right.

CHAIR APOSTOLAKIS: But why go through the effort to do this remains unanswered? Or you have arguments for it?

MR. ARNDT: We have arguments for it. There is, obviously, some debate as to whether or not they are convincing or not.

CHAIR APOSTOLAKIS: Okay.

MR. ALDEMIR: One comment about the plant simulator. It doesn't have to be faithful to the operation of the control system. You can use it also by activating or deactivating the appropriate components simply to see as a model of the process evolution level change, for example.

And so -- and that it doesn't matter whether it is faithful to the actual operation or system or not as long as it has the proper level dynamics so to speak.

MR. ARNDT: Okay. I'm going to skip through these next few things rather quickly. One of the issues is, of course, you've got to do the model testing. And the model has to be correct.

One of the comments we got was associated with the benchmark system and the accuracy of that and the dynamics of the valve closing and things like that. I mean we have gone back in and proved that.

The actual issue associated with how you model in -- this is a Markov model but in DFM or Markov, the various interconnections --

MR. ALDEMIR: No, no, this is a state diagram.

MR. ARNDT: Oh, I'm sorry. This is a state diagram. Right. You need to understand the states of the system. And this is rather complex and it is -- the point that you need to understand how the system might fail.

So in this particular case, we've got a state diagram which looks at state transitions. It doesn't care whether it is a hardware failure or a software failure. We're not modeling hardware and software separately. We're modeling hardware and software in its hardware/software interactions in an integral way.

What we do care about is states in the system that would lead to unique failure modes. And, again, this is a matter of determining what level of modeling detail you need. So, for example, there is operations with two computers, the backup and the main-running, operating with one computer with recovery, operating one computer without recovery, and various other kinds of characterizations.

The point here is you model it to a level of detail necessary to capture the unique features of the digital system. I've said that about four times in the last five minutes. The point here is -- it gets to your question of do you need these or not -- the issue is if you don't know whether or not a particular unique feature of the digital system will give you a different answer, then you should start as a default with modeling all the unique features that you have.

It is very difficult to arbitrarily say these things can be modeled by an on/off switch in an undeveloped basic event if you don't look at the system interactions associated with them. And, again, this is a look at the controllers associated with it. And the communications and issues like that.

Why don't I let you do this one, Tunc?

MR. ALDEMIR: Well, one of the problems was, of course, everybody knows Markov models, and by the way, when we say Markov models, it is not just Markov models. I distinctly say Markov model but the state transition diagram which is common to both DFM and Markov models and everybody knows that state models lead to computational complexity but as Steve said, you don't know. You have to do it the best you can. And then decide whether you need that detail or not.

So here we are trying to capture everything within the system. And as you see at least to a hundred million states, which is, of course, impractical. Now on the other hand, it is a well-known technique to conglomerate components into super components as long as they don't have individual external interactions. And we use that --

CHAIR APOSTOLAKIS: Excuse me, 100 million states --

MR. ALDEMIR: States.

CHAIR APOSTOLAKIS: -- of what? What system?

MR. ALDEMIR: That includes hardware and software in the sense that, for example, we have an arbitrary output failure mode for the computers. That is a software thing. On the other hand, you have power --

CHAIR APOSTOLAKIS: These are states of the system?

MR. ALDEMIR: States of the system, yes.

CHAIR APOSTOLAKIS: So they are

combinations?

MR. ALDEMIR: Yes, yes, yes.

CHAIR APOSTOLAKIS: And each parameter or whatever is modeled in a multi-state way?

MR. ALDEMIR: Yes.

CHAIR APOSTOLAKIS: How many states? Or it is not standard?

MR. ALDEMIR: Five pairs -- I cannot recall offhand. The first item lists the hardware components we are considering. And each has about five, six different failure modes. But that is what is leading to 100 million.

CHAIR APOSTOLAKIS: That's all I need to know.

MR. ALDEMIR: So after we do this conglomeration and census, for example, are regarded part of the computers and there was one argument, one comment it against that. They said well, why are you doing that? You may be needing the information someplace else. If you do, you don't. If you don't join them into the same component.

For example, we are both regarding the backup and the main computer as computers because they are identical. We are also using arguments like systems operational whether there is one or two computers so I don't have to have separate states for each computer.

Incidentally, we are not trying to be, as I said in the meeting last week, in the public meeting, we are not trying to be system-specific clever here which is a difficult thing to do and which would require engineering judgment. These are well-known techniques in state conglomeration or state reduction techniques. And used for all sorts of different systems.

CHAIR APOSTOLAKIS: So the best you could do is 2,200?

MR. ALDEMIR: That is very reasonable.

CHAIR APOSTOLAKIS: You could do it by hand, I suppose.

(Laughter.)

MR. ALDEMIR: By the way, French have been doing part of their control systems using Markov models about 15 years ago using 10,000 by 10,000 states -- I mean matrix.

CHAIR APOSTOLAKIS: Okay.

MR. ALDEMIR: We have done two million by two million.

CHAIR APOSTOLAKIS: You don't need to.

MR. ARNDT: Okay. We are running a little behind so I'm going to try and step through the rest of this fairly quickly.

So the extent of the analysis of the failure scenarios of the benchmark system looks at all the different failure paths. And that's, to some extent, the point. We want to look at all the different system interactions and different system failure paths to look at what interactions we might have.

And one of the comments was the need to do a comparison of the DFM and the Markov modeling methods. And we have added that from a qualitative standpoint to look at issue associated with the branches and determinations and things.

CHAIR APOSTOLAKIS: Now you said qualitative. You did not quantify anything here.

MR. ARNDT: No. We have not quantified in this document. We are going to do quantification in the next document.

CHAIR APOSTOLAKIS: But can one look at the results of this exercise here and provide failure modes and argue that these you could not have found using traditional methods?

MR. ARNDT: Yes.

CHAIR APOSTOLAKIS: Do you have any

examples of those?

MR. ARNDT: Do you know one off the top of your head?

MR. ALDEMIR: Well --

CHAIR APOSTOLAKIS: These are the answers to the argument.

MR. ALDEMIR: The problem is the following, as you well know, and this was brought up in 1992 workshop. If you know the answer, you can justify using other techniques to arrive at the same answer.

CHAIR APOSTOLAKIS: But still, it would be nice to have a few examples.

MR. ALDEMIR: Well, yes, well, I mean, we haven't -- as I said, the easiest way to do it is to have an independent group using traditional methods and another group doing dynamic methods. Then compare and see what they have found.

And that is the route actually NRC has chosen. So far we haven't had any comparison -- any basis for comparison with static methods yet.

CHAIR APOSTOLAKIS: Well, I'm not really asking for a formal comparison. But I mean if I look at your Slide 15, for example, where you have scenarios, a few of those and say look with the traditional fault tree, chances are you would not have found this.

MR. ALDEMIR: I showed you one last time, which is basically depending on when the valve fails, you can either have high level or low level or high level -- failure by high level or bi-level whose consequences are quite different when you do the PRA, overall PRA.

CHAIR APOSTOLAKIS: But that is the kind of thing I'd like to see.

MR. ARNDT: Okay.

MR. ALDEMIR: We had --

CHAIR APOSTOLAKIS: I remember from the last time.

MR. ARNDT: I'm sorry. We will provide that to you. The point is that is a somewhat subject evaluation.

CHAIR APOSTOLAKIS: Absolutely. No question about it. But at least you put something on the table for discussion.

MR. ARNDT: Okay.

CHAIR APOSTOLAKIS: Because I believe the criticism of today plus, as you know already 15 years or so, has to be addressed. Why do I have to go through this? And if you put a few examples on the table and start the debate, I know it is a lot of -- I mean the reactor safety study had the same reaction. Oh, a good engineer could have found this.

MR. ARNDT: Right.

MR. ALDEMIR: That is the argument. That is the argument. But, you know, we are coming from the premise that there has been enough experience in the past to show that dynamic methods will discover failure modes that traditional methods cannot. The question that is relevant to this community is it necessary for PRAs -- for power plant PRAs?

CHAIR APOSTOLAKIS: Absolutely, yes.

MR. ALDEMIR: Now the problem is this. Let's say that for argument's sake, we have shown that we have compared traditional methods against dynamic methods and shown that for all the reactors operating in the world today, everything can be handled very nicely by traditional methods. Okay, let's assume that this is the finding.

Does it mean that somebody is not going to come up with a reactor design ten years down the line that will be quite different? So our task -- we are working for the regulator -- our task is to come up with a general methodology that can be used as a basis. But the need will need to be regulated.

MR. ARNDT: Okay.

CHAIR APOSTOLAKIS: It was a subtle hint.

(Laughter.

CHAIR APOSTOLAKIS: I think even if the ultimate conclusion -- even if the ultimate conclusion is that the existing methods are pretty good or good enough, having gone through this --

MR. ARNDT: Yes.

CHAIR APOSTOLAKIS: -- will have increased our confidence --

MR. ARNDT: That's right.

CHAIR APOSTOLAKIS: -- in those methods. I have no problem with that.

MR. ALDEMIR: That's exactly right.

MR. ARNDT: As I articulated and I won't belabor it too much, that is the point. The point is to understand where the limits are for the particular examples, the cases that we care about.

MR. ALDEMIR: We would like to have a defensible methodology basically.

CHAIR APOSTOLAKIS: Okay. We all do, Tunc.

MR. ARNDT: In the DFM space, dynamic flow graph methodology for those of you who aren't --

CHAIR APOSTOLAKIS: Was it applied, too?

MR. ARNDT: Yes.

MR. ALDEMIR: Sure.

MR. ARNDT: We have applied it, we have looked at it in the inductive mode. We have done some qualitative comparisons of the scenarios. We updated a steam generator simulator package associated with it.

One of the nice things about DFM, of course, is it can be used in the deductive mode as well which is particularly useful for investigating failure modes. And looking at these issues associated with is the failure modes and effects analysis really getting you all the information?

CHAIR APOSTOLAKIS: Deductive, you mean if the level -- how can the level be such and such?

MR. ARNDT: Right.

CHAIR APOSTOLAKIS: Then work backwards.

MR. ARNDT: Exactly. Then work backwards.

CHAIR APOSTOLAKIS: The fault tree.

MR. ARNDT: Right. And because DFM integrates the process as well as the failures into a single analysis, it is particularly useful for these kinds of systems.

CHAIR APOSTOLAKIS: So you would have examples also from DFM at some point?

MR. ALDEMIR: This is already, I think, in the document. We did the comparison. We did the resolution upon your suggestion last time.

MR. ARNDT: So --

CHAIR APOSTOLAKIS: Well, I can't wait to get that document.

(Laughter.)

CHAIR APOSTOLAKIS: Is it coming out soon?

MR. ARNDT: As soon as I can force it through the process.

CHAIR APOSTOLAKIS: You try to avoid dates today desperately. You never give me a date.

MR KEMPER: It will be soon.

MR. ARNDT: It will be soon.

CHAIR APOSTOLAKIS: Thank you, Bill.

MR. ARNDT: That helps a lot. So like I said, you can track through the different process in an inductive or deductive manner to support particular failure scenarios.

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: The exact comparison because the --

CHAIR APOSTOLAKIS: Those of you who are wondering why I asked Dr. Guarro to be quiet he is the father of this DFM methodology. So he can't really review his own work.

MEMBER KRESS: Has he ever done that?

CHAIR APOSTOLAKIS: Has he ever reviewed his own work? Yes.

(Laughter.)

MR. ARNDT: So to date we think we have demonstrated that these approaches can be dealt with in a practical way and they can demonstrate a lot of the different unique aspects associated with it.

Now how practical it is and how much of this in terms of uncertainty analysis, unique failure modes, applicability to other systems is still open. And that is why we are going to complete the research.

One of the issues -- and I'll step through this rather quickly because I'm running over time -- is the issue of as you get more and more different failure modes and different states, you have to get the state transitions and things like that.

There is a lot of different ways you can do that with data, with certain expert elicitation and judgment. But one of the ways you can do it is through testing, both traditional testing and specific testing to look at how the system transitions from state to state.

One of those techniques is the fault

injection testing. You can look at it from a software standpoint, from a hardware standpoint. The concept is not that dissimilar to stress testing or accelerated testing for a piece of hardware. You stress test the hardware/software system by putting in faults in the system and seeing how it executes or how the fault protective systems keep that from becoming a failure.

So you develop a set of fault injection space that looks at the type faults, the location of faults, the timing and injection, the duration, and, most importantly, the system's context, which in software space is referred to as the operational profile to understand how these systems would fail and what they would fail.

And that allows us to develop a fault coverage parameter which is similar but not exactly the same as testing coverage or something like that that allows you to look at how you partition a failure space.

So the process basically is you construct a fault list. You find the failure rate of the device in whatever operational modes you are interested in. You do a fault injection experiment. You look at the response of the system. And you look at the coverage parameters associated with each of the failure modes.

You look at the non-coverage parameter. That is basically faults that were not caught by the system architecture or the system parameters and basically transitioned through to the end out put of a failure. And since the availability failure rate can be inferred from the non-coverage, you can then come up with transition rates for the particular failure modes that you are interested in.

This is not the only way to do this. This is a particularly powerful methodology and it has got a lot of applications. But there are other ways of doing this.

You can do it with non-parametric models. You can do it with software reliability models. But this one is particularly nice because you can actually physically go out and test it.

You also need, of course, a statistical analysis methodology because you cannot test every possible failure state. So you look at what the statistical coverage estimate is. And based on certain assumptions, you can come up with a number of injections trials you need to do to cover the system at a particular confidence level and a particular failure rate you are interested in.

CHAIR APOSTOLAKIS: See this is now something that can be tested --

MR. ARNDT: Yes.

CHAIR APOSTOLAKIS: -- by looking again at the operating experience. If I had applied all the injection techniques say to the Palo Verde incident --

MR. ARNDT: Right.

CHAIR APOSTOLAKIS: -- would it have prevented what happened?

MR. ARNDT: Right.

CHAIR APOSTOLAKIS: I think it is really a powerful way of saying something about --

MR. ARNDT: It is a very potentially powerful technique. And in point of fact when we originally started looking at this, we looked at it as an augmented inspection technique. Basically we have since started using it to help us provide additional data to support the risk stuff.

But when we first started looking at this about four years ago, we started looking at it as an augmentation of our inspection and analysis techniques. So we are currently working -- the second benchmark test has dual purpose.

We're looking at it as a what can we learn about this particular system we are testing as well as what data can we generate to support this particular project? But that is the discussion for another time.

And one of the issues is where do we get the data to start with, which helps augment what the partitioning of the data looks like. And we get it from exactly where you would expect to get it. We get it from actual failure data from this particular system. We get it from commercial failure databases like PRISM and Mil Standard and other things like that, which you heard Brookhaven talk about the last time that we were here.

CHAIR APOSTOLAKIS: But if you have a multi-state representation of the components and the systems, how would you get rates for state J? That seems to be --

MR. ALDEMIR: You inject faults to stimulate state J.

MR. ARNDT: The point is you come up with a --

MR. ALDEMIR: Some of those states are going to be covered by the system. Some of the --

CHAIR APOSTOLAKIS: We just talked about the fault injection.

MR. ALDEMIR: Right. But that --

MR. ARNDT: In general --

CHAIR APOSTOLAKIS: Transition rates from one state to another --

MR. ARNDT: To another are difficult. There are other --

CHAIR APOSTOLAKIS: It's going to be --

MR. ALDEMIR: We have to make something clear. What the fault injection tests give us is coverage which can be used either failure per demand or non-coverage which can be used as failure per demand or multiplied by the transition rate which is hard data from databases gives you the transition rate, whichever model you wish to choose.

If you use Markov, you change transition rate --

CHAIR APOSTOLAKIS: I hope we're going to have Subcommittee meetings before you finalize any of that.

MR. ARNDT: Yes, oh yes.

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: We will have lots of meetings.

CHAIR APOSTOLAKIS: My biggest objection -- well, not objection, my biggest concern with any of these methods when it comes to numbers is these rates. Where are they coming from? What do they mean? Why are they constant?

MR. ARNDT: Right. Or if they are changing, what is the change? And this method is not wed to a Markovian assumption. You could use semi-Markovian models and things like that.

CHAIR APOSTOLAKIS: Today I see the discussion more along the lines of the failure modes.

MR. ARNDT: Right.

CHAIR APOSTOLAKIS: But not the quantification. So I'm not going to raise any --

MR. ARNDT: Okay. When we do the quantification report in a couple of months, we can come back and talk to you in more detail about this particular issue.

CHAIR APOSTOLAKIS: Before anything is final I hope.

MR. ARNDT: Yes.

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: This is basically just a slide and I'm going to skip through it quickly. There is a mechanism that Tunc has developed for integrated DFM and Markov into a event tree for a traditional fault.

CHAIR APOSTOLAKIS: So again, what would be the events and the states?

MR. ALDEMIR: It is simply --

CHAIR APOSTOLAKIS: Are you going to write a paper on this?

MR. ARNDT: Yes.

MR. ALDEMIR: Yes. When I get a chance to.

MR. ARNDT: We've got a couple of conference articles on this. And we are working on a couple of journal articles on it.

MR. ALDEMIR: There are three journal articles that are in preparation but it is just a matter of timing.

CHAIR APOSTOLAKIS: With the blessings of Steve?

MR. ALDEMIR: Yes but they have been very nice. I mean it doesn't take for them to bless it but for us to put it together is time consuming.

CHAIR APOSTOLAKIS: Yes.

MR. ALDEMIR: Remember each of these has about six to seven authors so coordinating the authors is not that easy either.

MR. ARNDT: In any case, there is a methodology that has been developed. And we are using SAFIRE, not because we think SAFIRE is better than the other methods, it is because we can get access to the source code.

CHAIR APOSTOLAKIS: Right.

MR. ARNDT: So let me sum up and then turn it over to my colleagues to talk about the traditional modeling methods.

CHAIR APOSTOLAKIS: Well, we have a break in between.

MR. ARNDT: Yes, I think you have a break after this.

CHAIR APOSTOLAKIS: Yes.

MR. ARNDT: So we have developed this methodology. We have submitted to extensive peer review. We resolved as many of the comments as possible. We will have a comment resolution.

The first benchmark has been developed. And tested for steady state as well as transient conditions. The results have been compared and we have resolved the initiating events.

We are starting to do the preliminary analysis with the data. And that will be available in a few months. And we will come back and talk to you about them.

So we believe that this is a -- I should really watch my terminology -- conceptually proof of concept, we are there. In terms of practicality, in terms of effort associated with it compared to the cost benefit that Alex was mentioning, it is obviously something that we need to look at.

And how much we need versus how much level of detail versus the particular regulatory decision we are making is something we are going to have to work out. And let me go back to that for a second -- well, let me finish the last slide.

So we are going to do the next benchmark. We are going to do the quantification. We are also going to develop the stand-alone model so we don't have to integrate fully to get some failure mode information and things like that.

We are in the process now of putting together the second benchmark and specifying it and all that kind of good things. Some of our engineers and our contractors' engineers are actually at the training on the new system this week. And then when we get that up and running, we'll do the benchmark -- the second benchmark problem which, again, is the RPS, which has got different characteristics than the feedwater system.

And I know there has been a lot of consternation among the community associated with the fact that we did the feedwater system before we did the RPS but that was simply a matter of that is a system we could get. And in a perfect world, I probably would have done the RPS first and the feedwater system second. But that is the world we live in.

Let me take two seconds to go back and talk about this issue associated with the regulatory decision we are trying to make. If you go back to the three problem statements we talked about when Cliff was presenting, the first one was develop additional clarification on what was needed for the Part 52 design cert. and COL applications.

We have got a regulatory requirement that basically says if you are going to come in under Part 52, you have got to present the results of your PRA. So that is a specific regulatory decision we have to make as to what information do we need from the digital system aspects associated with that.

Problem Statement 2 basically says if possible, can we use some risk insights to make the decision criteria on things like D3 or communications or cyber or whatever better? That is a particular regulatory decision.

Statement 3 -- Problem Statement 3, which says develop a comprehensive methodology that uses the state of the art, regardless of the debate about what the state of the art is, to come up with a risk-informed decision-making criteria. That is a much higher threshold in terms of decision-making. We are establishing a 174-type process which allows us to generalize risk-informed applications of digital systems.

So as I mentioned when Cliff was talking, the research has basically three objectives. It originally had two, now it has three.

One, to get smarter about these systems and to understand the methods and maybe come up with an independent assessment tool for us.

Two, to take that information that we got smart about and write that generalized all-encompassing document which will probably be a reg guide but it may be some other document.

The third one is to take what we have learned to date and try and have input into that second problem statement associated with short-term improvements based on risk insights to the current regulatory process.

Our big debate, I think, is the industry thinks that the current methodologies can be pushed further. We're not sure yet. That is really where we are in that space.

As you know, the traditional modeling

methods approach is next and I think you want to take a break.

CHAIR APOSTOLAKIS: We'll take a break unless there are questions.

(No response.)

CHAIR APOSTOLAKIS: Okay. Back at five minutes past three.

(Whereupon, the foregoing matter went off the record at 2:48 p.m. and went back on the record at 3:08 p.m.)

CHAIR APOSTOLAKIS: Now we are talking about traditional methods. Okay.

MR. KURITZKY: I'm Alan Kuritzky. I'm from the Office of Research. I guess if you hear Mike Mayfield this morning talking about the speakers coming up, he mentioned that I had 25 years experience in PRA. He definitely didn't mention that I had any experience in digital I&C and there was a reason for that since I don't.

And that is the reason why from Brookhaven National Lab we have Gerardo Martinez-Guridi and Louis Chu with me here. They are going to handle the tough questions. The presentation I'm going to give was pretty much prepared by them.

You heard earlier today from Steven and also, I guess, at previous meetings about the dynamic modeling methods for digital systems. What I am going to talk to you about right now is our work on the traditional methods for modeling -- reliability modeling of digital systems, the difference basically being that by traditional we are referring to well established, commonly used modeling methods whereas the dynamic is more of the cutting edge, advanced-type methods.

The presentation today is going to -- I will give you a quick status of where we stand on our traditional methods research, what our plans are for this project, our objectives and approach, a short review of some of the traditional methods that we have looked at so far under this work. Also, we developed criteria for evaluating the different reliability models using those methods. So we will go over those criteria.

We also selected a number of applications or studies using those methods for comparisons against those review criteria. And comparing those models to the review criteria allowed us to identify the limitations and capabilities of the different methods. And essentially it establishes the state of the art for those methods.

And finally we will have some concluding statements including which traditional methods we have selected for a further look.

Near the end of last summer, there was some concern that the work being done under the traditional methods research was not totally in line with that being done under the overall Office of Research Digital I&C Reliability Modeling Program, including the dynamic work. So we had a project review meeting in October of that year and the outcome of that meeting was that we were going to refocus the traditional methods work specifically on identifying and demonstrating the capabilities and limitations of existing methods as they stand today.

We also -- what came out of that meeting was that we would emphasize and increase the amount of stakeholder interactions with the process. And also that the Office of Research should develop an integrated project plan for the overall digital I&C reliability modeling efforts and coordinate their work with the program offices: Office of New Reactors, NRR, NMSS.

We have developed the draft innovative plan for that work. It has somewhat been overshadowed because in the interim, as you heard earlier today, there was a Steering Committee established on the direction of the Commission, the NRC Digital I&C Steering Committee, and we have been working to supply them with a project plan. And that has kind of superceded the plan that we had worked out initially. Ours kind of feeds into that and maybe offers more detail in some areas.

The plan we have for the traditional methods research involves essentially five tasks. There is now a task 1a so I guess it is six tasks. But the first task which we are going to describe today -- it is the work we have done so far -- involves identifying what traditional methods have the most promise for use in licensing applications. Or for increasing or accounting for digital systems in current plant PRA models.

We have a draft letter report prepared by Brookhaven on that task and we are going to describe or discuss many of the aspects of that report in this presentation.

We also have added a task 1a which is going to involve an external peer review of the information from that report. The main focuses of that peer review will be on the criteria that were identified and also on the selection of which traditional methods to pursue.

We are now currently working on Task 2 in parallel. And Task 2 advances what we came up with in Task 1 to start developing the selected methods and how we will actually apply then to the test cases. The test cases in Tasks 3 and 4 are the same ones that Steven mentioned for the dynamic modeling methods, which is a digital feedwater control system and a reactor protection system.

Lastly, we also have a task to integrate the results into a PRA. In terms of methods involving traditional fault trees and event trees, that should be a pretty straightforward integration. To the extent that we use other types of techniques such as Markov, some variant of Markov modeling, there will need to be some type of -- some techniques used in order to smooth that integration.

Okay, Task 1, as I just mentioned, the objectives are to develop criteria for evaluating the reliability models and these draft criteria that we have identified could well find themselves in the future as part of regulatory guidance for what is acceptable in terms of, you know, risk-informed decision-making or use of risk insights.

We are going to use these criteria right now under -- well, we have used them under Task 1 to help us determine which methods have the most promise. But the most important aspect, I think, of those criteria are their potential for use as acceptance guidelines or attributes for modeling for later regulatory uses.

CHAIR APOSTOLAKIS: Is the Markov model is what the previous speakers also --

MR. KURITZKY: Yes.

CHAIR APOSTOLAKIS: So why is it the traditional method?

MR. KURITZKY: Okay. We are going to get to that actually in a few slides.

CHAIR APOSTOLAKIS: All right.

MR. KURITZKY: I think Steven talked a little bit about that in his previous talk. But we will try to amplify a little more about the use of Markov modeling techniques in both parts of the project.

Okay, the approach that we used for Task 1 we used a search of the literature as well as our experience to identify a number of traditional methods to evaluate. Those methods included fault tree and event tree methods. Again, some variant of Markov modeling techniques, the SINTEF method, which is used by the Norwegian oil industry and is also some type of simplified Markov modeling, reliability prediction methods, and also we looked at in the NASA PRA procedures guide, there is a section on software modeling that provides what seems like a fairly reasonable idea of how to quantify or include software failure probability into a fault tree model under the PRA.

In addition, we also had some information on a simplified analytical method that was used for a Japanese ABWR. And so we looked over that also.

After identifying the traditional methods to look at, we developed criteria for evaluating the methods or, more particularly, to evaluate the models that were using those methods. The criteria were focused on capturing all the unique or digital system unique features that might effect system reliability.

After coming up with the criteria, we identified applications of each of the methods from the first bullet for comparison to the criteria. In doing so, we have identified the capabilities and limitation of those models. And that would establish, like I said before, essentially where the state of the art exists right now.

We are engaging the technical community in this work. We have, as someone mentioned earlier today, there is a web page, a digital I&C web page on the NRC public website. We also, as was mentioned earlier, had a public meeting. Last week, it was the task working group meeting on digital system risk. That was a public meeting.

And we received -- well, we didn't receive a lot of feedback at that meeting. Industry has indicated they would try and supply us some feedback on essentially this presentation today, fairly similar, that we could then post on the website and we would have available to us.

Also we are planning, as I mentioned before, to have an external peer review panel go over the criteria and the methods that we selected. And that will probably occur sometime in the May/June time frame.

The traditional methods that we selected included fault tree/event tree methods, most standard. That is the one that has got wide use across the entire international PRA community. It has been in use for a very long time. It has been used for a whole different host of activities, different industries, aerospace, chemical has used it, of course it is the standard for the nuclear industry.

It is well suited for identifying plant failure modes, accident sequences, and then cut-sets that identify exactly what failures must occur in order to result in an undesirable state at the plant, i.e., core damage. It also is very useful for quantifying the probability of those various states occurring.

One limitation of the method is that it only treats timing events and interacts with plant processes in an implicit way. In an implicit and approximate way.

And essentially it deals with the timing based on what events are in the event tree, what order they occur, what if there can be some post-processing of cut-sets if there is a particular timing issue that isn't well treated by the event tree structure. And its interactions with plant processes really come about in the systems and success criteria that are used.

The issue of the Markov modeling, as Dr. Apostolakis just mentioned, we are using a type of Markov modeling in the dynamic research. The way that we differ in what we are doing here with Markov modeling is we are using it as essentially a way of characterizing the digital system hardware failure probability. In the dynamic work, it is being used as a dynamic technique to model the complex interactions of the various parts of the digital system and, most importantly, the interactions of the system with the plant process dynamics. Something we are not addressing when we use Markov modeling in this regard.

So the Markov modeling being done for the traditional methods is a much simpler -- it doesn't have quite the scope that is being used in the other effort.

Markov modeling has, in fact, been used for modeling nuclear power plant systems, including digital systems, so it is an established and existing technique. It allows, as you have heard from obviously the discussion that Steven and Tunc had before, it allows for explicit modeling of the different states that a system can be in and it accounts for repair of equipment, explicitly treats failures and repair times within the model.

One of the drawbacks of it is that with a complex system, you can quickly get a very large number of states. And so dealing with or resolving the model becomes fairly difficult.

It also considers interaction with plant processes implicitly in an approximate way. I think what you saw with the other effort is that they are trying to do a more explicit addressing of those plant processes but it can be done in a more simply way just, again, based on what systems and the success rates that are being used in the model.

As I mentioned before, the integration with existing plant PRAs is not going to be nearly as straightforward as it would be with a fault tree approach.

The SINTEF method, as I mentioned used by the Norwegian oil industry, it is an adaptation of the method that is laid out in IEC Standard 61508. It is a very, I guess, a simplified, even more simplified Markov model. One of the simplifications is that it entreats -- it breaks the system into subparts or subsystems and evaluates each system on its own, assumption that common cause failures will dominate the system unavailability or the subsystem unavailability.

It doesn't treat independent failures. And it also doesn't treat cross-combination of failures between subsystems. So those are some limitations for a more complex redundant system that we have in a nuclear plant that could end up being a significant drawback.

It does, however, explicitly model fault detection. And makes the distinction between safe and dangerous failures.

Another seeming drawback of the method is that apparently, at least from what we were able to see, from what we had documented, all the data that was used in the model for failure fractions, for beta factors, most of it was just based on expert judgment. And that limitation on data is something we are going to see showing up in most of our methods here.

Reliability prediction methods estimate the failure rate of circuit boards in terms of failure rates of individual components. It can be used for systems where you have series components. Again, for redundant systems, it is not very effective.

It is possible to be used as a source of data for some of the more robust modeling methods. Again, we were not able to identify the technical basis for a lot of the values used with those methods. That may be a limitation of our data gathering technique or it just may be that they are just not publicly available and they are not usually obtained.

The RPMs also do not address uncertainty as many of the -- well, certainly many of the models that use the methods that we are discussing did not address uncertainty.

The NASA PRA procedures guide software modeling method provide a framework for considering software failures in the PRA but, again, it just focused on the software. The NASA PRA procedures guide does not address specifically digital systems or hardware modeling. And so as a result, we didn't further pursue any applications of the NASA approach.

Some general observations from the review of these various methods, the fault tree, event tree, Markov, and SINTEF methods are fairly general. And so we pursued applications or evaluate applications of those methods in the work we did under Task 1. We also had an application of the simplified analytic method used for the ABWR and included that in our work also.

As I mentioned, the RPMs, they may be useful as a source of data for some of the other methods but they, themselves, were not really robust enough to deal with the types of systems we see in nuclear plants. And, again, the NASA approach was just for software and we had no application of that approach to review.

The next step in our work after

identifying which methods to pursue was to identify the set of criteria that we felt would be useful for evaluating digital systems and also might be useful for regulatory guidance later on.

Some of the considerations that went to those criteria or the identification of those criteria are the fact that we felt that the modeling should be supported by a systematic analysis of possible failure modes and effects. And this is particularly important with digital systems where there is a lot of unique aspects of the systems and types of failures that are not common to traditional pump-and-valve systems in the PRA.

The analysis should also go deep enough to identify and uncover any potential dependencies both within the system or between that system and any other system that is being used at the plant to mitigate any particular scenario.

The model should, of course, include software failures or address them in some manner, including common cause failure. Again, dependencies with the system and any other systems at the plant are important to identify. And human errors, both in terms of -- well, I guess in terms of errors introduced in upgrading hardware or software upgrades or human errors that result from inadequate man-machine interfaces, need to be accounted for in some manner.

There was some question in the technical community as was discussed previously as to whether the timing issues need to be treated explicitly in these models. Again, traditional event tree/fault tree models are static and do not explicitly treat timing.

The work that is being done under the dynamic research that Steven discussed with you just recently does try to deal with those with timing in an explicit manner. And that is one thing that we will have to try and determine based on looking at both parallel paths is how important that explicit modeling of time is to overall system reliability and to the understanding of potential failure modes of the system.

Self tests and self-diagnostic-type of features for digital systems should be included and self correction. However, when they are included, you must also consider not only the benefits of such systems but also some of the drawbacks. I think someone mentioned earlier, it may have been Paul, that while there is definitely benefit to having self-diagnostic features with the system, you also need to be concerned that they can introduce actual failures into your system and they can result in failures that would not have occurred if you didn't have that self-diagnostic capability.

So it is important to account for those features. But they need to be accounted for both in the positive and potentially negative aspects.

Quality data is a big key. Obviously with any type, if you want to quantify the models, you need data of good quality and that is something that right now is somewhat lacking. And by quality data, we mean it should be applicable both in terms of the system application and the system operating environment. The sources of the data should be provided. And they should be well documented, the analysis of the data and the parameter estimations should be well documented.

Uncertainty analysis is also something that we need to address. Many of the models that we looked at did not address uncertainty analysis. And by that we want to look at modeling uncertainty in terms of what assumptions were used and the impact of those assumptions as well as identifying what sources of uncertainty exist in the models. And the parameter uncertainty, evaluating and then propagating it through the model.

I think we had one model that did, in fact, do a fairly decent job with parameter uncertainty. I think it was the AP 1000, a vendor PRA which propagated uncertainties.

And, again, ideally the model should be easily integratable into existing plant PRAs. One of the goals of this work is to have -- to upgrade the PRA models so they can account for digital systems. And so we want to be able to integrate those into existing plant PRA models.

What is listed on this slide are the eight categories of criteria that we identified. We identified a total of 48 criteria. They fell into these eight different categories. If you look at these eight categories, they have a remarkable similarity to the challenges that were listed on Cliff's slide when he was discussing Problem Statement 2.

Again, level of detail of the model, how far down do you go, do you go down to the microprocessor level, do you do it a higher level? Very important, again, as I mentioned before, is a systematic identification of failure modes of the digital system. You know the unique digital features and aspects of those systems, we need to understand them so we can identify how the system can fail and include it in our models.

Software failure is obviously a big issue. The dependencies. Human errors, as we just discussed. Ease of integration. Data. And documentation results. All the same issues we just discussed in the previous slides are the genesis for where we came up with these 48 criteria.

Right now in the work done so far we did not give any relative weights to those criteria. We just kind of evaluated each of the models against them just scoring how many criteria they met or didn't meet. We did not assign any type of partial meaning of criteria. It was just pretty much a binary you met it or you didn't meet it -- yes, no. And we didn't give any weights to the different criteria.

But if these criteria are to be used in the future for regulatory guidance or other purposes, we will need to revisit that and determine not only do we hope to have feedback that may modify this exact list of criteria but also it may become evident that certain criteria are much more important for modeling or determining what the system unavailability is or failure probability is as well as which criteria are most important for understanding how the system works and understanding how to model the different features.

CHAIR APOSTOLAKIS: Yes, two through five it seems to me are essential.

MR. KURITZKY: Yes. Well, right now we believe all of them are essential. But you are right. Two through five are the guts of digital system modeling.

Just an example of some of the criteria, this is Criterion 2.2 dealing with -- I think this was -- identification of failure modes. Communication, voting, synchronization, those are specific aspects of digital systems, particularly ones that can lead to dependent failures. So that is an important consideration when putting together a digital reliability model.

A couple more examples of criteria. This is from Category 7, which is with the data, 7.1 is a question of whether or not you have actually what I consider plant-specific but application-specific or operating environment-specific data that can be used for the components as opposed to 7.4 which says if you don't have that data, if you are using generic data, is it applicable?

And, again, obviously to the extent we can get it, application and operating environment-specific data would be of much better value. Using generic data will lead to, of course, fairly large uncertainties and open up to all kinds of arguments as to whether it is applicable at all.

Okay, after we identified the methods and the criteria that we wanted to evaluate the models against, we went and looked for which types of models we could find for these different methods. In the fault tree methods, we identified three models. We have the AP 1000 reactor vendor PRA that was here at the NRC, and the ESBWR reactor vendor PRA.

And we also had a plant-specific model for a Westinghouse or a CE 80+ design for the ESFAS of a Korean plant.

Again, as I mentioned before, we did have a simplified model of a combined RPS ESFAS for a Japanese ABWR. It was a very simplified version or a simplified analytic model. We took a look at that as well as we had the Markov model of the Tricon platform that was our entry in the Markov arena. And then we also took a look at an example of the SINTEF method.

We evaluated all those against the list of the 48 criteria but our evaluation focused just on whether those models met those criteria. We did not attempt to evaluate or validate the models for the purpose of which the developers of the models actually used them. So we were not evaluating whether the AP 1000 was a good PRA or was the SINTEF application was a good application of the SINTEF method. Just rather whether those applications or those models, how well they met our criteria.

Again, as I mentioned, we evaluated each of the models against those criteria. There was obviously a large amount of qualitative judgment and subjective judgment in doing that assignment. This is one of the things that can be looked at as part of the expert review panel although more important is not so much how well the different -- or how we assigned the models to the criteria. It is the actually list of are these the right criteria? And are these the right methods to pursue?

The importance of knowing how well we did score the existing models against those criteria is in the fact that it helps us establish what is the current state of the art with these different methods.

Now the extent to which those applications that we collectively had for any given method, how well they collectively met those criteria kind of gives us that basis for where the state of the art stands right now. However, that is based, again, on those limited models that we looked at. So if there are other models out there that have done a better job at any of these particular criteria, then that could be collectively synthesized into future modeling efforts and, therefore, demonstrate that the state of the art is a little bit more advanced.

We made a strong effort to try and get some of these more international models of PRAs. To date we have not been too successful. We made contact with a couple of foreign agencies. We discussed some of the topics with them.

Generally what we are hearing back is that in past history, they have attempted to model digital systems and after throwing a lot of money at it, grew very frustrated in their inability to do a good job of modeling particularly the software. But we have not yet been able to obtain actual PRA models to see what actually went into their fault trees if they did, in fact, develop them.

But, again, we have an open invitation to all stakeholders that any type of information they can provide on other models, we would be happy to look at to see whether or not there are other criteria. As you can see from the fourth bullet, the most criteria that any single model that we looked at met was 16 out of the 48 criteria. So 21 of the criteria were not addressed by any of the applications. And an initial nine were only addressed by one application.

So to the extent that there can be other applications or models that address more of those criteria, we'd love to see it.

The fault tree/event tree models, the three fault tree/event tree models satisfied the most number of criteria.

MEMBER ABDEL-KHALIK: How much as your familiarity with these models contributed to that last bullet?

MR. KURITZKY: Well, I was going to say something. I don't know so much about whether or not our familiarity with those models contributed to that last bullet but they certainly had impact. But the development of the criteria was by people who are most familiar with those models.

And in honesty are -- envisioning again one of objectives is to be able to include digital system models in a plant PRA and so there is kind of a pre-bias towards, you know, we are obviously all eager to integrate that into a PRA model if it is a fault tree-type thing. So I'm sure there was some bias. I don't want to speak for Brookhaven, who did that work. But there is a potential for bias there.

But nonetheless, we tried to keep a pretty open mind as to how well the other methods or the applications of the other methods met the criteria.

MR. MARTINEZ-GURIDI: Yes, I mean the potential for the bias exists but I think we tried to be as impartial as possible.

MR. KURITZKY: Okay. Some of the --

MR. ARNDT: One thing I want to point out before we go on, when we talked about, in the first presentation, the fact that the short-term goals would be influenced by our research to date, the opposite is true as well. The industry has committed to provide us input on some of their techniques.

And we are trying to work with EPRI to do more collaborative work with them. So as we learn more from the industry, we are committed to factoring that into our research effort.

MR. KURITZKY: Yes. It is a living process.

MR. ARNDT: A living process.

MR. KURITZKY: Okay. Some of the observations after we applied the various models to the criteria, main strengths of the applications across the board mostly were that common cause failure of hardware within a system was included. It was typically modeled. However, again, the data for quantifying those contributions was somewhat suspect.

Individual and common cause failures of software were explicitly included in the models for most of the studies that we looked at. However, the extent to which they were included and the quantification of those events was, again, something that needs work. There was definitely a lacking.

Some of the main limitations across all of the studies, again, as I mentioned before, it is very important to have a systematic evaluation of the possible failure modes based on the very unique features, characteristics, and components of the digital systems. And we did not see that in the majority of the -- or pretty much in all of the studies that we looked at.

Again, I need to caveat some of these limitations by the fact that we are basing these comments, these review comments on the information we had available to us. So whether or not there are some proprietary or some other data that the developers of the models used and they did not release or it was not publicly available or we could not find, may, in fact, ameliorate some of these concerns.

But from the information we saw, there appeared to be a lack of systematic evaluation of the unique failure modes and effects for these digital systems.

Also in the failure parameter data, there just was not a lot of good quality data for quantifying these models. And what data was used, there was generally lacking any documentation or documented basis for the data.

Quantitative software reliability methods, of course lacking across the board. It is obviously a big issue. There are arguments as to how and if you can quantify software reliability or at least a failure probability for use in a PRA. So it is just a big open issue.

Treatment of uncertainties, again it was one that was found across the board for most of the applications with the exception of the Westinghouse AP 1000 PRA.

Just to go into a little more detail on some of the main limitations that we identified. The level of detail in the PRA models that we looked at did not appear appropriate to model all the different unique features and components of digital I&C systems. In some cases, aspects such as communication network voting, synchronization were not considered in the models.

The propagation of the failures, to propagate from the digital system out into other systems in the plant were not typically considered. Also, the basis for the effectiveness of some of the fault tolerance features was not provided.

And, again, as I mentioned earlier, some of the negative -- potential negative aspects of some of these features were not considered in the models.

The lack of failure parameter data, again, the raw failure data, as I mentioned, was not publicly available or at least we couldn't get a hold of it. Very likely proprietary manufacturer data. So most of the estimated hardware failure probabilities that were in these models were based on proprietary data.

The analysis is not documented, particularly, for instance, in the advanced reactors periods we have from Westinghouse and the ESBWR PRAs, there was nothing in there about where the data came from.

We did end up extracting some data from PRISM but that data had very large variability to it.

B&L estimates and failure rates using that data and obviously came up with some very large error factors. So I think also Steven mentioned they used some of that data for the dynamic method. I mean there is just a dearth of good data out there so it is what it is. But that is definitely an area that improvement is definitely welcome.

Some of the important parameters such as the hardware failure rates and the common cause failure parameters, again, just scarce. There's not much out there. So expert judgment is used to quantify a lot of these models.

Again, I'm not going to belabor the software issue. It is well known. The National Research Council or as we referred to previously as the National Academy of Science Report, recommend that software failures be included in the reliability model.

There was one dissenting opinion in that report. I guess Nancy Levinson felt that you just could not quantify software failure probabilities. But in general, the Council recommended they do be included in models.

Our comparison of the models that we looked at to the criteria just further underscored the fact that right now there is no consensus method for doing that.

So conclusions, we went through and identified a detailed set of criteria, again 48 of them, from what we felt would be the appropriate attributes for a digital system reliability model to be used in a PRA.

These criteria that we identified would apply to all reliability models of digital systems, not just necessarily traditional models. And they can be used to develop regulatory guidance -- either regulatory guidance specific for digital system licensing applications or for general PRA guidance such as Reg Guide 1200 or whatever other guidance would be applicable.

Again, we looked at six different models and applied them to the criteria to determine where the state of the art existed. As I mentioned before, even the best of models only met 16 of the 48 criteria. And there were a large number of the criteria that were not met by any of the models.

Nonetheless, even though the statistics on the criteria may be somewhat negative, it really, in our estimation, it boils down to three main areas that need to be improved upon for use of traditional methods. The first is, again, the systemic evaluation of failure modes, specifically digital systems. And regardless of whether we quantify or not, it is just an important thing to do to understand how the systems can fail.

The second thing is getting -- if we do want to quantify is getting appropriate data that we can use for the models.

And third is dealing with the 800-pound gorilla, the software reliability.

There is also the issue of uncertainty analysis. Again, that one is more in the application of the methods. It is not an inherent limitation of the methods themselves. Any of those methods you can perform uncertainty analysis for them even if the models we looked at did not do that.

Bottom line, we identified the fault tree/event tree methods and our version of the Markov methods as the two most promising methods for being able to model digital systems in a PRA.

Those two methods do not themselves inherently have the limitations that we just described above. The methods themselves don't. But any models you want to use applying those methods is still going to need to address those items.

So our bottom line conclusion is it may be possible to use those two methods to develop reasonable digital system reliability models but we do need to address those three main bullets at the top of this slide.

Next steps, as I mentioned previously, we're going to set up a peer review panel to go over the work that we just did under Task 1, essentially seeing whether or not we have the right criteria. And also seeing whether we have come up with the right methods for pursuing.

And then secondly, as you saw from the slide on the tasks coming up, we are going to go ahead and further develop these two methods and apply then to two test case systems so that we can further demonstrate the capabilities and limitations of these methods and establish where the state of the art exists.

CHAIR APOSTOLAKIS: Any comments?

MR. KEMPER: Yes, this is Bill Kemper. I just wanted to add that unrelated to this, we went off and had Oak Ridge try to ferret out some of this failure data for different purposes so that we could use it in terms of review, you know trying to target our reviews more effectively on digital systems.

And they, too, are struggling with trying to find some data that is usable. So this is clearly a big issue here.

CHAIR APOSTOLAKIS: Didn't Brookhaven also look at some data?

MR. KEMPER: Yes. Brookhaven did their own data search. But we had Oak Ridge do yet another one for an unrelated reason to this project and was hoping that the data would be usable maybe at some point once we looked at it for this, too, and we are not having much luck there either.

MR. KURITZKY: Yes, I think there are two aspects. The Brookhaven work -- the work that Brookhaven did previously on data, similar, I think, to what Oak Ridge did, they looked at data. In their search of LERs or in other software failure events, they were identifying -- not to come up with failure probabilities but just to see description of the events to see how the software can fail to understand different mechanisms of failure.

CHAIR APOSTOLAKIS: Which is the most important thing right now.

MR. KURITZKY: Right. It is a very important thing, exactly. And the second thing they looked at was also for hardware failure databases.

They actually looked at databases. Because with the software, again, you are just looking at events. You are not getting failure probabilities. With the hardware, we were actually looking to see whether or not there were some actual failure parameters, some actual failure rates, failure probabilities like we used for the hardware part of the digital system.

And so they were evaluating certain databases in that regard. And even that, again, was not too promising. But that's where we are.

MR. ARNDT: At the risk of overstating the point, there has also been several studies looking at software failure rates, if you will excuse the expression.

CHAIR APOSTOLAKIS: That's fine.

MR. ARNDT: NIST has done a study. Bev Littlewood has done a study. There have been a number of studies out there. The biggest problem with that is almost all of it is very application specific.

We heard this morning in detail the quality of the development process, the specific application, the amount of testing, the amount of V&V, software failure rates, if you are going to actually look at an independent software model, is extremely dependent upon what the application -- intended application is.

CHAIR APOSTOLAKIS: The context.

MR. ARNDT: Yes. Well, both the context and also the development process. So it continues to be a challenge. We are looking at it. We are working on it. We are obviously interested if we get applications from the industry that includes that kind of thing, we're going to have to be smart enough about it to be able to make an assessment. But it ain't easy.

DR. GUARRO: This is Sergio Guarro. One thing that kind of bothers me a little bit is this reference to digital systems without distinguishing what is inside a digital system because there is the hardware on which it runs. There is the software self-management as to the timing, memory, location, et cetera, et cetera. And then there is the function itself that the software hosted on the system accomplishes.

And it is not clear to me that the same matters would be good to model these three different aspects. I think evaluating a method against "digital system" without, you know, looking at the pieces of the digital system as they stand rather distinguished from one another may be not the right way to look at them.

MR. ARNDT: Yes, that is certainly an issue, Sergio. And this study, as well as others, is making certain implicit assumptions about that in essence because we are looking at the specific application, in this case the AP 1000 or whatever.

One of the reasons why we are exposing both of the variety of methods in traditional and dynamic to two specific benchmarks is to try and get a handle at least a little bit on the application-specific, the hardware-specific, the amount of V&V and those kinds of issues.

DR. GUARRO: But you see the thing is there are methods out there that may be good for one aspect. But if you evaluate them against something for which they were not even intended or at least for which they were not applied because the developer was interested in one of the three aspects -- in fact I know that some of the NASA work that I have been involved in was focusing on software. It was not focusing on the hosting hardware, for example.

So there is other work done at NASA on that. But, you know, I'm just saying so those were handled in separate ways. And so when you look at the results of a particular application that was intended for one purpose and you try to make a judgment across your definition of digital system, yes, that method will fail in the sense that it was not even tested in that direction so to speak.

So I think I would be a little bit more careful in the way you go about judging, you know, against your 48 criteria. Maybe you should partition for different aspects of the model.

MR. MARTINEZ-GURIDI: Well, I think we share your concern.

CHAIR APOSTOLAKIS: Who are you?

MR. MARTINEZ-GURIDI: Gerardo Martinez-Guridi.

CHAIR APOSTOLAKIS: Now you can speak.

(Laughter.)

MR. MARTINEZ-GURIDI: I think, in fact, we share your concern. Out of the eight categories that we have, the first category is the level of detail of the model. So in the level of detail, we are concerned that all the important details of the model, all the different aspects are taken into account.

So, for example, when we reviewed the different applications, we saw that there were at the fairly high level, that is actually one of our concerns, we feel that the necessary level of detail of the analysis has to be evaluated for the model to be actually, you know, good enough for the evaluation.

So we are aware of that. And we share your concern.

MR. KURITZKY: And this is Alan Kuritzky. Also, Sergio, I think to keep in mind is that what we're doing now is we are just looking at where the state of the art exists. We are not advancing it. We want to look at a snapshot of where we are right now in time.

DR. GUARRO: I understand. But I guess you should be careful in how you characterize, you know, some of these results. Maybe you want to say okay, this was untested in this area rather than, you know, marking it as not good for that area, you know, because as I said, in some cases, some of these methods were simply not intended or applied in the direction which you need applied.

MR. KURITZKY: Right. And again, this is Alan Kuritzky. Actually the results of our comparison had yes and no put in the table. But we also had a lot of N/As or not applicable or not available. So we recognized that not all the models that we looked at matched up exactly with the criteria, with all the criteria.

CHAIR APOSTOLAKIS: But I think we should -- we understand Sergio's concern.

DR. GUARRO: My concern is simply hopefully, you know, this evaluation is not a preclusion for, you know, some further evaluation in the future if there is a need and a benefit in looking at something. And it may be extrapolating it from where it was originally applied to a useful application in the nuclear plant area.

MR. KURITZKY: Okay.

MEMBER ABDEL-KHALIK: I have a question about the systematic evaluation of possible failure modes and effects. And the question in my own mind is whether this is really a problem with the analyst or a problem with the method.

But I sense that if you have an analyst who is familiar with the dynamic methodologies and so on, would that analyst be able to do a better job using traditional methods?

MR. KURITZKY: Yes. Well, it definitely goes to the quality of the analyst. What we were looking for specifically is having it somewhat systematic so that whoever happens to be -- there may be -- certainly it is very, you know, subjective in the sense that one analyst is going to go and do his failure modes and effects analysis for the system and come up with whatever failure modes he thinks of.

Another analyst could go and look at that same system and come up with not exactly the same list.

And what we want to do is because what we saw from the applications that we looked at was that no one seemed to do a fantastic job, that there should be some systematic, you know, some tools or something to help people do a systematic identification of the failure modes.

That way it would be a little more consistent across the board. And we wouldn't end up with certain models having well possibly lower failure probabilities because they just didn't consider certain failure modes that are more detailed -- you know, a better analyst, you know, did a more detailed look and found other failure modes.

So the idea was that it is definitely a function of the analyst but we want to have -- we feel there should be some kind of systematic method that would kind of level the playing field.

MR. ARNDT: Yes, actually there are three issues here. One is the one that Alan just mentioned. One is the fact that some methods are more likely to yield a broader set than others. And that is an issue associated with what is the best method? What is an acceptable method? And what is not an acceptable method? And that is something we have to work on and evaluate.

The third thing is, quite frankly, this is not a terribly mature area right now. And we can argue how mature it is but as we get better at this and as we do more of them, it is likely that we will get a better feel for what needs to be included and what doesn't need to be included. And have more examples and things like that. So I think that is part of the challenge we have right now.

MR. MARTINEZ-GURIDI: Yes, let me add my two cents here. I think another important aspect is that digital systems are just extremely complicated. And, therefore, for an analyst just to be able to think -- even if he is very prepared, very knowledgeable, just to be able to out of his -- off the top of his head come up with the failure modes is almost impossible.

For some of the systems, it is fairly straightforward because, for example, you may have valves. And the failure modes of the valves are pretty easy. It either closes or opens.

For digital systems, you have dozens of hundreds of signals going around communicating with the microprocessors, communicating with the actuating devices, getting feedback. So it is very difficult to find out in a reasonably complete way all the applicable failure modes.

That is really the main issue. I mean if you do an analysis, how do you get some assurance, at least have some level of confidence that you have been able to encompass all of the important failure modes that can actually lead to failure of the system?

And I think that is one of the greatest issues in this field. Just coming up and modeling a digital system in terms of an analog system is not going to do the job.

MEMBER ABDEL-KHALIK: Thank you.

CHAIR APOSTOLAKIS: Okay. Thank you. We'll move on to the last presentation. Let's try to wrap it up by five o'clock please.

MR. ARNDT: This shouldn't be very long.

CHAIR APOSTOLAKIS: Not just your presentation. The whole meeting.

MR. ARNDT: I understand.

This won't be very long and then, of course, you have to have whatever deliberations you want to have.

CHAIR APOSTOLAKIS: We have discussed more or less the presentation.

MR. ARNDT: I think we are closed on that. We can have an offline discussion if you think we should. And I think we probably should next week to make sure that we have -- we are covering everything you need.

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: This is relatively short presentation. Last time we were before the Subcommittee last year, I gave a somewhat longer presentation on where we were going on the development of regulatory guidance. And I'm going to -- this is a summary of that but it also updates it.

As we talked about earlier in the presentation, we have three goals. We've got Goal 1, Part 52 clarification of the guidance, Part 2, how much can we do in the short term using current methods, and Part 3 is the development of detailed, comprehensive risk-informed decision-making.

So the idea is as part of the risk program, we want to develop that guidance. Because -- and I think this says it in the next slide but I'll say it here anyway -- we want to look at the specific long-term issues and that we have short term issues. The longer term issues are going to get kind of pushed back a little bit in terms of schedule one because we want to understand what we can about the current applications to make ourselves smarter about it but also because of resources.

Now let me make a couple of quick comments about the point in the second bullet here. To develop the guidance, there are several steps we've got to look at. We've got to understand the failure data.

We've got to understand what possible methods might be usable. And that's a factor of two things. One, the research -- what we think is available. And two, what the industry brings to us. Because it doesn't make any sense to write a regulatory guidance on something the industry is not going to bring to us.

The third bullet is the whole issue that we've talked about a couple times today about categorization of the system. What systems really do need to be modeled and at what level of detail? And what are the criteria or guidelines associated with that? And we are going to come and talk to you about that as that develops.

The acceptable methods in the actual

guidelines, what we would like to do is reference specific acceptable methods. Obviously in reg guide or regulatory guidance if the industry wants to bring a different method to us that has the same performance, that is perfectly acceptable.

But it makes everyone's life easier if we can reference a particular acceptable methodology. And hopefully we will come to that as part of either the dynamic or traditional methods research or both.

A third this is the actual performance-based regulatory acceptance criteria. Or acceptance guidelines if you prefer that terminology. That is an evolutionary kind of process.

And I wanted to mention this. If you followed our work in the last three years, the first hack at that was the paper that Nathan and I worked for the PSAM meeting a few years ago. The second hack at it was some of the criteria that we developed in NUREG-6901.

The most recent version of that is the criteria you just heard about. So we are learning more. We are evolving. We are developing a better understanding associated with that. So I'll give you an example. In the PSAM paper we wrote three years ago, the criteria was you need to include all the important failure modes or be able to capture failures that have happened.

In what we heard today, we had specific criteria associated with particular failure modes have to be included. So as we get smarter about this, we are trying to include or exclude various requirements or criteria based on what we have learned. So that is the process.

To remind you, these are the criteria. So I won't belabor that.

We are working on -- I think I mentioned this earlier -- we've shifted some of our resources to the shorter term activities. One, because we want to learn from those activities, and two, because they have a shorter-term priority.

When you see the problem statements and detailed deliverables, this is the document -- the version you will see for Problem Statement 2. And I put this up -- or 3 rather -- and I put this up here for a very specific reason.

The points in that first tick there review the current models, characterize the acceptance criteria, assess the failure data. That is the same kind of thing that we are doing to develop the regulatory guidance. So that is something that is specifically articulated in the third problem statement.

MR. STONE: Steve, can I ask a question or make a comment?

MR. ARNDT: Sure.

MR. STONE: The one issue -- and Mr. Kuritzky pointed it out as the 800-pound gorilla here is that I like the process we have been going through here with doing the comparison between the dynamic modeling and the traditional modeling.

But the one issue that seems to be driving the risk or uncertainty in the risk is the software modeling. And I don't see a success path in this research program to reaching that at this time. That was my main comment. I'm just wondering how we are planning to address that?

MR. ARNDT: That is obviously a big issue. And we hope to, yes, get a success path. Any you can see in here review current modeling methods, including software modeling is one of the big efforts associated with trying to develop that.

We are taking two tacts right now which this may not be super satisfying but this is what we have got so far. One is in the dynamic reliability modeling methodology, we are looking at an integrated state space solution. That is to say not explicitly modeling the software or explicitly modeling the hardware. But modeling it as a joint state space.

There are some advantages to that and there are some disadvantages to that in both practicality issues and in theoretical analysis issues.

In the traditional modeling methods, we are looking at separate hardware models and software models and then the integration associated with them. How do you integrate the failure spaces associated with them? So that is going to address that specific aspect.

Obviously you can do traditional modeling methods in an integrated way or you can do dynamic methods in a non-integrated way. We are not currently looking at that specifically simply because there are only so many resources and that's what seemed to make sense to us at the time from both theoretical and practical considerations.

In Problem Statement 2, which is the short-term things, we are probably going to address that specifically. How we are going to address that specifically, I don't know. I think it will depend a little on what the industry brings to us in terms of their opinion on what can be done. And lessons learned. Lessons learned to date in that area is not very satisfying from the NRC side. So that very well, as we evolve our work in Problem Statement 2 on short-term usability of the current methodologies, that may be something that we say we can't do much until we solve that so let's find a short-term solution to that particular problem.

I'm getting ahead of myself because I haven't seen what the industry is going to bring to us yet. So I don't know exactly how much work we are going to be doing associated with that.

MR. KURITZKY: Steve, this is Alan Kuritzky again. I think also to get to Jeff's comment, there is a good point, right now the work that we are doing on the traditional methods research is identifying and demonstrating the capabilities and limitations as they are today.

So it is fair to assume that given that we are going to run into that 800-pound gorilla and are going to have to tackle him at some point, that that is something that likely will need to be addressed. So, you know, that is something that we will have to keep in consideration as this work progresses.

At some point we're going to have to say we can only dance around that gorilla for so long. Then we are going to have to dance with him.

MR. ARNDT: Okay. So basically to recap the strategy as we have it now, we are looking at understanding the characteristics of the systems that need to be modeled as articulated in 6901 and the equivalent traditional modeling NUREG, which is the past two output NUREG that Alan just talked about and other issues input from industry and others, identifying the methodologies that could be used, developing an understanding of the data, integrating the information developed from Problem Statements 1 and 2, supporting research and input from external stakeholders, develop the reg guide and send it out.

We were originally planning on doing that this year. Both inputs from our industry counterparts that basically said let's not get ahead of ourselves. I think they were concerned about the fact that we had published more on the dynamic modeling methods than the traditional modeling methods as you heard earlier as well as the priorities associated with the short-term issues, we have pushed those milestones out.

So basically this is just a summary of what I have said. And our intention right now is that the final regulatory guidance will be performance-based. That is to say we are not going to mandate a particular methodology. We may point to a methodology as acceptable but the guidance will be in terms of what are the characteristics of the methodology that is necessary to model the systems.

CHAIR APOSTOLAKIS: Very good. Thank you.

MR. ARNDT: Okay?

CHAIR APOSTOLAKIS: Thank you.

Shall we go around the table again to record first impressions?

MEMBER ABDEL-KHALIK: Well, I guess I'm still stuck on the first step. On the one hand, we have a very well thought out report by the National Academy that said there is not generally applicable effective way to evaluate diversity between two pieces of software performing the same function which implies that whatever backup system you would provide to the operators, whether that is safety related or non-safety related, has to be an analog system.

Now I was told that that is not true. And, therefore, you essentially disagree with the statement made in the National Academy report. And yet you haven't really shown me at least why and how you can support that conclusion. That is my biggest concern.

CHAIR APOSTOLAKIS: Thank you.

MEMBER ABDEL-KHALIK: Thank you.

CHAIR APOSTOLAKIS: Tom?

MEMBER KRESS: Well, I think it is possible to define diversity in terms of non-analog backups. And it would have to do with the various attributes of the diverse systems.

As far as -- you are never going to quantify diverse -- you are never going to say how much diversity is enough, how much is necessary. I think you will just have to use judgment and say if a given system has these characteristics and has followed these procedures and so forth, it is acceptable to us.

You do this all the time anyway in regulatory space. You are not going to be able to do what is implied in the statement that you are going to determine the risk implications of the diversity of the different levels. You are just not going to be able to do that I don't think.

Now I understand that is possibly the intent of some of the research processes you are looking at to actually be able to develop software reliability. But, you know, I think you are going to be a long way off from that.

So I support your approach in saying I want to develop the attributes of diversity and the attributes of defense-in-depth. And use judgement and expert opinion and say these are what I want to see in terms of these attributes.

And if the systems meet these attributes, then they are acceptable to us. So I think that is the only approach you are going to have.

MEMBER ABDEL-KHALIK: Well, I do fully recognize the complications of having both. I mean that doesn't necessarily enhance safety. But yet I'm just trying to resolve this dilemma.

MEMBER KRESS: I think you are going to be likely be in design-based space forever. You put together a deterministic way to evaluate these things with the hope that you render it to a safe level. That's a hope. And it seems to have worked in severe accident space in terms of design basis.

And there's a good -- I think there is a good possibility if you use the right judgments and the insights that you know, that would probably work here. You are never going to be able to validate it and say yes, we know that this system with this diversity and this defense-in-depth has a certain reliability. I'm just doubtful you are ever going to get there.

But I do support the research in that area because I think you learn a lot whether you ever get to that final point or not. You are learning a lot about software systems and how they operate and possible failure modes.

So I think you guys have a good plan. And you are working in the right direction.

CHAIR APOSTOLAKIS: Otto?

MEMBER MAYNARD: Well, first of all on the National Academy of Science Report, I thought it was an outstanding report, a lot of good conclusions and recommendations. I don't necessarily agree that you have to have an analog backup system. I'm not sure that is exactly what they were saying.

If you read their words, they are saying you could not have diversity in the software aspects of it but I think it is up to the NRC to take that report, make their own judgements. If they are not going to do something that is in there, whatever needs to be justified or discussed there, because I think the report also acknowledged that you can certainly make the systems too complex or make it less safe by doing too many things and stuff, too.

So I think it is up to the regulator to

decide what aspects we do. And I think there are some other ways of dealing with that issue that ultimately ends up with a safer and better system.

But I just think that issue needs to be addressed head on and dealt with. Not necessarily say that you have to have an analog backup system because I personally think that would not be the right way to go.

Overall, I'm impressed with the effort. This is the first meeting I have sat in on. The first time I've been here. And overall with the effort to date, a lot of good things are going on. I think overall a reasonable plan on the aspects of it that we have heard here.

I'm glad to see some schedules associated with these things. I was glad to see that included in some of the presentations as to when you are really going to be trying to deliver a product. And so I was appreciative of that.

My concern overall would be with ultimate timing on this whole thing. And both for the industry's input and for the regulator's input. You know this isn't a new issue. It is a new issue for the NRC but it is something that other industries have had to deal with.

I know that we have researched that. My concern is that if we take too long on this that we are going to end up -- things are going to be done by default rather than by actually making decisions up front. And putting the criteria in place.

At some point, we are going to have to recognize that we have reached the point of diminishing returns and decisions are going to have to be made. We know this. We don't know that. Let's admit that. Let's take a look at where we stand overall.

There are consequences for being too conservative. And there are consequences for not being conservative enough. And it is ultimately going to end up with a management decision on some of these things.

We are not going to find a perfect model or a perfect solution that we plug something in and it gives us an answer. It is going to ultimately come down to judgments by people using the best available information that they have. And doing that in a timely manner to support the next generation of plants and what we're doing so that we end up -- what I believe we are going to end up with with safer systems overall.

I have gone through this in the aviation side of things. Of having better, more reliable, safer digital systems available but not legal. And so, you know, what do you use and stuff? And I think that the sooner we could transition into the digital world, we are going to ultimately end up with a safer system.

There may be a slight decrease in risk -- or a slight increase in risk for a short period of time. I don't think that is going to be significant while we are going through our learning process. But it is going to end up with so much better from a risk and a reliability standpoint in the future.

I would like to make just a couple more comments on the simulator because I'm not real sure I understand how that was being proposed to be used in the dynamic modeling there. Simulator is very beneficial for a lot. It is very useful. It is very beneficial for training. It can be used for identifying potential issues in design and evaluation of safety analysis and stuff.

But you really do have to recognize the limitations of the simulator. I can change from an analog to a digital feedwater control system in the plant without ever making a change to my simulator whatsoever. I can do the same thing with the reactor protection system. Therefore, it may not be modeling exactly the digital I&C aspects of things unless your simulator is actually designed and is set up to do this.

So we have to recognize the limitations. I don't discount the simulator. But we also need to recognize the limitations of that, too.

But overall it is a good plan. Again, timing and making some decisions would be the biggest thing. I think that both the industry and the NRC have got to do it and make it happen.

CHAIR APOSTOLAKIS: Sergio? You will send me -- are you there?

DR. GUARRO: Yes, I am.

CHAIR APOSTOLAKIS: Yes, you will send me comments in writing. But would you like to say anything now?

DR. GUARRO: Just one observation on the analog backup question. I think it was a question of you know, how diverse is diverse enough because in reality I think when people say the digital backup would not be acceptable, when those people say that, they think of the fact that the specification process may be effected by the same flaws for the original system and so the backup system will fail by design the same way.

Well, that poses the question wouldn't similar logic specification, for example, being used for the analog, I mean, you know, if you think of a reactor protection system essentially the specification if for a logic that then, you know, you can implement with relays or things of that nature. Or you can implement with digital software.

And so I just want to note that it really is not the black and white of digital versus "analog" because I don't even know if the word analog applies for that particular example, but it is really a degree of gray. In fact, as you probably -- most of you know, we have this devices, you know, in our field-programmable gator rays, are they software or are they hardware, you know? They are something in between, right?

So I just wanted to note that because in considering the question of, you know, how far you have to go in diversity, I think this issue of analog versus digital, quote-unquote, falls in that category.

CHAIR APOSTOLAKIS: Okay. Thank you.

Well, I think I expressed most of my comments during the meeting. And I'll just repeat that I really would like to see more use of the data, the experience, the operating experience.

Maybe as you were talking about simulators, the human reliability group of the agency is planning to have a major benchmark exercise in Halden using their simulator.

You might want to think about whether you might do something similar. Not necessarily the simulator that you mentioned earlier but some collaboration with you simulator and their simulator and see whether you can look at some accident sequence, some initiating events and see what you get out of it since we have this agreement with the Halden people.

Other than that, I think you are on the right path. And overall it sounds good. I think forming this senior group has been very beneficial to the whole effort. And we'll see.

And we have discussed your presentation to the full Committee so we don't need to go back to it.

MR. ARNDT: And we will get back to you later next week --

CHAIR APOSTOLAKIS: Okay.

MR. ARNDT: -- to make sure we are on track.

CHAIR APOSTOLAKIS: And you will send us some documents. Send them to Mr. Hammer and he will make sure everybody gets a copy.

MR. ARNDT: Yes, sir.

CHAIR APOSTOLAKIS: So with that I think we are near the end of the meeting unless there are any more comments from the audience perhaps?

MR. ENZINNA: I'd like to make one comment please. I'm Bob Enzinna. I'm a PRA practitioner at ERIVA. I'm of the school of opinion that we are never going to be able to put a precise probability on the failure of software. But that doesn't mean we can't do things to reduce that probability.

When you are talking about software, there's two parts. There is the application software and there is the operating system. And Steve mentioned earlier, you know, things that can be done and are done to reduce the probability of failure in the application software, you know, V&V and tools for development, functional blocks, things like that.

The other part of it is the operating system. And the important thing about the operating system and the safety-related design is to make sure that the application software failures don't propagate via the operating system to other diverse functions.

And there are the attributes that are mentioned. And the other technical working groups should be telling us what those attributes are. The attributes of the operating system that provide robustness and things we are putting in our safety-related designs like cyclic processing, you know, constant bus loading, static memory allocation, there is a whole list of features like this that prevent an application or a specification error in the software of one function from defeating other functions by taking down the operating system.

And that's what I think we should be looking at is to find those attributes so that we can make the numbers better not necessarily define what they are, the numbers I mean.

CHAIR APOSTOLAKIS: But wouldn't you say though that the question what is the unreliability of a safety function or a safety system with embedded software, that that could be answered? Could be answered at some point in the future without saying that the contribution from the software is such and such?

But I can still talk about the unreliability of the system or the function knowing that because software -- in other words, again, this comes back to the software-centric versus system-centric approach. About the system, I should be able to say something. Or I take your argument to the extreme and say that, you know, the moment you put digital software in the system you cannot quantify, then, of course, I can't have PRAs any more. I can't have anything, risk-informed regulation.

I should be able to say something about the unavailability of these systems and their reliability during the required time, knowing that they are driven by software. So I think that is where the staff is trying to go.

MR. ENZINNA: Yes, I was talking about predictively. I mean we have operating systems in the product we sell. And, you know, this system has, you know, years of experience. You know 62 million hours of operating experience we have on the processor, the product we are selling now.

So we know the operating system. It has never had a common cause failure. It has never had a failure at all in all that time. So we can put a number on that based on operating experience.

The problem is with the application software is that every time you do it it is unique. And so as was said on one of the very first slides, a key thing is the functional diversity. The NAS has said this. You know Steve and Cliff said it. Industry consensus standards, they all come down on the side of, you know, functional diversity is important.

And it is important to make sure that the functionally diverse, you know, functions are actually -- are diverse. And the independent trains are independent. And that's where, you know, these attributes in the design can make sure that, you know, a failure doesn't propagate to other functions.

CHAIR APOSTOLAKIS: And that should lead me to some estimate of the probability. Otherwise, we are going back to the traditional system. The train has left the station already. We have to say something.

MR. ENZINNA: Our approach is to come up, you know, a conservative estimate. And from a sensitivity and uncertainty, you know, perspective.

CHAIR APOSTOLAKIS: You will be happy with a conservative estimate until it causes pain. Then you will come to think the way I think.

(Laughter.)

MR. ENZINNA: Fair enough.

CHAIR APOSTOLAKIS: Thank you very much

for the comment. And I think we have a very useful meeting today. And I appreciate everybody's contributions. And we shall see you gentlemen again in two weeks or something like that.

MEMBER KRESS: Two short weeks.

CHAIR APOSTOLAKIS: Thank you very much.

(Whereupon, the above-entitled meeting was concluded at 4:29 p.m.)