Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards Digital Instrumentation and Control Systems Subcommittee
Docket Number:	(not applicable)
Location:	Rockville, Maryland
Date:	Wednesday, June 15, 2005
Work Order No.:	NRC-461 Pages 1-195

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

DIGITAL INSTRUMENTATION AND

CONTROL SYSTEMS SUBCOMMITTEE

+ + + + +

WEDNESDAY, JUNE 15, 2005

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 1:30 p.m., George E. Apostolakis, Chairman, presiding.

COMMITTEE MEMBERS:

GEORGE E. APOSTOLAKIS, Chairman

MARIO V. BONACA, Member

THOMAS S. KRESS, Member

ACRS STAFF PRESENT:

MICHAEL R. SNODDERLY

ERIC A. THORNSBURY

NRC STAFF PRESENT:

STEVEN A. ARNDT, RES

HOSSEIN HAMZEHEE, RES

TODD HILSMEIER, RES

WILLIAM E. KEMPER, RES

MICHAEL E. WATERMAN, SR., RES

ALSO PRESENT:

TUNC ALDEMIR, Ohio State University

TSONG-LUN CHU, Brookhaven National Laboratory

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

1:31 p.m.

CHAIRMAN APOSTOLAKIS: This is the second day of the meeting of the Advisory Committee on Reactor Safeguards on Digital Instrumentation and Control Systems. I'm George Apostolakis, Chairman of the Subcommittee. Members in attendance are Mario Bonaca and Tom Kress.

The purpose of this meeting is to discuss the NRC staff's draft Digital Systems Research Plan and two specific research programs discussed in the plan: Software Quality Assurance and the Risk Assessment of Digital Systems. The Subcommittee will gather information, analyze relevant issues and facts and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee.

Mike Snodderly is the designated federal official for this meeting and Eric Thornsbury is the cognizant staff engineer.

The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in the Federal Register on May 31, 2005. A transcript of the meeting is being kept and will be made available as stated in the Federal Register notice. It is requested that speakers, first, identify themselves and speak with sufficient clarity and volume, so that they can be readily heard.

We have received no written comments or requests for time to make oral statements from members of the public regarding today's meeting. Now, we will proceed and Mr. William Kemper will start us off.

MR. KEMPER: Yes, as you said, we concluded our discussions yesterday on Software Quality Assurance. Today, we're going to continue on where Steve Arndt left off with his overview of our Digital System Risk Assessment Project. This is a project that has been collaborated with our PRA Branch for the research. Hossein, he is here to speak on behalf of the section. So basically, we're going to give you more details on each of the initiatives associated with that effort.

So, Steve, do you want to make a few comments before we get started?

CHAIRMAN APOSTOLAKIS: So is the first topic development and analysis of digital system failure data?

MR. ARNDT: Yes, I'll explain that in a second.

MR. KEMPER: Yes.

MR. ARNDT: Just to clarify the agenda and to remind you of where we left off last night, I gave a brief overview of the program plan as a whole. The program plan, as you remember, that diagram we had included both analysis and data, evaluation of models, separate programs to look at whether or not it is feasible to do digital system modeling, both from a traditional fault tree of entry aspect as well as using more dynamic methodologies.

So today what we have scheduled is three presentations. The first two will be together. Those will go over the data project as well as the first part of the effort for the traditional fault tree of entry modeling analysis. The third presentation will be from the difference perspective looking at the dynamic modeling methodologies. So without further ado, let me turn it over to our colleagues from the PRAB.

CHAIRMAN APOSTOLAKIS: So all these three presentations are done jointly with a PRA group?

MR. ARNDT: The first two presentations will be led by the PRA group. The third presentation will be led by myself and Professor Aldemir.

CHAIRMAN APOSTOLAKIS: Thank you.

MR. ARNDT: The whole program is a joint

program. We're just leading it.

CHAIRMAN APOSTOLAKIS: Are we ready?

MR. HAMZEHEE: Well, again, my name is Hossein Hamzehee. I am the section chief with the PRA Branch, Office of --

UNIDENTIFIED SPEAKER: This one here?

MR. HAMZEHEE: -- Nuclear Regulatory Research. With me is Todd Hilsmeier. He is the reliability and risk engineer and also we have Louis Chu from Brookhaven National Lab. And all three of us are going to help each other today to go over our effort in the PRA Branch.

CHAIRMAN APOSTOLAKIS: Where are the slides?

MR. HAMZEHEE: I'm sorry?

CHAIRMAN APOSTOLAKIS: Any questions?

CHAIRMAN APOSTOLAKIS: Why are the slides this way, Hossein?

MR. HAMZEHEE: I have no control.

CHAIRMAN APOSTOLAKIS: Okay.

MR. HAMZEHEE: Sorry. The purpose of this presentation is to describe our Digital Systems PRA Project Plan and also provide you with the status of our activities and have some discussions of some of the work that has been completed or is in the progress to be completed. We plan to quickly -- I will try to speak no more than 15 to 20 minutes to provide some background and then the objective of our work and talk about our overall integrated project plan.

And then Todd will talk in more detail about each element will pass in our overall program plan. And then we have Louis Chu here if there are some more detailed questions and status of what will be done and some more technical issues. So I believe all three of us together will provide a reasonable overview of the work that has been going on for some time now.

With that, I am sure you may have already heard that as we speak some nuclear power plants have expressed interest in replacing some of their analog I&C systems with digital. And as you may know, the advance reactors are already using digital or are planning to use digital I&C systems. And we have heard that right now Oconee, Callaway, Wolf Creek and Comanche Peak have shown some interest in operating their RPS system with a digital RPS.

And also, when these utilities submit their studies, then the NRR has to review and provide some technical evaluation and that would require some further research. And for us to provide the risk-informed approach to evaluate these submittals, we need to better understand how to model and quantify the reliability of these digital I&C systems.

And as you may also know, EPRI has completed a document. You may have talked about it earlier today or yesterday, so they are with me if you already know this, that they have provided report entitled "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades." Now, currently, we are working with NRR to do an acceptance review to see if the package as is is adequate for us to review. And if it is, then NRR will usually provide the schedule and perform the review and then give some comments.

CHAIRMAN APOSTOLAKIS: What criteria do you use in your acceptance review?

MR. HAMZEHEE: Well, I need to have NRR to talk about that. Is anybody from NRR here that can help us with that question? Is Matt here? Matt, do you know what that may entitle? Because I am not sure. They usually have some criteria that they make sure that when utility or EPRI provides a technical document, does it have enough information in certain areas, does it provide adequate details so somebody can review and see if it is acceptable. So usually, first, they do that performance and then if they find it adequate, then they do the detailed review. And what the exact criteria are, I'm not sure.

CHAIRMAN APOSTOLAKIS: Okay. Thank you. But ultimately, if the staff reviews this document, there will be an SER?

MR. HAMZEHEE: Correct.

CHAIRMAN APOSTOLAKIS: And then it would come back to us?

MR. HAMZEHEE: Right.

MR. SNODDERLY: We would review the staff's SER.

CHAIRMAN APOSTOLAKIS: Yes, okay.

MR. HAMZEHEE: But usually before we spend time and resources, we want to make sure that that document is acceptable.

CHAIRMAN APOSTOLAKIS: Sure.

MR. HAMZEHEE: For review. And then Todd will talk about we have a task associated with this for two different purposes and we'll talk about it more later on during this presentation.

Now, the objective of our work here is to -- our goal is to develop a probabilistic method for modeling the potential failures of a digital I&C system that can later be integrated with the probabilistic risk assessment using some of the traditional methods, such as long event trees and fault trees. And based on what we have seen so far at our work, it's obvious that currently the digital systems have not been treated uniformly and adequately in the PRAs.

And in some cases when they did do some modeling, they used like black-box approach with some point estimate for failure of probability. And the data and current methods that are available don't seem to be adequate and that's what's driving our work here. Now, we skipped a lot this one, because we talked about this and if need be, we'll come back to this. But let's go back to the next flow chart.

Now, I am going to spend no more than 10 minutes to explain how we put our program and task plan together. And as I said, then Todd will talk about each of those tasks and elements in more detail. For us to have a risk-informed approach, we have to be able to model the digital I&C and PRAs and be able to tell or quantify the reliability of a digital I&C. In order to be able to quantify the reliability of a digital I&C, we have to have models and we have to have data.

So these are the two elements then first we see in our work. We have to see if they are available, fine. If not, then we need to develop them. As we looked at the digital I&C, then we realized that they are different from other mechanical systems or other mod systems that we model and evaluate in PRAs, in the sense that they are hardware and software, and each has different characteristics.

Right now, we need to have models and data to hardware and software and then when we put the program plan together, if we look at the two blocks on the right and left and ignore anything to the top and bottom, for the time being, then you see that we broke our work, broke it down into two parts. On the left side, you see the hardware block that we have and the task plan the numbers represent the task in our task plan.

The first block is block number 5. If I can read it from here. And that is to gather and evaluate the reliability data. This is one of our tasks. And once we gather and evaluate data, hopefully, at some point, we feel like we have adequate data. Then we have to go back and see what kind of models and methods are available.

If there isn't sufficient methods, then we're going to develop and evaluate appropriate methods, such as George's favorite model, Markov, or others, fault trees or some others that can be adequate. We will use them and then at the end of this task, we will be able to at least recommend what method is appropriate for digital I&C.

CHAIRMAN APOSTOLAKIS: But why is Box 5 --

MR. HAMZEHEE: Yes, the first box --

CHAIRMAN APOSTOLAKIS: -- gathering an analysis of reliability data? Can you use the cursor to point to the box?

MR. HAMZEHEE: Yes.

CHAIRMAN APOSTOLAKIS: The cursor, the cursor.

MR. HAMZEHEE: The cursor?

CHAIRMAN APOSTOLAKIS: Yes, you can do that. Yes, that's the one. That's the one. That's the one. Why is that under hardware? I mean, do we-- don't you need data on the software failures?

MR. HAMZEHEE: Yes.

CHAIRMAN APOSTOLAKIS: It should be a common box feeding into both.

MR. HAMZEHEE: Correct. Now, what we're seeing is when it comes to data, we need two types of data. One is for hardware, one is for software.

CHAIRMAN APOSTOLAKIS: But that's not what the figure says.

MR. HAMZEHEE: But it does. If you look at the right block, the counterpart of that block on the right says software on the top and then it has a similar block.

CHAIRMAN APOSTOLAKIS: No, it doesn't.

MR. HAMZEHEE: If you want to look at the one that Todd has pointed to.

CHAIRMAN APOSTOLAKIS: No, it says develop software failure probabilities.

MR. HAMZEHEE: Yes, that is common.

CHAIRMAN APOSTOLAKIS: The Box 5, it seems to me, should be in the middle feeding both hardware and software. That's what you told us and that's what it is. It's just misplaced there.

MR. HAMZEHEE: Let me go over it and then when we talk about the detail, you'll see how they fall into the -- it doesn't matter how we put it here. But the reason we put it here is because we want to make sure if there are some more availability or products in one area, that doesn't impact the other one.

CHAIRMAN APOSTOLAKIS: It seems to me --

MR. HAMZEHEE: But technically it doesn't matter where you put those boxes.

CHAIRMAN APOSTOLAKIS: As long as you do it right, yes.

MR. HAMZEHEE: Yes.

CHAIRMAN APOSTOLAKIS: But the point is that we can't really claim that we understand the failure modes of software.

MR. HAMZEHEE: That's correct.

CHAIRMAN APOSTOLAKIS: So you know, collecting as much data as we can is probably a good idea.

MR. HAMZEHEE: Yes.

CHAIRMAN APOSTOLAKIS: Yes.

MR. HAMZEHEE: And that is what the Block 8. Would you put the cursor on Block 8? If you put the cursor on Block 8, the one running parallel is we're going to look at the hardware failure data, evaluate, analyze, gather and do the same thing for software. So technically, we're doing what you're saying, but we simply need to do hardware and software.

CHAIRMAN APOSTOLAKIS: Anyway, I suggest that Box 5 be moved to the middle. That's all.

MR. HAMZEHEE: All right.

CHAIRMAN APOSTOLAKIS: And that is the same way you are blocking for with two arrows? One leading to hardware and one to software, that's all.

MR. HAMZEHEE: That's right. That can be done, too.

CHAIRMAN APOSTOLAKIS: But will it?

MR. HAMZEHEE: Yes.

CHAIRMAN APOSTOLAKIS: It's a big deal. It's not a big deal, Hossein.

MR. HAMZEHEE: Yes, we'll do that if it's not a big deal. And then Block 6 is looking at the modeling techniques and what methods to apply. And then the next block, Block 7 is then to combine the two and try to quantify the reliability of the hardware. Now, again, you may say why do this separately? As we make progress, we may find out that we can combine them in the earlier stage. So this is just for presentation purposes, not done logically. It has to be separated.

And then if you move to the right drop under software, the Block A talks about developing, analyzing data for software. And then try to develop some methods for modeling the software. And then at the end, Block 9 is the software model quantification. And then you provide these two in a proper logical manner. Then you do the overall digital system reliability quantification.

CHAIRMAN APOSTOLAKIS: Now, hardware model quantification. You mean the hardware of the computer, not the pumps of it?

MR. HAMZEHEE: Of the RPS digital system. Of the digital system.

CHAIRMAN APOSTOLAKIS: The digital system?

MR. HAMZEHEE: Yes. Not the pumps.

CHAIRMAN APOSTOLAKIS: Oh, is it --

MR. HAMZEHEE: Not the --

CHAIRMAN APOSTOLAKIS: Is this only for RPS protection?

MR. HAMZEHEE: Well, as an example, it's for RPS, but you can have the --

CHAIRMAN APOSTOLAKIS: Yes, so it's --

MR. HAMZEHEE: -- control for monitor. The digital I&C systems utilities plan to operate to.

CHAIRMAN APOSTOLAKIS: Because they are the ones saying that is again box number 9 may be mislabeled, in the sense that there is a school of thought that says you will not have a software model quantification, because you are amending the software in the box system.

MR. HAMZEHEE: That's why I said we don't know right now how logically the boxes are connected.

CHAIRMAN APOSTOLAKIS: Yes.

MR. HAMZEHEE: But that's a good point though. You are right. So data Block 10, we try to, if it makes sense, combine it and come up with the overall system reliability quantification. And then Block 11 will make an attempt to integrate it with the PRA, so that we can come up with the risk contribution and risk assessment of a digital system with respect to planned risk, such as CDF and other risk matrix.

And then finally, our goal is at some point in time, and Todd will talk about schedule, we'll try to document all these things in the NUREG report. Now, let's go --

CHAIRMAN APOSTOLAKIS: I would expect -- I mean, this is a big task. I would expect that you will publish reports before NUREG.

MR. HAMZEHEE: I'm sorry?

CHAIRMAN APOSTOLAKIS: Wouldn't you be publishing reports say after you finish the data evaluation?

MR. HAMZEHEE: Probably not --

CHAIRMAN APOSTOLAKIS: Really?

MR. HAMZEHEE: -- public report. But we may have some intermediate technical reports, yes.

CHAIRMAN APOSTOLAKIS: Hum.

MR. HAMZEHEE: But at the end, we want to put them all into a NUREG report.

CHAIRMAN APOSTOLAKIS: But wouldn't you like to have some comments from the public on your data collection and conclusions that you draw from it? I mean, why do you want to have to wait until the very end?

MR. HAMZEHEE: That can be -- that's an option, yes.

CHAIRMAN APOSTOLAKIS: That's a good idea, I think.

MR. HAMZEHEE: Bill?

MR. KEMPER: This is Bill Kemper. We do have plans to convene a public meeting, at some point. We're not exactly sure exactly where perhaps we're going to do it. But we do intend to engage the public.

CHAIRMAN APOSTOLAKIS: Okay.

MR. KEMPER: We just have reason for it.

CHAIRMAN APOSTOLAKIS: Okay.

MR. HAMZEHEE: But hopefully before it becomes a NUREG report it has to go through public review and comment, more interactions with ACRS and others, before we can call it a NUREG report. And so now let's go back to the top of the block. If you look at Block 1, when we started this project it was about a year ago and again Todd will talk about it, but quickly, there was a draft EPRI report and we wanted to review that and gain some insight to see if that can help us with the work we are doing. So that was the purpose of that Block 1.

And then Todd, he will tell you where we are and the documentation that we have. And then Block 2, we also wanted to make sure we don't reinvent the wheel. So we went ahead and tried under that task to look at available data from other agencies, such as NASA, find out what else is going on, who has done what and then use them as applicable. So that was the purpose of Block 2, and then Todd again will tell you where we are and what we have done with those two.

And Block 3 is basically trying to figure out then how we would put all these things into a report. And now go back down to the -- all the way to the right. And those are again sensitive research. We try to envision what else can happen or the work that we may have to do. We haven't planned for the last block that says future activities yet in our current plan, but we have defined some potentials. So as the interest and the need arises and if the budget allows, then what we want to do is the first one is to support NRR when they do review the EPRI report.

And that actually when we put this block together was a year ago, and we were not sure if that was going to happen, but today when we're talking about it, it did happen. So most likely that future work is going to happen earlier. And then below it is once this work is complete, then we like to provide some guidance, because most likely even if we come up with one or two methods once the licensees start operating their systems to digital, they are going to come up with other methods.

So we want to be able to provide some guidance on acceptable methods, so that others can apply those guidance and develop their own models.

CHAIRMAN APOSTOLAKIS: So what is the time frame of all of this?

MR. HAMZEHEE: Todd is going to tell you. He is going to go over all of them. And then the last one is again as time goes on and we get more real applications from licensees, we're going to learn more and as we learn more, we may come up with new methods and applications. And that's again in the future activities. Now, this is all I'm going to say. If there aren't any questions, I'm going to turn it to Todd. If you have any questions?

MR. HILSMEIER: Am I registering okay? My name is Todd Hilsmeier from research and I work in the PRA Department. And a little background on myself. I've spent 6 years in consulting business doing PRA and then 6 years at plants Salem, Hope Creek, Diablo Canyon working in PRA. Then I joined NRC last September and the first project was the Digital Systems PRA Project.

And I'm going to continue where Hossein left off at. And the first task that we are working on is Task 1, which is review of the EPRI 1002835 report. And the purpose of reviewing this report is to obtain insights on the reliability methods for modeling digital systems. Our focus was not revealing the report for review and approval by NRC, but to gain insights on how we can use the report to develop reliability models.

And some observations that we observed from the reports is that the EPRI Technical report advocates risk-informing digital I&C systems by proposing the use of a simplified and a standard risk-informed method as it turns to current deterministic methods. And also we observed that the simplified risk-informed method should be clarified and demonstrated with examples.

I should note that we reviewed an earlier version of EPRI guide, it's final version, the current version does provide examples of a simplified method. And so this statement is no longer up to date. The simplified risk-informed method may not necessarily provide conservative risk values. And also the EPRI Technical report does not provide information on how to develop models needed for standard risk-informed traditional PRA methods.

However, the EPRI report does provide some characteristics to consider in reliability model development. The current schedule for Task 1 is the research division reviewed comments on our draft report and the final report for Task 1 will be completed June 30th.

CHAIRMAN APOSTOLAKIS: So I don't understand that. I mean, Hossein just told us that you are in the process of deciding whether to review it. This is a research review, not NRR review.

MR. HILSMEIER: But in itself --

MR. HAMZEHEE: There are two parts. There are two reasons we are looking at this EPRI report. One is to gain insight as Todd said to help us with our work to see if they've done some good work that we can benefit from. The other one is to support NRR in their review. So I think Todd is talking about the first purpose of that review. Am I right, Todd?

MR. HILSMEIER: Yes, that's correct. The review of the EPRI report for approval by NRC is a future task. The primary purpose of our review is just to gain insight on the report.

CHAIRMAN APOSTOLAKIS: This review was done within the Agency?

MR. HILSMEIER: Excuse me?

CHAIRMAN APOSTOLAKIS: Was it done in-house, the review?

MR. HILSMEIER: Yes, by myself and Brookhaven National Laboratory, Louis Chu.

CHAIRMAN APOSTOLAKIS: Okay.

MR. HAMZEHEE: I think just for clarity, most of our work is in-house with some help from BNL, in our area.

MR. HILSMEIER: And we reviewed the EPRI report before we had the final version. In Task 2, the purpose of Task 2 is review industry experience per methods and databases, failure databases of digital hardware/software use to model digital systems. The basic approach was to establish contacts with industry, such as NASA, Army, Navy, Air Force, DOE, DoD, the Defense Nuclear Facility Safety Board, FAA, automotive industry and then several contractors, OMNICON, RAC and Idaho National Laboratory, that's to name a few.

The second step in the approach is to search and collect guidance on the reports and then review the reports. And what we observed from industry is that most of industry managed digital system risk through a qualitative approach, which involves software development process, management, testing the software, documentation, QV&V of the software. And we found very little of industry that forms quantitative risk analyses.

I think there are some small isolated cases of quantitative risk analyses and digital systems, such as Idaho National Laboratory performed some digital reliability work for the Army and it's all classified and proprietary, so we weren't able to analyze the results. Also, OMNICON did similar work for the Navy.

I'll be talking about the Idaho National Laboratory Failure Rate Database under Task 5. However, we also observed that NASA is moving to a quantitative risk evaluation approach using PRAs. We looked at the NASA Fault Tree Handbook and the NASA Peer Review Procedure Guide, that was developed by experts with extensive nuclear power plant PRA experience. Task 2 is currently being worked on and the final report will be completed by August 30, 2005. Any questions on Task 2?

Task 3, we don't have a slide for, it's simply documentation of all the work that we do in creating an outline. We document as we go and one document at the end. We want to make sure we stay up, make sure we document all our thoughts and not miss any information.

Task 4 is developing supporting analysis for the Digital System Reliability Project and basically involves obtaining information about the behavior of the digital system, such as developing FMEA, failure modes and effects analysis and dependency analysis for the system. And the FMEA dependency analysis is a foundation of reliability model. And we also want to develop guidance on how communication and voting should be modeled.

These supporting analyses will support the development of the Digital Systems Reliability Model. We need to apply the supporting analyses to a case example. And our case example will be the Digital Reactor Protection System proposed for Oconee. For reactor trip demand using the Teleperm platform, the expected period of performance is expected to start in

July of 2005, next month, and we expect to complete it in September 2006. Any questions?

CHAIRMAN APOSTOLAKIS: Don't worry, there are -- there will be.

MR. HILSMEIER: Okay. No questions. Hossein questions me all the time.

CHAIRMAN APOSTOLAKIS: Do you feel you have been treated unfairly?

MR. HILSMEIER: No, no.

CHAIRMAN APOSTOLAKIS: Okay. I understand. Maybe you are doing a better job.

MR. HILSMEIER: I love this job in consulting and working at the power plants.

CHAIRMAN APOSTOLAKIS: Okay. How much are you going to tell us about the data now?

MR. HILSMEIER: I was going to skip this task. I know this is your favorite task. Task 5 is development of the failure database for digital hardware. And for the analysis, our approach for developing the database was reviewing failure rate databases.

These databases were Military Handbook Telcordia and PRISM. And I'll talk about this approach in the next slide. It also serves industry for additional digital failure data. Industry such as

LERs and EPIX from nuclear power plants, also NASA, the SPAR model and FAA. And then last, under approach is development of a population variability distribution using the proprietary PRISM failure records.

CHAIRMAN APOSTOLAKIS: What's PRISM again? What's PRISM?

MR. HILSMEIER: It's a software package developed by Reliability Analysis Center used to predict failure rates.

CHAIRMAN APOSTOLAKIS: Who is Reliability Analysis Center, is that the NASA people?

MR. HILSMEIER: It's a consulting company.

CHAIRMAN APOSTOLAKIS: Huh?

MR. HILSMEIER: It's --

DR. CHU: They work with the defense industry a lot. It's like consulting.

CHAIRMAN APOSTOLAKIS: It's consultants?

DR. CHU: Yes.

MR. HAMZEHEE: It's proprietary.

CHAIRMAN APOSTOLAKIS: Huh?

MR. HAMZEHEE: It's proprietary though, it's not available.

CHAIRMAN APOSTOLAKIS: So prohibited. Do you have access to it?

MR. HAMZEHEE: We have purchased it and yes, we do have access to it.

CHAIRMAN APOSTOLAKIS: Oh, okay.

DR. CHU: Yes, we are not supposed to tabulate all the failure rates found at database.

CHAIRMAN APOSTOLAKIS: Is it a failure rate database or is it failure modes? Are you using it in any other way?

DR. CHU: They have raw data in the form of failures in this number of hours.

CHAIRMAN APOSTOLAKIS: For software?

DR. CHU: For hardware.

CHAIRMAN APOSTOLAKIS: Okay. Anybody can do that.

DR. CHU: That actually is the only thing that we were able to find that kind of data, raw data.

CHAIRMAN APOSTOLAKIS: For what?

DR. CHU: Digital hardware.

CHAIRMAN APOSTOLAKIS: Digital hardware? Well, I mean, if you rely on this a lot, maybe we ought to look at it. There are mechanisms still handling proprietary information. Yes.

MR. KEMPER: Did -- you say we purchased it, right? So we --

MR. HAMZEHEE: Yes, for our own use to

include in ACRS we can look at it.

CHAIRMAN APOSTOLAKIS: Yes.

MR. HAMZEHEE: Oh, yes.

CHAIRMAN APOSTOLAKIS: Definitely, we are part of the Agency.

MR. HAMZEHEE: Sure. As long as you agree with us.

CHAIRMAN APOSTOLAKIS: As long as what?

MR. HAMZEHEE: You agree with us.

MR. HILSMEIER: Task 5 continued. The first bullet was reviewing the failure rates databases and Military Handbook, Telcordia and PRISM, that's what I'm going to discuss next. The analysis of these three sources Military Handbook and Telcordia will be documents and PRISM is the software program. They use empirical formulas to predict failure rates.

CHAIRMAN APOSTOLAKIS: Can you tell us what that means?

MR. HILSMEIER: Yes, basically, they take a base failure rate and apply pi shaping factors.

CHAIRMAN APOSTOLAKIS: Oh.

MR. HILSMEIER: To adjust failure rates for quality.

CHAIRMAN APOSTOLAKIS: The basic failure rate comes from standard methods, though?

MR. HILSMEIER: Yes.

CHAIRMAN APOSTOLAKIS: Bayesian or what, maximum likelihood?

DR. CHU: They didn't provide the detail of how they estimate.

CHAIRMAN APOSTOLAKIS: You know why? They don't have an advisory committee to review those. You guys wouldn't do that.

MR. HILSMEIER: That's why we didn't use the data. I mean, the empirical formulas.

CHAIRMAN APOSTOLAKIS: See, the problem with these things is they do it and then, you know, people say oh, gee, this is DoD or NASA or whatever. They have been doing it, so it must be right. Well, no, it's not right.

MR. HAMZEHEE: I think we came to this same conclusion. And I think he is going to tell you the problems that we have found.

CHAIRMAN APOSTOLAKIS: And I agree with him, yes.

MR. HAMZEHEE: Okay.

MR. HILSMEIER: The empirical formulas work well when, in limited cases, the data is applicable and sufficient. But in that case, one can just use the data explicitly calculated by failure rates.

CHAIRMAN APOSTOLAKIS: So a broken clock is right twice a day.

MR. HILSMEIER: Exactly.

CHAIRMAN APOSTOLAKIS: Yes.

MR. HILSMEIER: So the other concern we had with these three sources was the lack of uncertainty consideration. And is it correct they didn't provide any uncertainty, the empirical formulas don't provide uncertainty?

DR. CHU: Right. One situation I asked why don't you consider uncertainty? And the answer I got was there are so many sources of uncertainty, you can't handle it.

CHAIRMAN APOSTOLAKIS: Well, that's a good reason. And besides why get an uncertainty about the wrong point estimate anyway.

MR. HILSMEIER: So we didn't use these sources, the empirical formulas. We also reviewed industry experience failure databases. The existing PRA failure databases touch as far as NASA, PRA guide, IEEE, did not contain digital component failure rates. The advanced reactor PRAs may contain limited additional failure rate data, which is proprietary.

CHAIRMAN APOSTOLAKIS: If you can get

those.

MR. HILSMEIER: Yes, and we plan to evaluate this further under the second phase of data analysis.

CHAIRMAN APOSTOLAKIS: Now, that was another thought. Is that not what is this kind of data? Is that true, Louis?

DR. CHU: I'm sorry?

CHAIRMAN APOSTOLAKIS: Nobody has that kind of data. You are going through this, because you have to. Do you really think there is somebody out there that has a databank that has well-documented failure rates for software components or hardware?

DR. CHU: I tend to think the manufacturers do have.

CHAIRMAN APOSTOLAKIS: Yes, they will tell you FFA has.

DR. CHU: Actually, some -- most of the data in the PRISM software came from some manufacturer. The name they don't tell us.

CHAIRMAN APOSTOLAKIS: Of course they don't tell you, because if you go and look, you will reject it like they rejected PRISM.

MR. HAMZEHEE: But I think, George, I mean, we have to start from somewhere.

CHAIRMAN APOSTOLAKIS: No, I'm not saying we shouldn't do it.

MR. HAMZEHEE: And this database --

CHAIRMAN APOSTOLAKIS: But I'm just telling you that we know the answer.

MR. HAMZEHEE: Yes, but I think from manufacturers you get some reasonable data, because you have numerator and denominator, even though you may not have high confidence, but it's a good start. And as these systems are installed and we get more operating experience, then we update the information. That's really one way to go I think. The only way you can really get some numbers and do some quantification.

CHAIRMAN APOSTOLAKIS: Well, I repeat it's not the numbers that worry me, it's the actual failure modes. I don't think we really understand those.

MR. HILSMEIER: All right. We also evaluate industry operating experience, such as the nuclear power plant LERs, double event reports and EPIX data, FAA, Army, the Department of Energy, and they contain digital failures, but the reports are not detailed enough. They don't describe what digital component failed. As Steve mentioned yesterday, the reports don't say -- specify in the meantime between failures and specify additional systems that are deployed that have not failed.

So there is a lot of information just from these databases to calculate, to estimate a failure rate. But we will evaluate some of these databases further in the second phase of data analysis. Because there is a second phase I'm kind of hinting at our conclusion.

MR. HAMZEHEE: And I also would like to add, George, that we will welcome any insights you have. If you have some information that we can use, this is a good time. So we are also asking you to help us if you have some additional information in some of your other work or involvement.

CHAIRMAN APOSTOLAKIS: I mean, even in my additional comments, didn't I have a citation, which is admittedly old, but was -- somebody at NASA had collected information, actual data. What does that mean, Louis? You didn't read the comments or you checked the reference and it's not useful?

DR. CHU: I think I didn't read the comment carefully.

CHAIRMAN APOSTOLAKIS: Thank you very much. You come here.

MR. HILSMEIER: I didn't hear the

question. I'm sorry.

CHAIRMAN APOSTOLAKIS: Well, there is -- all I know is in that paper by Garrett and me and also in the added comments. I don't have any thing additional. Do you have the paper by Garrett, Chris Garrett and me? That's all I got.

MR. HILSMEIER: All right.

CHAIRMAN APOSTOLAKIS: But I'm surprised I don't see any of that here, because they have individuals, not organizations, individuals have collected information occasionally.

MR. HILSMEIER: And we also reviewed a NASA failure database. I mean we didn't review it. We tried getting the NASA failure database and this is through Dr. Dezfouli.

CHAIRMAN APOSTOLAKIS: Who would have it at NASA?

MR. HAMZEHEE: Normally, that would be read from ISO and Bill Vesely and those guys can help.

CHAIRMAN APOSTOLAKIS: All right. Keep going.

MR. HILSMEIER: All right. Thank you. Right. Dr. Dezfouli was saying that --

CHAIRMAN APOSTOLAKIS: They are looking for it just as you are.

MR. HILSMEIER: The data will be available for publishing in 2006. However, there is a Conference Spec 2000 between NRC and NASA to establish a cooperative, I'm not sure of the correct words, but, agreement to work on the Digital System Reliability and for the second phase of data analysis, we're going to try to get the proprietary data. If not, then use the public available data. And another question is will the data have sufficient detail.

CHAIRMAN APOSTOLAKIS: It is an IEEE or some other publication on computers, which seems to publish periodically an evaluation of major failures? I don't remember what the title is. Are you familiar with it, Steve? I'm not sure it's IEEE. It's some other organization.

MR. ARNDT: It's not IEEE.

CHAIRMAN APOSTOLAKIS: Computers.

MR. ARNDT: It's one of the computer societies.

CHAIRMAN APOSTOLAKIS: Yes, yes. And again, they don't go out of their way to collect data.

MR. ARNDT: Yes, it's not --

CHAIRMAN APOSTOLAKIS: But they take a few cases of created ways and they analyze it. So you may have to do some of that. I mean, you're not going to find the database anywhere I don't think. But you may create a database by picking some of these. And as I say, that paper by Chris Garrett has some information. But it's already a little old. But if you see the name of the journal, then you go to more recent issues and see whether they have more.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Again, don't expect them to solve your problems.

MR. HAMZEHEE: Again, we're trying to do our best to see what is available, make sure we're not missing anything. And then at the end we have to use what is available with some uncertainty and, you know, again, we got to start from somewhere in order to quantify some reliability. So even if we don't have the amount of data we need, we can still do some quantification with some uncertainty there.

This is exactly the problem we had 30 years ago when we started doing PRAs. We didn't have data for every single component for every equipment in the plant, but then there was high uncertainty associated with those. So I think it's a good start and hopefully as utilities --

CHAIRMAN APOSTOLAKIS: I'm not questioning why you're doing it. I'm just trying to help. I think you have to do this as long as you have the right amount of skepticism.

MR. HAMZEHEE: Yes.

MR. HILSMEIER: We also plan to look at the COMPSIS data, which is international effort to collect I&C operating experience. And it's still in the early stage of data collection.

CHAIRMAN APOSTOLAKIS: They started in 1999.

DR. CHU: Yes, I read that.

CHAIRMAN APOSTOLAKIS: Huh? Have they collected anything in the six years?

DR. CHU: That is a fairly -- they started collecting.

CHAIRMAN APOSTOLAKIS: Yes, I mean, that--

DR. CHU: Steve Watson can tell you.

CHAIRMAN APOSTOLAKIS: Steve who?

DR. CHU: Steve.

CHAIRMAN APOSTOLAKIS: So what do you have?

MR. HAMZEHEE: You need to speak in the microphone and introduce yourself, otherwise that lady is going to get mad.

CHAIRMAN APOSTOLAKIS: And we don't want that to happen.

MR. HAMZEHEE: No.

MR. ARNDT: The COMPSIS database is an international OECD effort along the same lines as the IEPD and things like that to collect data from various international or national databases and agencies that get data as part of their regulatory responsibilities like our LER database.

CHAIRMAN APOSTOLAKIS: But have you connected them?

MR. ARNDT: What we did was we started a trial project in '99 to try and figure out whether or not this was practical. We collected a small sample of data to help us write the Coding Guidelines and what information you need and things like that. We got about 100 data points. Not over the useful, but interesting. As of this year, we are starting to collect full scale with all the signature countries required to submit all their latest data.

CHAIRMAN APOSTOLAKIS: That's all nuclear?

MR. ARNDT: This is all nuclear.

CHAIRMAN APOSTOLAKIS: If you have 100, I mean, I was hoping to see one or two or three examples and I don't see any. You know, you guys don't want to educate us?

MR. HAMZEHEE: I'm sorry, I was asking a

question.

CHAIRMAN APOSTOLAKIS: I'm asking Steve. Louis, do you have any examples you can give us?

DR. CHU: Well, we -- all we have done is using the data from the PRISM software and we used the hierarchial Bayesian analysis to come up with a failure rate.

CHAIRMAN APOSTOLAKIS: Are you going to talk about any of that?

DR. CHU: Yes, I will.

MR. HAMZEHEE: Yes.

CHAIRMAN APOSTOLAKIS: Oh, you mentioned that you have done it, but you're not talking about it.

MR. HAMZEHEE: Well, we did. If you would like --

CHAIRMAN APOSTOLAKIS: You said we did. But, you know, this is a subcommittee. Subcommittees, we generally are going to do that.

DR. CHU: Page 14 and 15.

CHAIRMAN APOSTOLAKIS: Yes.

DR. CHU: Talks about that.

CHAIRMAN APOSTOLAKIS: It says we did it, at least. It doesn't say how you did it. This is a Subcommittee meeting. In Subcommittee meetings we want to know the how. Okay. Todd, you want to tell us, Todd?

MR. HILSMEIER: How we got the failure rates?

CHAIRMAN APOSTOLAKIS: Well, I was hoping to see, you know, several examples of say here is the means and then here our role of 2001 and here is why it's interesting. You know, that kind of thing.

MR. HILSMEIER: Right.

CHAIRMAN APOSTOLAKIS: Maybe in a future meeting we can do this, huh?

MR. HILSMEIER: Yes.

MR. KEMPER: If I could offer just back on Tom's question, if nothing else, if all else fails, we intend to use COMPSIS precisely for that purpose.

CHAIRMAN APOSTOLAKIS: Absolutely.

MR. KEMPER: We are paying into it, you know. There is a fee every year and there is about, I forget, eight or 11 countries, I think, have --

CHAIRMAN APOSTOLAKIS: Well, he says you have 100 points, I mean.

MR. KEMPER: In countries.

CHAIRMAN APOSTOLAKIS: That's great.

MR. KEMPER: And we'll start collecting data pretty soon and George Tartal is our representative to that committee.

CHAIRMAN APOSTOLAKIS: Yes.

MR. KEMPER: And he'll go there twice a year represent.

CHAIRMAN APOSTOLAKIS: Where are there, Paris?

MR. KEMPER: Sometimes it will be, sure.

CHAIRMAN APOSTOLAKIS: At one time you go to London, is that what you're saying?

MR. KEMPER: It could be.

CHAIRMAN APOSTOLAKIS: Marseilles.

MR. KEMPER: Right. But that's the idea. We will each agree the incidents occurred in our countries.

DR. BONACA: What about Huntsville?

CHAIRMAN APOSTOLAKIS: Huntsville, Alabama?

MR. KEMPER: But at any rate --

CHAIRMAN APOSTOLAKIS: Anyway, as an action item for the future, we need to spend some serious time looking at what kind of data is available to us, what we learn from it, how we learn, don't just give me Latin names with a hierarchial base.

MR. HAMZEHEE: You know, George, for this meeting we were planning mainly to spend no more than an hour to go over our program plan and to some detail of some of these tasks, but if you like, we can then meet with you again to spend a few hours on each of these tasks.

CHAIRMAN APOSTOLAKIS: I think we should do that.

MR. HAMZEHEE: And get more technical.

CHAIRMAN APOSTOLAKIS: I think this is going to be one of the major issues that the Agency will be facing in the next several years.

MR. HAMZEHEE: Sure.

CHAIRMAN APOSTOLAKIS: And we ought to be on top of it.

MR. ARNDT: We can, as part of our ongoing interaction, highlight a couple of main particular tasks in the various programs. This one for this program and go into a much greater level of detail. We will work through Eric and try and figure out the level of detail you're interested in and work that out.

CHAIRMAN APOSTOLAKIS: I'm a little overwhelmed by this. I mean, are we going to review the individual projects of some going on past judgment? I mean, this is down the road. You or the program with some detail here as well, but --

MR. HAMZEHEE: We were not planning to have a detailed time review. But if you are interested, we can send you some of our preliminary documents, reports and get some feedback from you.

CHAIRMAN APOSTOLAKIS: In what form?

MR. HAMZEHEE: Some like internal documents that are, you know, formal documents.

CHAIRMAN APOSTOLAKIS: Feedback though has to be formal.

MR. HAMZEHEE: Right.

CHAIRMAN APOSTOLAKIS: The feedback has to be a letter from the Committee.

MR. ARNDT: What is probably the easiest way to do it is to schedule meetings at decision points. We have looked at the data and we think we can't do much or we need to do more or whatever and then present those kind of things.

CHAIRMAN APOSTOLAKIS: Yes. Maybe that's a good point.

MR. ARNDT: We did an evaluation of this and we chose these two models to pursue or things like that.

CHAIRMAN APOSTOLAKIS: No, I agree with you, Steve. I think that makes perfect sense. But let me bring another factor into this. This reminds me of the days when we were struggling with how to formulate the frame work for risk-informed regulatory decision-making. That ended up being Regulatory Guide 1.174.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: And in the sense that here, just as then, the way to proceed forward is not obvious. I mean, we are really looking for ways of doing it and how to do it.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: I mean, now everybody says 1.174, you know, as if it's the most natural thing in the world. But I know people have to agonize over it, you know. And the ACRS got involved early in the process and we had what some people call participatory review, instead of waiting until the end.

So the staff will come to us and say well, gee, we're thinking of doing this or that. What do you guys think? And we will, you know, say well, you know, this makes sense, this doesn't make sense. If you feel that that kind of participation will be beneficial to you, I would rather go that way than wait until you have a draft NUREG and then have the Committee say we don't like it, so that doesn't come as well.

MR. ARNDT: Yes. And I agree. I think for some of these tasks, particularly this one and some of the others, we will investigate something and we'll think we have a direction and that's what I mean by a decision.

CHAIRMAN APOSTOLAKIS: Okay. So I would like to have this being one of the areas where we can do that. After you guys have thought about it and say well, we're going to follow this route, maybe we can have a meeting and get whatever reason you can get from us.

MR. ARNDT: Yes, okay.

CHAIRMAN APOSTOLAKIS: Do the Members agree?

DR. KRESS: I think it's great.

CHAIRMAN APOSTOLAKIS: I'm not running this, you know. Well, actually, if they disagree with that, I would have heard it all, so, but it was just a courtesy. No, but I really think this is the best way to proceed, because this is a very difficult subject.

DR. KRESS: Usually we do this with the full Committee.

CHAIRMAN APOSTOLAKIS: Yes.

DR. KRESS: On 1.174 rather than just two or three Members.

CHAIRMAN APOSTOLAKIS: Well, yes, yes. In this case, probably the Subcommittee, I think.

DR. KRESS: We might want to combine some Subcommittees.

CHAIRMAN APOSTOLAKIS: The Subcommittee probably will have a meeting or two and then go to the full Committee for a letter. I would rather communicate with the staff than using letters.

DR. KRESS: Oh, yes.

CHAIRMAN APOSTOLAKIS: My understanding is that the ACRS Staff doesn't like us to give you informal comments. I mean, we give you comments here, but not in writing.

MR. HAMZEHEE: We can give you status at-- more often, but for that, then it can't be as frequent, because it takes a lot of your resources to prepare letters.

CHAIRMAN APOSTOLAKIS: No, I'm not saying every week.

MR. HAMZEHEE: No, no.

CHAIRMAN APOSTOLAKIS: I don't want to see you every week.

MR. ARNDT: The feeling is mutual.

CHAIRMAN APOSTOLAKIS: Louis, I would really like to know a little more about it though. Can you tell us anything? I mean, you know that, you know, A, B, C, D means nothing. Is there any detail you can give us now or is it pretty much over?

MR. HILSMEIER: I can give --

CHAIRMAN APOSTOLAKIS: Yes, go ahead, Todd.

MR. HILSMEIER: I can give you some numerical guidance.

CHAIRMAN APOSTOLAKIS: Yes, no, I don't need all the numbers.

MR. HILSMEIER: Okay. Because this process, this task is still ongoing, that's -- and we're counting time.

CHAIRMAN APOSTOLAKIS: Do you remember of a failure mode that was kind of unusual and is worth mention?

DR. CHU: Right now, we are looking at the hardware failure part.

CHAIRMAN APOSTOLAKIS: Yes.

DR. CHU: We don't have detailed description of any failures. What we have is, as I indicated earlier, we have from one source of data for this particular component. We observe high failures in hours, that's all.

CHAIRMAN APOSTOLAKIS: That's all?

DR. CHU: Failure may represent, you know, products that get returned to the manufacturer and manufacturer return to analyze yes, it fail or identify specific cause of failures. But we don't have that information. All we know is this failure --

CHAIRMAN APOSTOLAKIS: You mentioned two events yesterday, one of Turkey Point and the other Davis-Besse. So at least you have those and you may have more than --

DR. CHU: Yes, Turkey Point. Okay. In terms of nuclear experience, Turkey Point is one that we have found, too, but that's a well-known one and then there's --

CHAIRMAN APOSTOLAKIS: That doesn't count.

DR. CHU: It was an equipment failure.

CHAIRMAN APOSTOLAKIS: It was not an equipment failure. It was a software failure.

DR. CHU: It was software. And then another one that seemed interesting is one at Pilgrim. There it's, I will call it, a real software common cause failure.

CHAIRMAN APOSTOLAKIS: Okay. What happened? Do you remember?

DR. CHU: It was during a storm and there is this voltage regulator that controls the voltage out of the transformer. The software was programmed such that when you have certain under-voltage, it will just trip the transformer. And of course, the same software is used on different transformers. And during this storm, the trip occurred. All the transformers lost power and you lost vital AC buses, so it is an interesting event at Pilgrim. This is based on my understanding by reading the LER.

And then there is another incident. I don't remember the specific controller. It's someone like, you know, there are two controllers, the main controller, a backup controller, but the main controller failed in such a way it prevented the backup controller from taking over. So it's some kind of dependency that caused it. That's interesting, too. You know, it is this kind of dependency we would hope to capture.

CHAIRMAN APOSTOLAKIS: Yes, that's the kind of insight we want to gain, yes. Yes, absolutely, yes.

MR. SNODDERLY: Because mainly, I know there are some folks here from Duke, but I would imagine when they come in with their application for

Oconee, they are going to look at your database and the first thing they are going to say is it's not applicable to us because, you know, we -- you know, we have this system and it's different than yours. Okay. So your database doesn't apply.

But if you can say, you know, have you considered this specific type of under-voltage or common cause failure, they can say yes, we either have that design flaw or we don't, we designed it out. So I think it's something you have -- it goes back to, I think, some of the concerns that maybe NRR has, is that I'm going to be presented with plant-specific applications of specific digital replacements, and I think it's going to be much more valuable to understand, as Dr. Apostolakis has said, the failure modes and to identify all --

CHAIRMAN APOSTOLAKIS: Sure.

MR. SNODDERLY: -- the commonality as opposed to we think digital systems of aux feed water systems have this failure rate, because I'm going to say my aux has that probability.

CHAIRMAN APOSTOLAKIS: This is the cornerstone of everything we do because, for example, yesterday we heard about fault injection techniques and they said we start with a space and we select the faults. The natural question is how do you select the fault to test against what happened at Pilgrim, right?

This is operating experience. This is the real thing. Okay? That would be a contributor. I mean, it can't be their only thing, the only basis, but it's certainly very important to know. So this data collection thing is really, in my mind, one of the most important tasks that we have in this program. Now, can you speed it up, Todd, a little bit? Yes, skip this and this.

MR. HAMZEHEE: You don't want to hear conclusions?

CHAIRMAN APOSTOLAKIS: I don't know. What is 16?

MR. HAMZEHEE: It would be probably conclusion.

CHAIRMAN APOSTOLAKIS: 16, what is 16?

MR. HAMZEHEE: 16?

MR. HILSMEIER: Task 6, Development of Reliability of Digital System Hardware Model.

CHAIRMAN APOSTOLAKIS: So you seem to have decided that either a fault tree or a Markov Model will be good enough. Is that what you're saying here? How did you decide that? I thought you were reviewing methods or you are not reviewing methods for hardware then? You are reviewing methods only for software failure, because the third bullet seems to say we know which way to go.

UNIDENTIFIED SPEAKER: George, this --

CHAIRMAN APOSTOLAKIS: Louis has announced it.

DR. CHU: We are really looking at kind of modeling the hardware of the digital system.

CHAIRMAN APOSTOLAKIS: Yes. So you have decided for hardware, this is the way to go?

DR. CHU: We feel that the Markov Model captures a lot of the digital system features.

CHAIRMAN APOSTOLAKIS: Well, you may be right, but you probably need to support that. Maybe not now, but in the future.

MR. HAMZEHEE: I think once the work is done, we're going to have some justification and bases, definitely.

CHAIRMAN APOSTOLAKIS: What I'm saying is that in the future meetings or, you know, when you have to submit reports, these things have to be supported. Don't just say, you know, we feel it's good. The Agency does not feel, Louis. The Agency is cold-blooded logic.

DR. CHU: We have tasks. We have tasks to develop models. At that point we will evaluate it more to see if it's a reasonable model.

CHAIRMAN APOSTOLAKIS: Anyway, what I'm saying is that the message you are sending there is something that may be premature.

MR. HAMZEHEE: We agree, but so far, based on what we have seen, either fault tree or Markov would be okay. I mean, not if there are some special cases that may not be --

CHAIRMAN APOSTOLAKIS: I don't know why. I mean, a fault tree I can understand, but the Markov, I mean, we start playing with states and transition rates when we just said that there is no date. It's an interesting way of proceeding. Okay. 17?

MR. HILSMEIER: Task 7 involves quantifying the Hardware Reliability Model. We'll discuss the core contributors, the system failure probability.

CHAIRMAN APOSTOLAKIS: Now, the hardware failures, shouldn't you talk about the environment at some point, I mean, what harsh environments you may have and what these will do to the hardware?

MR. HILSMEIER: I believe that should be-- that would be in the failure rates, the environment reflected in the failure rates. Is that correct?

CHAIRMAN APOSTOLAKIS: I don't know.

DR. CHU: Yes, but we don't have data to differentiate. If you look at what's in the Military Handbook or PRISM, that kind of method, they do explicitly try to account for it, but we don't know what is the basis that they come up with a pi factor of .35 or whatever. And then my suspicion is that they may have, you know, as stated, a particular component, a particular situation where they try to extrapolate to other situations.

CHAIRMAN APOSTOLAKIS: Even without this expert opinion, I mean, they feel that it was down by whatever, 70 percent, but I thought that was the whole point, that if you have an accident and you create harsh conditions, there is concern about the hardware of a machine, because under normal conditions, what, you expect random failures?

MR. HAMZEHEE: I think qualitatively we will include it, but how are we going to actually quantify it and do we have data to support it. That's the question.

CHAIRMAN APOSTOLAKIS: Oh, I don't now.

MR. HAMZEHEE: See, that is -- for qualitatively, you are right.

CHAIRMAN APOSTOLAKIS: Didn't the report

from the National Research Council address this issue? I think they did.

MR. HAMZEHEE: I'm not familiar with that.

CHAIRMAN APOSTOLAKIS: There was a report on digital software in the nuclear industry. I mean, it's a few years old now but, in fact, our consultant, Mr. White, was a member of the group.

DR. KRESS: It wasn't the National Research Council. Wasn't it the National Academy?

CHAIRMAN APOSTOLAKIS: It was the National Research Council, yes. The academies issue their reports through the National Research Council.

DR. KRESS: Oh, that's right. They do.

CHAIRMAN APOSTOLAKIS: It's the other NRC, as they say.

DR. KRESS: Yes.

CHAIRMAN APOSTOLAKIS: So I think -- no, they have a lot of good discussions there and probably they are addressing this issue, too.

DR. CHU: George, our current task is kind of limited. Look at what's available out there. You know, somewhere someone has ASME database or has collected some data.

CHAIRMAN APOSTOLAKIS: The Academy report may also verify or may have information.

DR. CHU: In the case of software, I mean, we are starting the task. We are starting the correct software failure experience. It looks like they are-- a lot of it is interesting experience.

CHAIRMAN APOSTOLAKIS: These Academy reports usually are reviewed by everyone and his mother and it's a good idea to know what they say, because there was no consensus about that. That's why, in fact, it never came up with any complete recommendations, because they couldn't agree. They just couldn't agree, but the discussions they had there might be very enlightening and they have a long list of references.

MR. HAMZEHEE: We'll look into it.

MR. HILSMEIER: Task 8 involves developing an acceptable method for including software failures in digital system PRAs, and the first task step in Task 8 is to review software-induced failure events from different industries to identify failure modes, failure causes, current frequencies and to gain insight into modeling software failures in the PRA. This sub-task was included under recommendations from ACRS. I don't recall what meeting that was, 2004. And then the second --

CHAIRMAN APOSTOLAKIS: This is the

presentation that follows, right? Isn't that what Steve Arndt and Tunc Aldemir is going to talk about?

MR. ARNDT: Pardon me? What was the question?

CHAIRMAN APOSTOLAKIS: Development of NASA modeling software failures. Isn't that what you're talking about later?

MR. ARNDT: Not exactly. As I talked about last night, we're intentionally going at this from two different perspectives. This effort is looking at it from more traditional efforts of looking at hardware modeling and software modeling and fault tree modeling and things like that. The other effort is looking at it from an integrated digital systems type analysis that looks at using the more complicated, integrated methodologies. So it's the same concept, but from a different perspective and we'll take about that after this presentation.

CHAIRMAN APOSTOLAKIS: All right.

MR. HILSMEIER: And next we'll review additional literature on development of the Software Reliability Model. We'll address issues such as software failure rates, meaning full and consideration of uncertainties and evaluate different reliability methods such as fault trees, Markov, reliability growth models and the other methods that we find from the review.

Then we'll develop the Quantitative Software Failure Model and evaluate existing software reliability models and establish a linkage between software and hardware models, and determine software failure parameters that have to be quantified. Different types of software have different effects on digital systems and they may have to be modeled differently. We'll apply the Software Reliability Model again to the digital protection system for a time, and the scheduled time frame for this task is July 2005 to September 2008.

Task 9 involves quantifying the software failure probabilities identified under Task 8. And this task is estimated to be performed in October 2007 and completed by September of 2008. Task 10 involves quantifying the Digital System Reliability Model incorporating the hardware and software together and performing --

CHAIRMAN APOSTOLAKIS: For all of the system?

MR. HAMZEHEE: Yes. For instance, for RPS systems.

CHAIRMAN APOSTOLAKIS: The digital RPS?

MR. HAMZEHEE: Yes, the digital RPS. The analog we already have.

CHAIRMAN APOSTOLAKIS: No, but you would not include the rods.

MR. HILSMEIER: That's right. And we'll perform sensitivity calculations to evaluate --

CHAIRMAN APOSTOLAKIS: You know, there is a very good discussion in that Academy report on these things and for the RPS, it might work, but for other systems probably not, because all it does is it gives a command scram, collects data and gives a command. In other situations, we're saying that the argument is that you cannot just talk about the software in isolation from the bigger system. If the software, you know, controls parts of the hardware and receives commands and all that, but in the RPS probably it's a simpler system, because all it does is monitors variables and says shut down.

MR. KEMPER: Well, if I could add. This is Bill Kemper again. To a large extent that's true, but it's also variable trip calculations that go through the various RPSs, so that is a bit of sophistication maybe that we have to investigate.

CHAIRMAN APOSTOLAKIS: Right. Right. True. But I mean, if there is a system where this approach works, then probably this is the kind. Okay. Task 10.

MR. HILSMEIER: Task 10 is scheduled to start in October 2007 and be completed in 2008, in December. Task 11 involves integrating the Digital System Reliability Model into the PRA. And if we choose to use Markov in that model, then we have got to develop an integration method. We also need --

CHAIRMAN APOSTOLAKIS: Now, this work for Oconee, because you mentioned Oconee several times, this is not in support of the NRR activity. I mean, this is just the method development within RES and the reason why you're using Oconee is because you're going to have information.

MR. HILSMEIER: That's correct.

MR. HAMZEHEE: Correct.

CHAIRMAN APOSTOLAKIS: Okay.

MR. HILSMEIER: And also under Task 11, we'll develop guidance on when diverse systems can be considered independent. And that's scheduled to start in October 2007 and complete in March 2009. The last task is developing, preparing a NUREG report that documents all the tasks and, as you mentioned earlier, we will have intermediate reports.

CHAIRMAN APOSTOLAKIS: Well, you gentlemen may want to think about a schedule for interactions with us. I mean, pass it by Eric. Not too frequent, not too infrequent. Hossein, this is the report. Steve doesn't want anybody else to see what the report is. Okay. Any questions from the Members of the Subcommittee? I guess not. Please. Please, identify yourself and speak with sufficient clarity.

MR. WATERMAN: This is Mike Waterman with Office of Research. And just going back to my experience over at NRR, I would like to bring up a point about using manufacturing data, is the denominator in that data is going to be biased by the warranty period of the equipment that's reported to the vendor.

So if you just rely on that data, all you're going to get really reported to the vendor is equipment that failed during the warranty period where the company using that equipment thinks they can get a new piece of equipment for it. Now, if that company instead has a piece of equipment fail beyond the warranty period, it's more expensive for them to report the data and still buy the equipment than it is for them to simply buy a replacement part, stick it in and get back to operation. So you're probably not going to get a lot of out-of-warranty reports on that.

Let's see here. The other basis is is that if you have got equipment out in the field, the manufacturer says look how long my equipment has been running. And then when you go out to the field, you find out two years prior to that that equipment was replaced by another vendor's equipment. And so you can't just say well, it hasn't failed so look how long it has run without failure. It might be sitting over, you know, acting as a reef out in somebody's harbor by then. So it's kind of hard to use manufacturing data.

As a matter of fact, in dedicating COTS equipment, we have four processes that can be used to dedicate COTS equipment for safety-related applications. That's special tasks and inspections, supplier surveys, source verification and use of historical data. That fourth option always has to be combined with one of the other three simply because, you know, historical data is just not all that reliable.

With regard to using nuclear power plant LERs, keep in mind that LERs are submitted when safety systems are challenged. So the only time you're going to get an LER is if the reactor trips or something like that happens or a piece of safety-related equipment is inoperable. You may have lots of other failures in a plant that have occurred. But you may never hear about them, you know, it costs money to do an LER if they didn't affect safety. So you have got to kind of keep that factored in there also. So just a couple of comments on using historical data.

CHAIRMAN APOSTOLAKIS: Thank you.

MR. HAMZEHEE: Thanks, Mike.

CHAIRMAN APOSTOLAKIS: Any other comments from the audience?

MR. TOROK: Yes.

CHAIRMAN APOSTOLAKIS: Yes, come in, come up.

MR. TOROK: I'm Ray Torok from EPRI and I guess we have been looking at, I guess, things related to this for a couple of years now and I have some suggestions about, I mean, questions about what you have been looking at and maybe things that would be helpful.

One of them is have you guys looked at the sensitivity of the core damage frequency to how the I&C is modeled in the PRA, you know, and more specifically, what is the target reliability that you need from the I&C to make it a negligible contributor to risk compared to everything else, because in the grand scheme there are many components in each system, you know, pumps and valves and so on, and there are many systems in a plant.

And so it may be that the reliability you need from the I&C is really pretty modest in the grand scheme of things and it may not be or it may be that you don't need a precise, you know, determination of the reliability. At least that's the way it looks from a lot of sensitivity studies that we have done.

Another question is in regard to the use of data from other places like NASA for example. When you look at NASA software, are you looking at serial number one, a one of a kind of software, you know, based system as opposed to a commercial device where there are 40,000 or 50,000 of them in the field.

Now, what we found in talking with commercial vendors and reviewing, doing design reviews and so on on their equipment including their software, is that by the time a commercial device has matured in the field, the manufacturer's historical data shows a trend where the software-based failures go to nothing and then they stop changing the software. They stop fixing it, because it's as fixed as it's going to get, and the hardware failures continue, all right, which is kind of what you expect, because once you have the hardware right or the software right it stays stable.

The hardware continues to degrade with time and so on.

We have also talked with vendors were they meticulously kept records comparing their old analog devices to their new digital counterparts, because they wanted to prove to themselves that the digital devices were at least as reliable as the old analog devices, so that had data on that. Now, whether or not they want to share it with you, I don't know. You know, we signed non-disclosure agreements and whatnot.

But the manufacturers are really up to speed on that and many of these cases, now, I'm talking primarily about simpler components, transmitters, you know, signal controllers, simple devices compared to PLCs, but in those cases once the software gets mature, it's mature, you know, and that's the end of the changes for that.

So another question then that goes with that is have you guys looked at the possibility of comparing the analog to digital reliability to get a handle on what these digital systems are, because the analog systems are modeled in the PRAs right now. That leaves us a black-box and, in many cases, I suspect the black-box is more than adequate in the context of the PRA because of all the other contributors, right?

The other thing I wonder about when you're looking at the data, especially for software, is that you look -- I suggest that you look at the root cause. A lot of things that are determined to be or that are called software failures turn out to be requirement specification errors and, in fact, I know many stories about digital failures at various times and every one of them comes back to a requirement specification error not a software error at all.

CHAIRMAN APOSTOLAKIS: So?

MR. TOROK: So then the question, of course, is how do you roll that into what you do with, you know, your -- with your model in PRA?

CHAIRMAN APOSTOLAKIS: Yes. And how is that consistent with your earlier admonition to look at what kind of reliability should the software have compared to the hardware if the failure models are different? You know, it seems to me it's not just a matter of the number. It's a matter of us understanding how they fail and digital software don't fail in a continuous manner like analog or the non-physical components.

MR. TOROK: No, I --

CHAIRMAN APOSTOLAKIS: It seems to me you have to understand first the failure models.

MR. TOROK: I agree, and that's why in the method that we're proposing, we would love to talk to you more about it.

CHAIRMAN APOSTOLAKIS: Yes, sure.

MR. TOROK: And I think we should. I think we should participate in some of these discussions, because we have kicked these things around quite a bit. And that's why we ended up looking to what we call this defensive measures approach where you're trying to understand and evaluate the specific design features that are implemented in these software-based systems to preclude certain types of failures, because that has a tremendous impact on the reliability and in some cases, you get into very subtle things.

CHAIRMAN APOSTOLAKIS: Maybe what you are proposing in your report, I don't know, is how to manage the issue of adding software to plants, because you're talking about, you know, I guess defense-in-depth and diversity issues.

MR. TOROK: Well, yes, and what we're looking at, of course, is defensive measures built right into the software.

CHAIRMAN APOSTOLAKIS: Yes.

MR. TOROK: Either intentionally as a

defensive measure or because something inherent in the design structure provides some defense against common cause failure, you know, and simple --

CHAIRMAN APOSTOLAKIS: So your report might be more useful to NRR, because these guys are developing methods for assessment, the assessment of this. And after that they will go to the management, but you, of course, are interested in what do we do now. I mean, the industry has to have something, some guidance, so you're probably ahead of the curve, but it doesn't hurt for them to know what is already done on this.

MR. TOROK: You know, of course, the problem we end up with is software failures aren't random at all, right? So what it comes down to is understanding what kinds of failures the software is--

CHAIRMAN APOSTOLAKIS: You see, that's why I keep questioning the use of Markov Models. You know, they are not random. We have to understand that and appreciate that. Now, there may be some instances where, you know, the models are fine but, you know, you have to really conclude that after some argument.

MR. HAMZEHEE: Yes.

CHAIRMAN APOSTOLAKIS: Okay.

MR. HAMZEHEE: And I think there were some good remarks and I would like to just make two points that are related. One is right now, as we speak and as you know, the reliability of, for instance, analog RPS is like a $1E^{-6}$ failure probability. So if they are so highly reliable, can you beat that with the digital?

CHAIRMAN APOSTOLAKIS: Anyway, the --

MR. HAMZEHEE: So we have to make sure, number one, how they compare.

MR. TOROK: Well, there is --

CHAIRMAN APOSTOLAKIS: No, he wants you to compare it with the failure rates of pumps.

MR. HAMZEHEE: Well, but right now this is with RPS?

CHAIRMAN APOSTOLAKIS: Then you are at least more free.

MR. HAMZEHEE: Because they are highly reliable with analog systems. We don't know how reliable the digital is, number one. Number two, you're right again with respect to the software, but the problem that we may have, and we don't know because of some of these unknowns, is the software is highly reliable, but if there is a bug someplace, it can bypass all the redundancies within your system. So that could wipe out the whole system. That's why you have got to be careful as to not allow any failures in your software.

CHAIRMAN APOSTOLAKIS: If it fails, you don't know how it's going to fail.

MR. HAMZEHEE: Exactly. You could wipe out the whole system regardless of how many channels you have, how many redundancies you have.

MR. TOROK: That's true and the thing that typically gets software into trouble is when it encounters conditions that were unanticipated by the designer or untested, that sort of thing. Well, it turns out there are many defensive measures that can be incorporated into the design of the feature, I mean, into the design of the software, I'm sorry, to handle those things. So that's why in our method it's very important to find those.

CHAIRMAN APOSTOLAKIS: Anyway, maybe the message here is that -- oh, I'm sorry.

DR. BONACA: You made a statement regarding, you know, the importance of using commercial devices where the potential is that since you have the software so, therefore, the software folds back under from that.

CHAIRMAN APOSTOLAKIS: Yes.

DR. BONACA: But I always sense that for

power plants, I mean, the way I see it, if I think about replacement RPS and ESF, it's going to be really probably one or two applications at least in the short-term. So how does that insight apply? I mean, am I misunderstanding what you're communicating there?

MR. TOROK: Well, I'm not sure. Let me try this in -- a number of the applications that are being done right now, like at Oconee they are using a Teleperm XS platform, right, a commercial device, a commercial PLC.

DR. BONACA: Commercial? Let me understand now, commercial?

MR. HAMZEHEE: He is saying you can't use commercial, because these are safety-related systems. How can you use commercial for RPS, for instance?

MR. TOROK: Well, there is commercial grade dedication to get commercial grade equipment in there. In the case of the Teleperm, it has been reviewed by NRR and there is an SER out on it. So those things have been done.

MR. HAMZEHEE: There's a quality requirement even for commercial. You have some quality requirement.

DR. BONACA: The software logic is going to be one application, right? The software logic that you have put in on this platform is going to be one application.

MR. TOROK: That's right. That's a good point. So what you find in a platform like that where it's a very flexible platform by design, right, the weak link from a software standpoint isn't in the invented software that's on the platform or the operating system or any of that stuff. The weak link is the application code. That's where you have got to be very careful.

DR. BONACA: And that's what we're concerned about.

MR. TOROK: That's right. So the object in a case like RPS is to keep that as painfully simple as you can, right, and then to go through the right QA process and so on.

DR. BONACA: And that's what troubles me somewhat. This goes back to the presentations we had yesterday morning regarding the new approach. For example, we go from Reg Guides who are very prescriptive about what you're going to monitor and what controls you have in the RPS to one for new plants that is very generic, general, provides all these error guidelines.

And you know, my concern is, you know,

maybe the proliferation of uses that you may have, so you get the bigger software on a bigger platform as a capacity, so that you can handle more things, and I think that in general brings with itself a higher fault probability, it seems to me.

MR. TOROK: I agree, so it's the weakest link. Nothing is better than keeping it simple.

DR. BONACA: Yes. I'm trying to understand how you go about 4b.

CHAIRMAN APOSTOLAKIS: But not simpler, as Einstein said.

DR. BONACA: Yes. But even, you know, I mean, after TMI, for example, one of the objectives was the one of minimizing literally the functions that you put in front of an operator, make them really meaningful, so that you have a good picture but, you know, the word at that time a lot of companies that proposed very large systems with many more functions, etcetera, and the objective was they want to say forget about this stuff. You want to focus on really critical pieces of communication to the operators. Okay? And I am trying to understand how the digital systems are going to go away from this philosophy, maybe. I don't know.

MR. HILSMEIER: That's a good point.

MR. TOROK: It's certainly concerned with the digital systems and a fair question to ask is what have you done to make sure that you're not going to overwhelm the operator or have made it too complicated? Is this a fair question?

DR. BONACA: Or create again other failure modes inside the software that were not foreseen.

MR. TOROK: That's right. And the other thing, the same consideration, if you add a diverse backup for a software-based system to deal with the common mode failure, because you add complexity when you do that, so you want to be careful about where you do that.

CHAIRMAN APOSTOLAKIS: Thank you very much. Anybody who wants to be hated? We will reconvene at 3:15.

(Whereupon, at 3:00 p.m. a recess until 3:20 p.m.)

CHAIRMAN APOSTOLAKIS: Back in session. The last presentation will be by Mr. Arndt and Professor Aldemir of Ohio State. Is that the plan? Yes.

PROF. ALDEMIR: Yes, sir.

CHAIRMAN APOSTOLAKIS: And you need, what, an hour and 45 minutes or something like that?

MR. ARNDT: An hour and a half to two hours depending upon how many questions we get.

CHAIRMAN APOSTOLAKIS: There are no questions.

MR. ARNDT: Yes, right. I will be giving the first part of this presentation and since you have heard more than enough of me for the last two days, Professor Aldemir will be giving the latter part of the presentation. Why don't you go ahead?

CHAIRMAN APOSTOLAKIS: Now, there is also a report, which is a NUREG draft report out of Tunc's shop.

MR. ARNDT: That was provided for background.

CHAIRMAN APOSTOLAKIS: Just background.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: You are not asking us to comment on it.

MR. ARNDT: No, it's a draft, so just background.

CHAIRMAN APOSTOLAKIS: But it will become a NUREG report.

MR. ARNDT: If we decide that it's of sufficient quality, etcetera, etcetera, then it is anticipated it to become a NUREG report.

CHAIRMAN APOSTOLAKIS: But I'm just wondering. I mean, there is some speculation here that a rating of various methods against some criteria, I don't know, I mean --

MR. ARNDT: We'll talk about that today.

CHAIRMAN APOSTOLAKIS: Ah, okay. Go ahead.

MR. ARNDT: Just as some basic background, we talked about this a lot last night. The NRC encourages the use of PRA and associated analyses to the extent possible. In the National Academy study, as well as the ACRS letter associated with it, they encouraged the development of risk-informed application in this area.

Particularly, to go back to the National Academy study, the specific recommendation was that the NRC should strive to develop methods for establishing the failure probabilities of digital systems for use in probabilistic safety assessment. These methods should include acceptance criteria guidelines, limitations of use and for rationalization and justification for the methods chosen.

So the idea behind this is to look at the different kinds of methodologies. As has been recommended by the ACRS, it would be preferable if we could do this in an integrated fashion. Now, we may not be able to do that, but what we want to do is look at near term PRA applications, which means you have to integrate the rest of the current PRA and develop them in such a way that it makes the most sense.

So because of this, what we need to do is look at the need to account for dynamic interactions with the process, the interactions between the digital system itself, the various components in the digital system as well as the systems that they are controlling and tripping.

So as I mentioned yesterday, what we're trying to do is look at this from two different aspects, one from the traditional fault tree/event tree analysis, one from a dynamic modeling analysis. So what we're trying to do is figure out whether or not you can build models that can account for these effects and then feed them into our current regulatory structure.

As we talked about yesterday, we have an overall program plan that looks like this. What I have done is I have shaded in green the areas that this presentation is referring to. In the previous presentation that Hossein gave, they are looking at some of the other parts of the program. So for example, the failure modes, the traditional methods, hardware, software quantification and the evaluation, that's a simplified version of their chart. On the other side, the stuff we're going to talk about this afternoon, is looking at the dynamic modeling methodologies.

CHAIRMAN APOSTOLAKIS: But several of the methods that you will talk about have not been designed just for dynamic methods. I mean, I'm surprised that the guys on the left have not looked at that and they just talk about traditional fault trees and Markov. I mean, we will see them later, but --

MR. ARNDT: Yes, you can --

CHAIRMAN APOSTOLAKIS: I mean, the two groups don't seem to talk to each other, do they?

MR. ARNDT: We do talk to each other.

CHAIRMAN APOSTOLAKIS: Over the phone?

MR. ARNDT: Yes, but we're down the hall from each other. It's a challenge.

CHAIRMAN APOSTOLAKIS: But, Todd, really, I mean, in your presentation I would have expected to have seen a longer list of potential methods from which you will pick one after you decide what is applicable to your methods like these guys have been doing, and I know what methods Tunc is going to talk about. I mean, some of them are unique to dynamic systems in the sense that Tunc is talking about, but not all of them.

MR. ARNDT: No.

CHAIRMAN APOSTOLAKIS: Not all of them.

MR. ARNDT: And what I think Todd was trying to say is this is an example of a methodology. They haven't come up with their actual solution yet.

CHAIRMAN APOSTOLAKIS: No, but the way they were presenting it, they said we'll go either with fault trees or with Markov. That means that's it, one of the two. And now, we're going to hear about five or six methods and I think most of them apply to them as well.

MR. ARNDT: They potentially apply.

CHAIRMAN APOSTOLAKIS: Yes, potentially, potentially, maybe, perhaps.

PROF. ALDEMIR: May I make a comment here? My name is Tunc Aldemir and I am a faculty with Ohio State University. I have been working with Probabilistic Risk Assessment for over 20 years and specifically in dynamic methodologies.

What I think the issue here, which was mentioned earlier, is that we are approaching it from -- I mean, it's the diversity issue like we had national, what is it, Los Alamos and Sandia and then Lawrence Livermore, not really competitors, but doing different methodologies. We are approaching the same problem using different approaches. I think that's the issue, right?

CHAIRMAN APOSTOLAKIS: I don't know why you guys are commenting on what I said so much.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: All I said was that they did not present a complete set of potential methodologies and I keep hearing well, we're doing it two different ways and perhaps and potential. I think it's a true statement.

MR. ARNDT: It is.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: Onward. So the objective of the study is, basically, to look at the different kinds of methodologies that might be available, make some conclusions and choose the kinds of methodologies we can use, develop an understanding of the potential advantages and disadvantages and do some pilot studies on the proposed methodologies.

As you heard earlier, the other side of the problem is also going to do some pilot studies and what we're planning on doing is having at least two different pilot studies, one that has the likelihood to be more successful than traditional modeling like RPS, and one that has more likely challenges associated with dynamic modeling like the auxiliary feed water system.

So we're going to look at the various issues associated with the current PRA modeling methodologies, fault trees/event trees, review the advantages and limitations of dynamic methodologies, review the industry practices, has anybody else used dynamic methodologies effectively, look at the existing regulatory framework and what does that drive us toward?

What do we need to accomplish? What level of detail do we need to do, so this might be implementable from a regulatory standpoint. And then look at the minimum requirements associated with doing this. Is there something associated with the dynamics of the failures or with the system itself that requires us to do this? We don't want to do this simply as an academic exercise if the particular interactions in the system --

CHAIRMAN APOSTOLAKIS: So don't go to Ohio State.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Well, you have a professor and you are asking him not to do an academic exercise.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: All right.

MR. ARNDT: But the point that we're trying to make is if we do this research and it turns out that these are really neat methodologies, but they are not necessary to get an accurate answer, we don't want to require or encourage the industry to do something more than is necessary. Now, there may be situations where you do need it and that's what we're trying to understand, and we believe that there is at least a good possibility that that's the case or we wouldn't be doing it. And then identify the requirements associated with it.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: So at this point, I'm going to let Tunc talk for awhile and you can give him a hard time.

PROF. ALDEMIR: Okay. When we got the task -- I went through the introduction, I guess. When we got the task, we said what is it that makes analog systems different from digital systems? So we looked through the literature and we really didn't find a complete list. Actually, we didn't even find a partial list. So we tried to characterize.

Incidentally, on this project, we have three people who are professional computer science people, two professors and one student, so the computer expertise is not being provided by the nuclear people.

CHAIRMAN APOSTOLAKIS: By the way, do you have anybody at Ohio State in the Computer Science Department who worries about software failures?

PROF. ALDEMIR: There is no such person.

CHAIRMAN APOSTOLAKIS: There is nobody anywhere in the Computer Science Department.

PROF. ALDEMIR: No, you are right. You are right. I checked for that, because I wanted to establish a Reliability Engineering Program a long time ago. There is no such person, but we will have somebody who is as close to it as you can get. That's Mike Stusky, who is working on our project. So what we found are the following and, again, this is probably not a complete list, but this is the best we could come up with.

First of all, the firmware and software components of the digital I&C systems do not demonstrate any wear characteristics, so they don't respond to accelerated testing, stress testing, etcetera, so it's hard to test them the way you would do hardware. Firmware, software reliability cannot be accurately modeled using your bathtub curve approach. What happens is that you have the infant mortality come down and come to sort of a plateau and then slightly increase, because every time you fix software you may be messing it up more.

So then the third difference is that, and this is a big one, there may be complex interactions between the constituents of the digital I&C system and between the digital I&C system and the process physics, which may lead to potentially significant dependencies between failure events, such as digital I&C systems rely on sequential circuits that have memory, and so the system response is not just dependent on the existing system state, but also on the system history as well as the rate of progress.

Tasks may compete for digital controllers resources, which may lead to problems such as deadlock and starvation. Choice of external/internal communication mechanisms for the digital I&C system, such as buses and networks, and the communication protocol affects the rate of data transfer. The ability to coordinate multiple digital controllers directly and explicitly may necessitate a finer degree of communication and coordination between controllers. A digital --

CHAIRMAN APOSTOLAKIS: I don't know what that means.

PROF. ALDEMIR: Right now, I will go through an example. I will go through an example later on to show process couples events.

CHAIRMAN APOSTOLAKIS: Okay. Okay. We can do that later.

PROF. ALDEMIR: And all I'm saying here is that it makes it tighter. A digital controller can remain active and not only react to data, but anticipate the state of the controlled monitoring system and actually do prognosis rather than just diagnosis.

CHAIRMAN APOSTOLAKIS: Now, this is, your bullet here, your third bullet, not the second, but the third one, really the major issue in the software safety community and that's why I said earlier for the reactor protection system, you may be able to model the software sort of independently of the rest of the system. But in general, the school of thought that follows that says that the software is embedded in the hardware system that it controls and you have to study it as one system. Okay. And I still think that applies to the other guys, too. It's not just you.

MR. ARNDT: Well, the issue is --

CHAIRMAN APOSTOLAKIS: And this is a major issue that was discussed in the Academy.

MR. ARNDT: Yes. And the issue is where do you draw that line until you go at it from both sides?

CHAIRMAN APOSTOLAKIS: If you want to draw a line.

MR. ARNDT: Yes, if you want to.

CHAIRMAN APOSTOLAKIS: I don't even know why you draw it.

PROF. ALDEMIR: Another important difference is that the failure modes of the digital I&C system are not defined, well-defined. For example, failure of one component, constituent of the system can affect the rest or other parts of the overall system. A system may not fail only on specific input, but on other inputs that are semantically similar or even equivalent or correlated.

Software may be able to mask intermittent failures in hardware, so it may be failed, but you may not be aware of it. And there is an example here. Digital I&C systems share data transmissions, functions, process equipment, which makes them more vulnerable to common cause failure. It is possible for the I&C system to introduce new events, new failure events and also, as part of this as well, multi-testing may introduce new failure dependencies between systems.

Software is not a physical entity and testing alone is not sufficient to verify that software is complete and correct and, in fact, there is a fair amount of literature on this. And software defects may remain hidden for long periods and suddenly appear when a certain execution path is exercised.

CHAIRMAN APOSTOLAKIS: Which is typical of design error.

PROF. ALDEMIR: Right.

CHAIRMAN APOSTOLAKIS: If you have a design error that will appear only if you have a strong earthquake, you know, that's the problem.

PROF. ALDEMIR: In fact, this came up before and I want to make a comment as to the use of conventional reliability models or potential use of the conventional reliability models to model software failures. Solenoid wells have a failure PDF, probability distribution function, for failure that is almost like a delta function. So you know, there is an analog in the hardware world and what we are talking here, if nothing happens, unless something happens and so it's like a delta function.

CHAIRMAN APOSTOLAKIS: For equipment that are there to mitigate the consequences of severe external events, this is a major issue. If I have a major earthquake, if I have a major tornado and I have built into my plan systems and components that will protect me against those, it is a design error there I have never known until I'm hit. So in the hardware there is exactly the same problem.

PROF. ALDEMIR: There is a problem.

CHAIRMAN APOSTOLAKIS: And if they find in one of the plants, they had problems, that they had run out of oil or lubricant or something, I don't remember now, it was in the old days. A previous incarnation of the ACRS worried about design errors every time they met, so this is very well-known.

PROF. ALDEMIR: Well, this has been discussed already, so I'm not going to spend too much time and the previous presentation covered much better than I am covering.

CHAIRMAN APOSTOLAKIS: Well, let me ask you this. We always keep saying about other industries. Have we ever found anything in other industries that was useful to us?

PROF. ALDEMIR: No.

CHAIRMAN APOSTOLAKIS: No.

PROF. ALDEMIR: The answer is no from my side.

CHAIRMAN APOSTOLAKIS: The answer is no.

PROF. ALDEMIR: There is one exception and then, this is the last bullet. NASA, of course, has been using dynamic methodologies for awhile, so that is an --

CHAIRMAN APOSTOLAKIS: A small group at NASA, not NASA itself.

PROF. ALDEMIR: But they are very much interested in doing right now.

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: Mike Stamatelatos wants to actually join forces with NRC on this.

CHAIRMAN APOSTOLAKIS: A lot of people are interested, but what are they doing?

PROF. ALDEMIR: Well, we'll try to coordinate.

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: Okay. So the question is -- and we kept mentioning dynamic methodologies, but we did not really justify it. The justification changed through implicit statements. I mean, when I was listening to differences between digital systems and analog systems, the need was implicit, but I want to make it a little bit clearer here.

What happens is that these dynamic interactions between plant processes and triggered and stochastic events, which may happen in reactor protection and control systems, may lead to coupling between failure events and I will illustrate that later on by an example from feed/bleed cooling of a PWR following a small break.

Cases reported in the literature, and there aren't too many of them as far as I know, maybe three or four, all on this process control system interaction indicate that the event tree/fault tree approach may yield conservative, but this may be an important point, but may be overly conservative results. This may be a point for the industry maybe.

Omission of failure scenarios is possible if dynamic interactions between plant physical processes and triggered or stochastic logical events are not accounted for. The first study, as far as I know and it may be the only study as far as I know, is by Cacciabue and Amendola and Cojazzi. It's about, what, 15, almost 20 years old. They discovered that you may be missing important scenarios if you don't use -- if you use static methods in conventional event tree/fault tree.

And dynamic methodologies, I will define formally in a little while, will be needed only for systems in which significant interactions are possible. If they are not and RPS system is a good candidate, but as was mentioned earlier, there may be also complex interactions within that system through the software, so we are not too clear if it's really going to be applicable. But if there is any system, reactor-related system, that is probably a good candidate.

We need to worry about two types of interactions. The first one is the interaction between the I&C system and, in our case, the reactor protection and control system and controlled and monitored plant physical processes, such as heatup and pressurization of the reactor and level control, which I will call Type I interactions. This is not standard from literature. We are just inventing the terminology, Type I interactions.

And I call them Type I, because historically they were the first ones that were discovered. Interactions between the constituents of the reactor protection and control system itself, such as communication between different components, multi-tasking, multiplexing, and there are lots more. So we call them Type II interactions.

From a reliability modeling viewpoint, Type I and Type II interactions are separable only for single-input, single-output I&C systems.

CHAIRMAN APOSTOLAKIS: Like a scram system.

PROF. ALDEMIR: Even then, again, it depends how many single-input, single-output. Yes, multiple-input, single-output I am not too sure. This assessment you validated but, again, you know, it's kind of speculative at least, but sounds reasonable, I guess.

Generally, it is difficult to integrate a dynamic model into existing plant PRAs, almost all of which are based on the ET/FT approach. Now, this is a critically important point, because there are dynamic methodologies available and I believe you can use them for all sorts of fancy modeling, however fancy your system may be. But then what do you do with the results is a big issue, because it has to go into a complete plant PRA and that is based on codes like SAPHIRE and CAFTA.

So you have to come up with cut sets. You have to come up with the dependencies between. You have to figure out the boundaries of the system within the existing PRA, take it out, put the new one in. That's a major task and I don't think that anybody knows how to do that yet.

So what are dynamic methodologies, and I will look at first for Type I interactions. There are three types, three major types, continuous time methods, discreet time methods and what I call visual methods. I first called it graphic methods. My colleagues did not like it, so I called it visual methods and most of which are semi-dynamic and I will define that in a little while.

So continuous time methods. The first one is the continuous, not the first one historically, but the one that is most comprehensive and then includes almost everything else, is called the continuous event tree approach, which was proposed by the late Jacques Devooght from the Free University of Belgium, a very elegant theory. It consists of a set of linear integral differential equations. It includes everything about the system. You can model almost anything that you want, but it's very complicated, too.

Then there is the discreet space, but continuous time analog of this. The one problem with CET or the continuous event tree is that it is hard to model transitions on demand or failures on demand. So we came up with a discreet space version of it. This one, the continuous cell-to-cell mapping technique, which allows failures or modeling failures on demand.

When you go to discreet time methods, of course, the first one is Monte Carlo. I mean, if you could --

CHAIRMAN APOSTOLAKIS: What do you mean? Monte Carlo is a method of propagating uncertainties. Why is that a discreet time method?

PROF. ALDEMIR: You can do the same thing to failures.

CHAIRMAN APOSTOLAKIS: But Monte Carlo you can use everywhere.

PROF. ALDEMIR: Right, right, right.

CHAIRMAN APOSTOLAKIS: I mean, it's a method for solving a problem. It's not a model or a methodology.

PROF. ALDEMIR: But it is a methodology to approach the problem. If you really can afford the computational time, in fact, that's the best thing to do.

CHAIRMAN APOSTOLAKIS: But you will still need a model and you may still need the CET.

PROF. ALDEMIR: You will need a failure model, sorry, a probability distribution function to describe your failure. You are right in that. But when I say --

CHAIRMAN APOSTOLAKIS: Not only that, but I mean how the components interact, how they interact with the process system. I mean, this is just a method for --

PROF. ALDEMIR: If you have a system simulator and you use a model --

CHAIRMAN APOSTOLAKIS: So I will need a model.

PROF. ALDEMIR: Yes, you are right.

CHAIRMAN APOSTOLAKIS: I need a model.

PROF. ALDEMIR: Right.

CHAIRMAN APOSTOLAKIS: This is not a methodology like DYLAM, for example, DYLAM is a methodology.

PROF. ALDEMIR: You are right.

CHAIRMAN APOSTOLAKIS: And Monte Carlo is not.

PROF. ALDEMIR: When I said methodology,

I implicitly was thinking of stochastic methodologies.

CHAIRMAN APOSTOLAKIS: I would delete it from here. I mean, it's just a tool for --

PROF. ALDEMIR: Okay.

CHAIRMAN APOSTOLAKIS: -- working with any of those.

PROF. ALDEMIR: Okay. Then there is a dynamic event tree generation approach and there is a slew of methodologies. DYLAM is the first one as far as I know, developed by Ispra Mendelo and I think Mendelo was the main contributor. Then there is the one that Nathan Siu developed at MIT while he was at MIT. They are similar in principle, but they differ in branching rules. Then there is the Accident Dynamic Simulator by Ali Mosleh at the University of Maryland. There is the Integrated Safety Assessment methodology developed by --

CHAIRMAN APOSTOLAKIS: This is what the chemical guys use?

PROF. ALDEMIR: No, no, this is by Jose Izquierdo from Spain.

CHAIRMAN APOSTOLAKIS: Because there is an ISA that is being used by the MOX people. Is that what they call it, Integrated Safety Analysis?

MR. SNODDERLY: Right.

CHAIRMAN APOSTOLAKIS: This is not it?

MR. SNODDERLY: Right. No, it's something else.

PROF. ALDEMIR: No, this is not it. This is by Jose-Maria Izquierdo from Spain and the Spanish NRC, by the way, or their equivalent of it is using it to assure that the scenarios are complete for the licensee reports. And there is the cell-to-cell mapping technique, which was developed at Ohio State and it's a discreet time, discreet space version of --

CHAIRMAN APOSTOLAKIS: So there is one less C.

PROF. ALDEMIR: One less C, yes.

CHAIRMAN APOSTOLAKIS: Which C did you drop?

PROF. ALDEMIR: Actually, historically, this came first. This came later and this came last.

CHAIRMAN APOSTOLAKIS: Yes, but, I mean, what is the extra C? It stands for what?

PROF. ALDEMIR: Continuous cell-to-cell mapping technique.

CHAIRMAN APOSTOLAKIS: Oh.

PROF. ALDEMIR: Cell-to-cell.

CHAIRMAN APOSTOLAKIS: There should have been a D there. Where is the D?

PROF. ALDEMIR: Discreet.

CHAIRMAN APOSTOLAKIS: Discreet.

PROF. ALDEMIR: Okay. Professor Apostolakis is going to argue with that probably, but there is also a DDET/MC. DDET/MC is a dynamic event tree generator developed by --

CHAIRMAN APOSTOLAKIS: That's okay. We don't need it.

PROF. ALDEMIR: -- a Belgian chap, Pierre-Etienne Labeau, Pierre-Etienne Labeau, but what happens with the MC part is it is used to quantify uncertainties associated with the inputs to dynamic event tree. See, there are two types of uncertainties and I'm talking about aleatory and epistemic, but there are two types of uncertainties that you need to analyze when you look at the event tree.

Firstly, the branching probabilities and the numbers you use are just numbers and you don't know if you are right or not. So there is one approach which likes to sample over a given distribution rather than using discreet numbers. There is another approach, which uses the Latin Hypercube, that means that you generate more than one branch, and then you say, but you started an initiating event. How do you know your initiating event was right in the first place? So you have to sample over the uncertainties in the initiating event and that's where the MC part is coming from.

I'm sorry. I'm sorry. I get in a lecturing mode. Visual methods. You know, the common denominator for these methods is that they have all graphical interfaces. You can look at them and you see system topology.

CHAIRMAN APOSTOLAKIS: But again, I don't know. I mean, isn't the Petri net a discreet time, discreet space and state?

PROF. ALDEMIR: You can look at it different ways, true.

CHAIRMAN APOSTOLAKIS: But is it true?

PROF. ALDEMIR: Yes, sure. But as I said, the common point is that --

CHAIRMAN APOSTOLAKIS: You have --

PROF. ALDEMIR: -- of these methods is that the commonality is going to be the visual aspect of it.

CHAIRMAN APOSTOLAKIS: No. I mean, you really have to make that very clear, I mean, in your report or whatever. I understand the difference between continuous time and discreet time. They are different things. What you call visual, I mean, they fall into one of the previous two categories. The additional thing they have is that, as you say, you know, they pictorially represent what is going on. This is definitely a discreet time, discreet state, isn't it?

PROF. ALDEMIR: Sure.

CHAIRMAN APOSTOLAKIS: And the same applies to DFM?

PROF. ALDEMIR: Oh, yes, yes. I mean, dynamic flowgraphs.

CHAIRMAN APOSTOLAKIS: Yes, right.

PROF. ALDEMIR: GO-FLOW.

CHAIRMAN APOSTOLAKIS: Yes. I mean, all of these are one of the previous two groups.

PROF. ALDEMIR: Yes. The reason I grouped them differently, and -- well, dynamic flowgraph, GO-FLOW, Dynamic Fault Tree, Event Sequence Diagrams. Oh, sorry. We'll come to that.

CHAIRMAN APOSTOLAKIS: Oh.

PROF. ALDEMIR: The reason --

CHAIRMAN APOSTOLAKIS: But DYLAM is pictorial, too, is it not?

PROF. ALDEMIR: Not really, no. You don't have to come up with a visual outlay of system topology before you can start your model. These you have to.

CHAIRMAN APOSTOLAKIS: So what I would suggest is that you place them in the previous two categories as appropriate, and then you put an asterisk or something next to them and say these are also visual.

PROF. ALDEMIR: Okay.

CHAIRMAN APOSTOLAKIS: They have a visual component.

PROF. ALDEMIR: That's a good suggestion.

CHAIRMAN APOSTOLAKIS: Because it took me awhile to figure that out. I say why is he doing it that way?

PROF. ALDEMIR: Well, you know, if you really look --

CHAIRMAN APOSTOLAKIS: No, look, I understand.

PROF. ALDEMIR: But --

CHAIRMAN APOSTOLAKIS: Let's go on, because it's kind of late.

PROF. ALDEMIR: All right. Fine. Well, I put the disclaimer that this is only my brainchild. Nobody else is to blame and I take all the blame.

CHAIRMAN APOSTOLAKIS: Yes. The problem with these categorizations, Tunc, is that when you say "accuracy," when you say "ease," when you say "desirability," you have to have some quantitative measure because, you know, otherwise I don't know why you gave a 10 to ESD. I mean, what is that, you know, Event Sequence Diagram.

PROF. ALDEMIR: Well, I can explain that.

CHAIRMAN APOSTOLAKIS: But I don't even think it's a methodology. It's just a reliability block diagram.

PROF. ALDEMIR: No, no, not really.

CHAIRMAN APOSTOLAKIS: Oh, come on.

PROF. ALDEMIR: Not really. Not really.

CHAIRMAN APOSTOLAKIS: And where is the event tree approach? Do you have the event tree there?

PROF. ALDEMIR: The event tree is -- these are dynamic, these are dynamic. You have -- of course, the dynamic event tree is a whole bunch of them, DYLAM, DETAM, DDET, ADS and so forth, but event tree is not here.

CHAIRMAN APOSTOLAKIS: Why? I mean, I don't want to get in details over this. DFM gets a 3?

PROF. ALDEMIR: DFM gets a 3.

CHAIRMAN APOSTOLAKIS: Why?

PROF. ALDEMIR: I will explain. I will

explain that. I was going to pick a few and explain why I am giving these numbers and, as I said --

CHAIRMAN APOSTOLAKIS: But do you understand my problem with all this?

PROF. ALDEMIR: Not --

CHAIRMAN APOSTOLAKIS: You are not really giving us some objective criteria for the classification and I don't know why this is useful.

PROF. ALDEMIR: Okay. I cannot give you quantitative criteria.

CHAIRMAN APOSTOLAKIS: So why do you give me the data?

PROF. ALDEMIR: If somebody wants to have some idea of how difficult they are to use, how accurately they can represent system dynamics --

CHAIRMAN APOSTOLAKIS: What do you mean difficult? You don't have any difficulty there.

PROF. ALDEMIR: Ease of probabilistic model construction.

UNIDENTIFIED SPEAKER: The second column.

CHAIRMAN APOSTOLAKIS: But you know, this is meaningless, because maybe a methodology that is more involved and it's a bit more difficult has bigger benefits, too.

PROF. ALDEMIR: True. True. I mean, I'm

not --

CHAIRMAN APOSTOLAKIS: Where are the benefits?

PROF. ALDEMIR: Here, I mean, the benefits accuracy is the system representation of system dynamics.

CHAIRMAN APOSTOLAKIS: Oh, I'm sure Dr. Guarro will disagree on the 3 you gave DFM.

PROF. ALDEMIR: Yes. As I said, I will take the blame.

CHAIRMAN APOSTOLAKIS: He already, in fact, disagreed with it. He talked to me about it.

PROF. ALDEMIR: Well, these numbers are just --

CHAIRMAN APOSTOLAKIS: We're getting into terrible territory here but, you know, what can you do?

PROF. ALDEMIR: No, no.

CHAIRMAN APOSTOLAKIS: I mean, I'm familiar with the method.

PROF. ALDEMIR: No, the --

CHAIRMAN APOSTOLAKIS: I don't know why you gave it a 3.

PROF. ALDEMIR: I was --

CHAIRMAN APOSTOLAKIS: It seems to me it

is as accurate as anything else.

PROF. ALDEMIR: I don't know if we should get too technical here, but, you know, the process modeling is you go by large increments in changes in the process variables. So I am not sure how accurately you are modeling this process dynamic.

CHAIRMAN APOSTOLAKIS: Listen, Tunc. If I have a method that is very high level, okay, it will be accurate, because at a very high level it tells me that if this happens and the operators do this, you know, then that, it's very accurate, but it's almost useless, because it's very high level. Okay?

PROF. ALDEMIR: True.

CHAIRMAN APOSTOLAKIS: If I have a small LOCA and I don't have a high pressure injection and I don't have this and that, I'm in trouble. It's extremely accurate, but it's not useful. You have to go further down and say ah, what does it mean not to have high pressure injection? And you do fault trees, you do this and this and that.

Now, according to this classification, as I understand it, this second way of doing business would not be too accurate, whereas the first one is accurate, because it's a very high level.

PROF. ALDEMIR: No, no, no, not high

level, detail, system detail. How much --

CHAIRMAN APOSTOLAKIS: ESDs are high level.

PROF. ALDEMIR: ESDs.

CHAIRMAN APOSTOLAKIS: ESDs. Don't go into the puzzle.

PROF. ALDEMIR: Okay. I mean, I guess you may be right, but my understanding of it is that the transitions are from continuous event trees.

CHAIRMAN APOSTOLAKIS: But the ESD, the Event Sequence Diagram, is the way NASA is using them and the way they have been used in the nuclear industry. They just say you lost the system. Then you have the standby system. If it fails, you go over there. If it works, you go here. Then you have that. I mean, that's a high level sequence.

PROF. ALDEMIR: As you will see at the end, that's why we are not using it for benchmarking.

CHAIRMAN APOSTOLAKIS: But what --

PROF. ALDEMIR: There is no nuclear application.

CHAIRMAN APOSTOLAKIS: All I'm saying, Tunc, is --

PROF. ALDEMIR: We can change this.

CHAIRMAN APOSTOLAKIS: -- you are asking

for trouble with this table.

PROF. ALDEMIR: I agree.

CHAIRMAN APOSTOLAKIS: And I don't know how useful it is.

PROF. ALDEMIR: Okay. No problem. We'll get rid of the table.

CHAIRMAN APOSTOLAKIS: You understand?

PROF. ALDEMIR: Yes.

CHAIRMAN APOSTOLAKIS: Okay.

PROF. ALDEMIR: No problem, no problem.

CHAIRMAN APOSTOLAKIS: It's not that I disagree with everything you have there, but it's --

PROF. ALDEMIR: I understand.

CHAIRMAN APOSTOLAKIS: Anytime you do anything --

PROF. ALDEMIR: No sense in creating controversy. No, I understand.

MR. ARNDT: No, let me do it. The point was we're trying to go through all the different methodologies that are available or have been discussed in the literature and come up with some way of working through the ones that might be possible.

CHAIRMAN APOSTOLAKIS: I understand the intent.

MR. ARNDT: Okay.

PROF. ALDEMIR: I am using it as --

CHAIRMAN APOSTOLAKIS: I understand the intent.

PROF. ALDEMIR: I am using it as a rationale to chose methodologies.

CHAIRMAN APOSTOLAKIS: But you went too far.

PROF. ALDEMIR: Okay. Fine.

CHAIRMAN APOSTOLAKIS: You went too far.

PROF. ALDEMIR: Okay.

MR. KEMPER: If I could offer this. If there is any help that you can give us --

PROF. ALDEMIR: Yes.

MR. KEMPER: Because what he is trying to do here is to construct a screening criteria, right, to determine which are the one or two methodologies that we should pursue. So if there is anything that you can help us with on this, we would be more than happy.

CHAIRMAN APOSTOLAKIS: Okay. So this table I suggest deletion.

MR. KEMPER: Well, we need some screening criteria. I mean, without some objective --

CHAIRMAN APOSTOLAKIS: Well, it's not this or nothing. I mean, come on. He has looked at all these other things. He has arguments. He knows how they work.

PROF. ALDEMIR: But see, we have a little problem here, because we cannot communicate informally, right? That's one thing.

CHAIRMAN APOSTOLAKIS: Well, one way of doing this, if you really want to, is to poll people. I mean, you don't just give your view. You could have approached the actual developments of these and asked them to rank either their own method or the other guy's method.

PROF. ALDEMIR: That is a very good suggestion.

CHAIRMAN APOSTOLAKIS: Yes. That might have been more reasonable.

PROF. ALDEMIR: That's a very good suggestion.

CHAIRMAN APOSTOLAKIS: And you should have a range of things.

PROF. ALDEMIR: But do you agree with the metrics?

CHAIRMAN APOSTOLAKIS: Oh, I don't know. No, the benefit, where is the benefit? I said there has to be some benefit.

PROF. ALDEMIR: Oh, this is a benefit.

CHAIRMAN APOSTOLAKIS: I mean, certain methods are more complicated.

PROF. ALDEMIR: Accuracy is the system representation of system dynamics.

CHAIRMAN APOSTOLAKIS: I mean, I don't know. Is the theory of relativity complex? Yes, yes, but that's the only way of understanding a few things.

PROF. ALDEMIR: This is the benefit part. If you don't like the --

CHAIRMAN APOSTOLAKIS: Where is the benefit, the accuracy?

PROF. ALDEMIR: Accuracy, accuracy is the benefit.

CHAIRMAN APOSTOLAKIS: You would have to explain to me more or what do you mean by accuracy? Again, I tell you, if I stay at a high level I'm more accurate, but I'm not very useful. Benefit means, you know, somebody like NRR or whoever who wants to use it in doing something with it, is he going to find it useful? If you give him a very high level description of the system, that's not useful. It's a good starting point like, you know, small LOCA, high pressure injection. Yes, thank you very much. But there are many ways of achieving high pressure injection.

PROF. ALDEMIR: Well, you know, if there is any procedure where we can get comments from you, you know, without --

CHAIRMAN APOSTOLAKIS: This is the procedure.

PROF. ALDEMIR: Okay. Then can you give us metrics that I can use?

CHAIRMAN APOSTOLAKIS: Why do you want -- I don't understand, I mean.

PROF. ALDEMIR: As Bill said, we need screening criteria to justify the kind of methodologies we are going to use for benchmarking, which will come on later on.

CHAIRMAN APOSTOLAKIS: What are the objectives of your answers? Where do you want to go with this and then to evaluate these according to your objectives.

PROF. ALDEMIR: This is actually what we tried to do, because we actually want to go to the fault. We want to have accurate system and we want to have an accurate model. We want to have an easily constructed model. We want that model to integrate well with an existing PRA.

CHAIRMAN APOSTOLAKIS: Well, you already-- well, first of all, I mean, I am not supposed to solve your problem here, but you listed a number of possible problems very early on. Okay. Maybe you can start with those and ask yourself whether some of these methodologies could be helpful in addressing these unique issues that you raise.

PROF. ALDEMIR: That's in the second table, which you argued with again.

CHAIRMAN APOSTOLAKIS: And ask, you know, what are the needs of the Agency, right? Ask the NRR guy what does he want to know?

PROF. ALDEMIR: Okay. Yes.

CHAIRMAN APOSTOLAKIS: Okay. Right?

PROF. ALDEMIR: Okay.

CHAIRMAN APOSTOLAKIS: Like we know with standard PRAs we want to understand not only what the level of risk is, but also what are the dominant contributors. Okay. So a methodology that gives us a dominant contributor, is good enough. Right? So you know, think about it that way. I'm not saying it's a straightforward, simple problem, but this certainly invites --

PROF. ALDEMIR: No, you are right. But I mean, as I said, you know, this is what we could come up. Any suggestions are --

CHAIRMAN APOSTOLAKIS: Because if I look

at this now, I know, for example, that later on, because I listened to you at the ANS meeting, you are proposing to compare DFM with something else. If I look at this table, I wouldn't chose DFM.

PROF. ALDEMIR: But this is not the complete picture, because --

CHAIRMAN APOSTOLAKIS: It gets a 3, a 5, a 7 and a 7.

PROF. ALDEMIR: Wait until -- oh, sorry, I don't have it here. But this is conditional. This is only for the process side.

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: It does not include the digital aspects. There is another table there, which tries to combine both.

CHAIRMAN APOSTOLAKIS: I see.

PROF. ALDEMIR: So this --

CHAIRMAN APOSTOLAKIS: But why is ease of modeling a factor?

PROF. ALDEMIR: Well, because --

CHAIRMAN APOSTOLAKIS: I mean, if it's a complex problem --

PROF. ALDEMIR: True.

CHAIRMAN APOSTOLAKIS: -- even the methodology would be false.

PROF. ALDEMIR: True. But if it is so complex that you need a four year degree, I mean, a four year program to learn it, then it's not going to be very useful to a lot of people.

CHAIRMAN APOSTOLAKIS: But it shouldn't be up there at the same level as the accuracy.

PROF. ALDEMIR: Fine.

CHAIRMAN APOSTOLAKIS: What we defined as accuracy.

PROF. ALDEMIR: I mean, as I said, any suggestions are welcome.

CHAIRMAN APOSTOLAKIS: And if I have two methodologies and one is very accurate and the other is not so accurate, but it's easier to use, then I can see how you can go with that one. But to say accuracy and ease of use are the same benefit, I mean --

PROF. ALDEMIR: Fine. We can change the metrics in any way that --

CHAIRMAN APOSTOLAKIS: Anyway, I think you get the message.

UNIDENTIFIED SPEAKER: Yes, I think so.

PROF. ALDEMIR: Yes. Okay. Now, the Type II interactions. Again, these --

CHAIRMAN APOSTOLAKIS: Type II now is within the --

PROF. ALDEMIR: Within the system. Markov Models, and when I say Markov Models, you know, I'm not going to spend too much time on these, because we I think discussed this at some length yesterday, and when I refer to Markov Model, I only refer to Barry Johnson's model, because there are others.

There are basic methodologies. The Markov Models, and again this has been discussed, so I'm not going to talk about it, Bayesian methodologies. The one that we looked at in detail is by my colleague from MIT.

CHAIRMAN APOSTOLAKIS: Again, why is that a dynamic methodology? I mean, poor Bayes is not dynamic.

PROF. ALDEMIR: It is dynamic in the sense that your model is being updated as you get new information.

CHAIRMAN APOSTOLAKIS: But that's not what you meant by dynamic earlier. Dynamic, you said interactions with a physical process, I mean.

PROF. ALDEMIR: It is taking into -- well, this is Type II within the system not physical process. This is Type II. So, Barry Johnson, sorry. My colleague's methodologies are Golay's Bayesian update method and it has got a lot of assumptions and part of which is that software is being developed. It's not really applicable to -- let me get their information on this. It's not really applicable to existing software. The number of paths, possible paths within the system, has to be estimated. You are assuming a lot of -- making a lot of assumptions.

CHAIRMAN APOSTOLAKIS: The University of Maryland --

PROF. ALDEMIR: Pardon me?

CHAIRMAN APOSTOLAKIS: The University of Maryland yesterday told us that they also want to know that, the number of paths.

PROF. ALDEMIR: Yes, yes, yes, right. You are making assumptions on the choice of the priors. You are rejecting some execution paths, but you don't really know whether you should have looked at them or not.

CHAIRMAN APOSTOLAKIS: That's fine, that's fine.

PROF. ALDEMIR: Okay. So dynamic flowgraph methodology is, as you will see later on, the best one, in fact, compared with earlier what I said, everything combined. It turns out to be the best one. The only restriction we could find out, and that comes to what Professor Apostolakis was referring to earlier, why we ranked it low, is because it is making certain assumptions on how to model the process.

And, for example, level change, high level change, low level change, medium level change and kind of qualitative descriptions. It's based on digraphs, which are qualitative in nature, and that is where 3 is coming from actually. So you don't know.

Now, if you talk to the method developers, then they tell you that sure, I can take 10, 15 levels, 100 levels, but the model becomes very complicated.

CHAIRMAN APOSTOLAKIS: True.

PROF. ALDEMIR: True. There is a self-check mechanism. But the thing that we were looking at, at this point, is how they have been used in the literature, not speculate on how they could have been used. So if you look at what has been out there, which is a NUREG on a feed water control system, the system dynamics are qualitative.

CHAIRMAN APOSTOLAKIS: That's not on the table.

PROF. ALDEMIR: Right, right. But the reason I mention NUREG, because this is an NRC-related meeting. That's why. So I mean, there is a NUREG.

That's the point. But you know, that is the reason why 3, not necessarily because of the inherent limitations of the methodology. Petri nets.

CHAIRMAN APOSTOLAKIS: The analysis of the reactor at Sandia, I thought, was pretty interesting that Chris Garrett did. You have that paper.

PROF. ALDEMIR: I don't have it.

CHAIRMAN APOSTOLAKIS: Where he found, in fact, a fault in the software.

PROF. ALDEMIR: I don't have that. Which one are you talking about, this one that was more recently published?

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: Oh, the reliability and system safety?

CHAIRMAN APOSTOLAKIS: I believe so, yes, where he found that there was a denominator, k minus 1.

PROF. ALDEMIR: Right.

CHAIRMAN APOSTOLAKIS: In the program.

PROF. ALDEMIR: Right, but that was -- oh, okay.

CHAIRMAN APOSTOLAKIS: Yes, he found it.

PROF. ALDEMIR: No, no, I don't mean that. I mean --

CHAIRMAN APOSTOLAKIS: He went to the developer and the developer, first of all, was shocked that he was there and, second, he said, which is related to what you guys were saying yesterday --

PROF. ALDEMIR: Right.

CHAIRMAN APOSTOLAKIS: He said but there will never be a situation where k is 1. But the interesting thing is -- do you have that paper?

PROF. ALDEMIR: Yes, yes, I have that paper. I have the paper. Let's see, Petri nets.

CHAIRMAN APOSTOLAKIS: In fact, that could be one of your criteria. Has the method under scrutiny ever been used in a case study and has it identified anything?

PROF. ALDEMIR: Well, we tried. We did actually try to do that. That's the only reason why, as I said, we are using -- you will see. We will zero in on two methodologies and that's the only reason why we're doing that, because it has been implemented.

CHAIRMAN APOSTOLAKIS: I'm trying to help.

PROF. ALDEMIR: No, I understand, I understand. Okay. Petri nets.

CHAIRMAN APOSTOLAKIS: It may not go, but the motivation is there.

PROF. ALDEMIR: That's all right. Petri

nets. Again, you know, they seem to do a very good job within Type II interactions, but I am not too sure how well they model Type I interactions, and then I will have a complete table later on with a different ranking.

Test-based approaches, as the name implies, is just test-based, so then there are all sorts of issue, you know, how do you select your test cases and the system must be mostly complete. Testing is a value-added activity. It shows presence, but not the absence of error. Test cases may not be rigorous enough to exercise the system to predict accurately its reliability and, of course, they don't model Type I interactions, which is interactions with the process. Black-box models are the type of models --

CHAIRMAN APOSTOLAKIS: I don't see the word black-box. Oh, down there. So you skipped the software metric?

PROF. ALDEMIR: We discussed this yesterday at great length.

CHAIRMAN APOSTOLAKIS: But what do you think?

PROF. ALDEMIR: I mean --

CHAIRMAN APOSTOLAKIS: Black-box.

PROF. ALDEMIR: Because it's going to

start anew.

CHAIRMAN APOSTOLAKIS: Well, let me ask you this. I see these others without necessarily agreeing with them, but I see them as, you know, taking a piece of software and doing something to it. Is the software metric approach doing the same thing or is it more generic?

PROF. ALDEMIR: My opinion is that it is generic but, you know, the rankings and so forth, the choices are by our computer science people, who felt more qualified. Their impression of metric-based approaches is that -- I mean, if you want me to mention the kind of things that they had problems with, measured the software development process, but not the end result of the process.

It has yet to be shown that this method can scale to high reliability requirements with a large system, which they claimed yesterday it does. The metrics chosen are based on expert opinion and may change as new metrics are discovered and, of course, does not model Type I interactions.

CHAIRMAN APOSTOLAKIS: So what is this Schneidewind?

PROF. ALDEMIR: Schneidewind Model. Well, it's a black-box model and the name implies they treat it as a black-box. They chose -- NASA used it for modeling one of the missions. And it has got -- it uses a non-homogenous Poisson process as the basis to predict the reliability of software components, assumes that the software system is changed only when there is an observable failure, failure data needed for quantification, but may not be available, because they have the data on the shuttle system, needs mechanism to select cases, test times and reword criteria. In other words, there is no justification of what's being done, and it has been only implemented on software. So again, you know, it does not model the complete system.

CHAIRMAN APOSTOLAKIS: Okay.

PROF. ALDEMIR: So we tried to come up with --

CHAIRMAN APOSTOLAKIS: So you do have. Why are you asking me then? You do have your criteria here.

PROF. ALDEMIR: These are requirements. Okay. We tried to go through a screening process to gradually reduce, so we went through a screening of Type I interactions. We went through a screening of Type II interactions. And then we did a screening of both. And then we tried to come up with requirements.

So if you want me to use them as metrics, that's fine.

CHAIRMAN APOSTOLAKIS: I think this is the ones --

PROF. ALDEMIR: Great.

CHAIRMAN APOSTOLAKIS: -- that you should be using and No. 3 is the most important of them all.

PROF. ALDEMIR: Yes, no problem.

CHAIRMAN APOSTOLAKIS: No problem.

PROF. ALDEMIR: So I don't know. Well, I'll just go through them fast. The model must be able to predict future failures well. The reason I mention it is because there are models based on existing performance and they are not necessarily all that great, because you don't know if you have covered everything. And there are models that people have based on neural nets, for example, which are based on totally the operation of data, which is not very practical to predict future events.

The model must account for the relevant features of the system under consideration. You must be able to model all types of complex interactions that are taking within the system. Also, you need to worry about if you are omitting things by using assumptions. So you have to make sure that your assumptions are reflecting the true operation of the system, which ties up with 3.

This we discussed in great length. The model must be able to represent dependencies. No. 5, desirable feature. It must not be hard to learn. No. 6, data used in the quantification process must be credible to a significant --

CHAIRMAN APOSTOLAKIS: Oh, you have more?

PROF. ALDEMIR: I have 11. You must be able to differentiate between a state that fails one safety check and that those that fail multiple ones, must be able to differentiate between faults that cause function failures and intermittent failures, must have the ability to provide relevant information to the users and that has to do with the -- one of our internal reviewers argued with that, for example, that Monte Carlo methodology does precisely the same, but the intention here is that it provides you information that you can use to integrate the results into a full PRA like cut sets and so forth.

And talking about integration, when you integrate this system, this model into the full PRA, it must be able to match with the rest. For example, like a Markov Model, you need a lot of detailed system information, which the fault tree is not going to give you. By the same token, you have to extract the information out of the Markov Model to put into the PRA. But you can do that even qualitatively using graph theoretical methods, so you can get qualitative information out of Markov Models.

This kind of goes with 10. Models should not require highly time-dependent or continuous plant state information. So if you think that these are good metrics, we can use them.

CHAIRMAN APOSTOLAKIS: I think they are pretty good, but I'm wondering why the previous speaker didn't use something like this. Todd? I mean, shouldn't you have some list of requirements, as well, in the development of your models?

These are not unique to time-dependent, I mean, dynamic methodologies that Professor Aldemir is talking about. They are general requirements, except the last one, for any model, so it seems to me since both of you are part of the NRC, you should have a common set of requirements, should you not? Maybe you should increase the number of telephone calls.

MR. HILSMEIER: That's a very good idea.

CHAIRMAN APOSTOLAKIS: Now, honestly, Todd, is this the first time you've seen this?

MR. ARNDT: We have shared our graphs with Todd.

CHAIRMAN APOSTOLAKIS: Just about. No, but, I mean, I would expect, I mean, you know, you have the two approaches that Steve has talked about, but a lot of the elements are common. And one is the requirements for what you are trying to develop, and all the methodologies that Tunc mentioned, he just about exhausted everything. I mean, so I don't see why they don't apply to you.

Now, you can reject some of these for obvious reasons like the continuous event tree and say my God, this is too much for me, because I'm dealing with this problem, which is perfectly all right. This is good. So I would expect to see a little closer collaboration.

PROF. ALDEMIR: Another table.

CHAIRMAN APOSTOLAKIS: Now, wait, wait, wait.

PROF. ALDEMIR: Okay.

CHAIRMAN APOSTOLAKIS: Where are you setting as a requirement that the model should be capable or at least have a promise of handling certain things that we have observed, such as the sequencer issues that Mr. Waterman mentioned yesterday?

PROF. ALDEMIR: Well, that is implicit in 4, of course.

CHAIRMAN APOSTOLAKIS: In where?

PROF. ALDEMIR: In 4. Model must be able to represent dependencies between failure events accurately and quantitatively.

CHAIRMAN APOSTOLAKIS: I don't know. Classify what you told us yesterday, Mike, as a failure, I mean, as being one of dependencies. I don't think so.

MR. ARNDT: Yes. It's basically, the way Tunc defined it is, a Type II dependency. The issue is, and we could probably define it better, but it's a design fault associated with the interaction between two parts of the software.

MR. WATERMAN: No, I think that's a Type I failure. You don't know the failure exists until you get some kind of Type I demand that it performed. That's why they ran on and on and on and didn't realize they didn't have HPI about 30 percent of the time, because they didn't have any external event that said hey, work for me and then the software said I'm not going to do that. So I think that's kind of a Type I event. You don't know the failure exists.

CHAIRMAN APOSTOLAKIS: Yes. In any case, I think it's this kind of experience.

MR. WATERMAN: Yes.

CHAIRMAN APOSTOLAKIS: I mean, the impression I get from you guys, both teams, is that there is precious little out there regarding nuclear experience. At least, you know, if you can say okay, I know these four incidents.

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Does this methodology have any chance of modeling?

MR. ARNDT: That coupled both in with, as Tunc mentioned, the ability to represent dependencies, what we probably should do, and when tested gets accurate results on the examples that we actually have.

PROF. ALDEMIR: Oh, oh, we should put that as the 12^{th} requirement that compare actually.

CHAIRMAN APOSTOLAKIS: Does it have any chance of modeling the existing operating experience?

PROF. ALDEMIR: You know, it is implicit in here, but --

CHAIRMAN APOSTOLAKIS: A catchall.

PROF. ALDEMIR: In other words, what I meant, implicitly meant with 1, also includes that future failure, as well, because if something comes up, we should be able and once something comes up, literally happens, we should be able to model it. So it is implicit in there, but maybe we should make it more explicit.

CHAIRMAN APOSTOLAKIS: I would rather do what you just said, make it 12.

PROF. ALDEMIR: Okay. Make it 12.

CHAIRMAN APOSTOLAKIS: And use explicitly the words operating experience.

PROF. ALDEMIR: Fine.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: To show that you are fully aware of it.

PROF. ALDEMIR: Well, I'll take notes.

MR. ARNDT: We'll get it from the transcript.

PROF. ALDEMIR: The transcript. Okay. Good.

MR. ARNDT: Something on the order of ability to integrate operational experience.

PROF. ALDEMIR: Okay. That's good. Can I go on?

CHAIRMAN APOSTOLAKIS: Yes, please.

PROF. ALDEMIR: Another table. Now, here, why I'm doing what you just said I should do in the first place, but I am doing it myself and not giving numbers in this situation.

CHAIRMAN APOSTOLAKIS: This is progress, saying X and O is really progress versus --

PROF. ALDEMIR: And lots of question marks, as you see.

CHAIRMAN APOSTOLAKIS: -- 1, 2, 3, 4, 5.

PROF. ALDEMIR: No, you are right. I mean, this was done for our internal screening purposes. We put it there and we were invited to come.

CHAIRMAN APOSTOLAKIS: Also, these are the 11 requirements?

MR. ARNDT: Yes.

PROF. ALDEMIR: Yes.

CHAIRMAN APOSTOLAKIS: Oh, well, that's much better, Tunc.

PROF. ALDEMIR: As I said, we have done it, but again this is my personal opinion. Again, I don't want anybody to jump on anybody else, because this is what I thought is the case.

CHAIRMAN APOSTOLAKIS: We will only jump on you.

PROF. ALDEMIR: But you are right in the sense that we should test this and that's, I guess, one of the reasons why we have this meeting in the first place, to have input. We should test it. We should send it out as a survey to the developers, to all the stakeholders, so to speak.

CHAIRMAN APOSTOLAKIS: This one.

PROF. ALDEMIR: This one, right. And we have comments from some of the reviewers, internal reviewers, on this, for example, and it got revised actually. Now, I don't want to go through this again.

CHAIRMAN APOSTOLAKIS: That's okay.

PROF. ALDEMIR: But if you want, I can give you some justification. For example, let's take DFM. DFM, you see no zeros here.

CHAIRMAN APOSTOLAKIS: What is 4? What is 4?

PROF. ALDEMIR: 4 is capable to what I just said earlier and then we have this.

CHAIRMAN APOSTOLAKIS: So it is not " It is not hard for an analyst to learn."

PROF. ALDEMIR: No, no, it is the --

CHAIRMAN APOSTOLAKIS: "Must be able to represent dependencies."

PROF. ALDEMIR: Dependencies.

CHAIRMAN APOSTOLAKIS: Yes, I think there's a question mark there. You are right.

PROF. ALDEMIR: I mean, right, you will see that that's one where we are going. I mean, that's what we are aiming at. We're going to test it.

CHAIRMAN APOSTOLAKIS: And then 6, "The data used must be credible."

PROF. ALDEMIR: None of them has that. None of them has credible data.

CHAIRMAN APOSTOLAKIS: Yes, everybody has a question.

PROF. ALDEMIR: Right, right, nobody.

CHAIRMAN APOSTOLAKIS: And then what else do you have? 8. What is 8? "The model must be able to differentiate between faults that cause function failures and intermittent failures." I don't know what that means, but I guess you are right.

PROF. ALDEMIR: Well, I can go into that.

MR. ARNDT: Take yes for an answer.

CHAIRMAN APOSTOLAKIS: No, that's fine. Move on.

PROF. ALDEMIR: Okay. But you see, what I'm trying to get at is that whenever there is an internal, initial, not internal, initial screening first and then try to combine both, there is an implicit screening for the others, but I didn't show that. And then I didn't make a table.

CHAIRMAN APOSTOLAKIS: Tunc, as you know, even if you send this out, it's like any new field.

Most of the developers of these methodologies have not used somebody else's methodology, so they really cannot pass judgment. They have some idea.

PROF. ALDEMIR: That is a good point.

CHAIRMAN APOSTOLAKIS: They have some idea like you organized this workshop in Turkey years ago. Okay. People listen to other people and so on, but they haven't really tried it. They haven't really. You know, so they are very familiar with their own methodology, but not with other people's approach.

PROF. ALDEMIR: I doubt that this is the proper forum, but as you well know, Ohio State is part of the University Consortium to help Idaho National Lab to conduct research towards future reactors, and our task is as instrumentation control and PRA. So as the first task of this academic center of -- and there are academic centers of excellence established at each five universities.

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: Our first task, we were planning to organize a workshop on dynamic methodologies in PRA.

CHAIRMAN APOSTOLAKIS: That's not what --

PROF. ALDEMIR: No. The reason I mention that, do you think it's a good idea to use this as a forum to get opinions?

CHAIRMAN APOSTOLAKIS: I think the best way to do what I said is through benchmark exercises where people are forced to use somebody else's model to actually do real work, but these tend to be expensive.

PROF. ALDEMIR: That's exactly right.

CHAIRMAN APOSTOLAKIS: And you have a large number of methods here.

PROF. ALDEMIR: That's right. So we have to screen. That's the whole problem.

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: We have to screen.

CHAIRMAN APOSTOLAKIS: But you see, the biggest problem with workshops or anything else is people just don't listen to others.

PROF. ALDEMIR: Well, we saw that in Turkey.

CHAIRMAN APOSTOLAKIS: You don't have to go so far to see it.

PROF. ALDEMIR: No, I don't mean that. I mean the workshop. I am trying to explain.

MR. ARNDT: You can go to an ACRS meeting, people not listening to you.

PROF. ALDEMIR: Excluding present company.

CHAIRMAN APOSTOLAKIS: No, I'm serious, and this is true everywhere. I mean, that's why in the beginning there is chaos. Take PRA, you know, in the '70s and '80s. There is no classical statistics. There is classical-based. Classical now in the year of 2005, you realize that there hasn't been a single PRA done in a classical way. So at this point you say well, maybe then they are right, okay, but that's the way it is.

PROF. ALDEMIR: Well, we tried to then do the screening, because it's expensive to benchmark everything.

CHAIRMAN APOSTOLAKIS: I don't see anywhere though you saying I'm going to look at the basic assumptions behind these things and make a judgment myself whether these assumptions are sound. I think you should do that.

PROF. ALDEMIR: Well, it is, of course, implicit in those tables. I mean, what I say are you modeling the process, it's implicit in that. If the assumptions are too restrictive, you are not modeling it correctly.

CHAIRMAN APOSTOLAKIS: But I would also come to my favorite theme of the last two days. Markov approach, fundamental assumption, cost and transition rate from this state to that state. It's not justified.

PROF. ALDEMIR: Let me say a few words on that. Okay. Let me go through this and then I'll come back to Markov and then say a few things.

CHAIRMAN APOSTOLAKIS: And I think GO-FLOW is --

PROF. ALDEMIR: Actually as good as Petri nets, actually as good as --

CHAIRMAN APOSTOLAKIS: Which tells me a lot.

PROF. ALDEMIR: As good as -- you know, the reason -- what?

MR. ARNDT: Just to go to that slide.

PROF. ALDEMIR: Well, okay. When we ranked these things, we found out that, again, purely subjective basis, because there is no real benchmarking, but dynamic flowgraph methodology, that's the one that we found, let's put it this way, least objectionable with the least restrictions, least number of assumptions.

CHAIRMAN APOSTOLAKIS: But let me also add something here, because other people may not remember. All these approaches, not all but certainly the DFM, it doesn't give you any probabilities. It just gives you failure modes, sequences that lead to failure. This is very important, because Steve also yesterday, every time I pushed him hard, he said oh, but there's always benefit here because we understand the structure of the model. I think most of these models help you do that.

MR. ARNDT: Yes, they do.

PROF. ALDEMIR: All of them.

CHAIRMAN APOSTOLAKIS: But some of them do not claim that they produce probabilities. There is a good reason for that. The developers were modest people.

PROF. ALDEMIR: Well, okay. Let me go through this and I will come back to Markov and say a few words.

CHAIRMAN APOSTOLAKIS: Okay.

PROF. ALDEMIR: Because to respond to some of the comments that were made yesterday. Dynamic flowgraph methodology we found has the least. The only thing that we could see in the dynamic flowgraph is this potentially not describing the system process or the process dynamics correctly and if you don't do it correctly, as I will show you in a little while, you may be missing sequences. Also, you may be coming up with the wrong numbers if you are going to quantify it.

Now, the second choice, although Professor Apostolakis may not agree, is the Markov approach. Maybe this is the time. The Markov approach. Again, one of the important reasons why we zeroed in on these two is because there are applications in the literature on systems that pertain to nuclear systems. Markov has that. Dynamic flowgraph methodology has that.

Now, Markov, as was mentioned yesterday, maybe it's the right time, has to work with numbers, but not necessarily so. If you want to extract qualitative information out of the system, you can look at the -- you can regard the lambdas as placeholders. You can use a search, graph theoretic search scheme through the matrix, transition matrix, and you can come up with very a well-defined, very detailed scenario as to how the accident progresses.

Now, there is no machinery to do that automatically, I agree, but it can be done. So you can get qualitative information. That's one. The other thing is that even if the numbers are wrong, you can do, of course, sensitivity analysis.

CHAIRMAN APOSTOLAKIS: But the question is how do you transition from one state to the other?

The assumption there is independently of the number is that there is a constant rate of --

PROF. ALDEMIR: No, no, no.

CHAIRMAN APOSTOLAKIS: But I'm saying that there is.

PROF. ALDEMIR: No constant, no assumption on constant rate.

CHAIRMAN APOSTOLAKIS: I mean, if there is a design error, I don't know why I would transition from one state to the other. There is a design error, for heaven's sakes. If the conditions are there, it will never work, because it's wrong. That's where I have a problem. With the Markov I go there, I come back, I go there, I come back.

PROF. ALDEMIR: What you are saying is that the transition is dependent upon the initial conditions.

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: Right.

CHAIRMAN APOSTOLAKIS: I mean, the fundamental assumption is that I can go from one state to another. And what I keep hearing from the experts, who have experience with these things, is that the specification error is a requirement there. So if the damn thing doesn't work under these conditions in one case, it will never work, because it's wrong and Markov doesn't allow that. Now, don't tell me about semi-Markov, I mean, come on.

PROF. ALDEMIR: Well, no, but I will come to something else, you know.

CHAIRMAN APOSTOLAKIS: This is my problem.

PROF. ALDEMIR: No, that is a valid assumption, I mean, not assumption, valid statement, but let me say something about the failure rate. Constant failure rate or non-constant failure rate is no problem, because if there is --

CHAIRMAN APOSTOLAKIS: Well, yes, but there are still transitions though.

PROF. ALDEMIR: Well, I mean, if you assume that the concept of a transition, constancy or non-constancy is no problem, it can be taken care of.

CHAIRMAN APOSTOLAKIS: Absolutely.

PROF. ALDEMIR: The other thing, and it is not by the way, it is not a bad assumption. If you are basing your failure data on the field data and on a maintained system, it is not a bad idea to use constant failure rates.

CHAIRMAN APOSTOLAKIS: I can't think of a single incident from the ones that Mike described yesterday, others that I have seen, this Canadian reactor, the Bruce reactor where they had a problem a number of years ago, where it was a matter of transition. It was wrong and the right conditions were created and the error came to the surface. It was a design error or specification, if you wish, or whatever that was dormant until the right conditions were created.

Now, I can't see for the life of me any Markov approach dealing with that. We need something new, something fresh and I don't know what that is. If you ask me, I don't know. I'm sorry, I don't know, but I'm not going to go with the wrong approach just because I don't know.

PROF. ALDEMIR: I mean, what I am trying to say is that if there is a transition possible, whether it is due to the software failure, so to speak, or whether because the software was designed wrong and the initial conditions prompted that transition, as long as there is a transition, that's okay.

CHAIRMAN APOSTOLAKIS: I understand that, yes.

PROF. ALDEMIR: That's fine.

CHAIRMAN APOSTOLAKIS: Yes, if it's a transition.

PROF. ALDEMIR: I mean, that is my system topology. That is my system topology.

CHAIRMAN APOSTOLAKIS: My problem is that I don't see very many cases where there is a transition, so you and I and others have to eventually convince ourselves that, you know, under certain conditions perhaps it's okay, under others it's not. But the big issue now in front of us, and I don't think you should feel responsible that you can solve it.

PROF. ALDEMIR: No, no.

CHAIRMAN APOSTOLAKIS: This is a real issue.

PROF. ALDEMIR: Yes.

CHAIRMAN APOSTOLAKIS: I mean, this is a new issue.

PROF. ALDEMIR: No, all I am trying to see is, first of all, you know, you need a couple of methodologies, as you said, to kind of look at what is available, what are their weak points and their strong points.

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: And when looking at available methodologies, what we are seeing is that these are the two most promising. The others don't rank as high. That's why we are using them.

CHAIRMAN APOSTOLAKIS: You know, I explained to somebody, but maybe I should say it again, just a little lecture here.

One of the labors of Hercules was to capture and kill a bandit who was between Athens and Corinth. His name was Procrustes. I will tell you how you spell that later. What he did, he would grab travelers, at that time, you know, by walking or whatever, rob them and then he had a bed. He would stretch them out on the bed.

If they were shorter than the bed, he would stretch them to fit the bed and, of course, they died. If they were taller than the bed, he would cut off pieces of them until they fit the bed. And from that a saying came about, which is much better known in Greek, but in English, too, I just seen it, the Procrustean bed.

All these people who are taking existing methods from reliability and put them on software are using the Procrustean bed. They are taking something that doesn't fit the bed and either they stretch it or they cut it off until it fits the bed, and that is not an approach, an acceptable approach anyway and as Hercules demonstrated.

PROF. ALDEMIR: Well, I mean, I agree with you, of course. There is nothing to disagree but, you know, we have to do -- either we do nothing or we do something.

CHAIRMAN APOSTOLAKIS: Correct, something, correct.

PROF. ALDEMIR: If we are -- and if we have to have time constraints, we have to do something fast. We have to use available stuff.

CHAIRMAN APOSTOLAKIS: Listen. It cannot be a Procrustean bed. You have to do something. I agree. But remember Procrustes and what happened to him. So let's go. Don't feel that you have to do something --

PROF. ALDEMIR: No.

CHAIRMAN APOSTOLAKIS: -- even if it's wrong.

PROF. ALDEMIR: But I can make the same arguments about all the other, for example, common cause failure models.

CHAIRMAN APOSTOLAKIS: No, they are not like that. Come on. They are not. They are crude, but they are not wrong. There is a big difference, a big difference.

PROF. ALDEMIR: Okay. So --

CHAIRMAN APOSTOLAKIS: So where are you now, Slide 19?

PROF. ALDEMIR: Slide 19 and, basically, the model story of this Slide 19 is that the top two ranking ones are dynamic flow methodologies.

CHAIRMAN APOSTOLAKIS: I see you have an example later.

PROF. ALDEMIR: I will come to that.

CHAIRMAN APOSTOLAKIS: Maybe the Subcommittee is interested more in that. We keep seeing acceptance criteria and they more or less repeat themselves, don't they?

PROF. ALDEMIR: Acceptance criteria. By the way, we are defining it in a slightly different way.

CHAIRMAN APOSTOLAKIS: I understand that, but, I mean, you have already stated your position.

PROF. ALDEMIR: Yes, right. Okay.

CHAIRMAN APOSTOLAKIS: So I'm asking you whether it would be worthwhile going to Slide 22.

PROF. ALDEMIR: Okay.

CHAIRMAN APOSTOLAKIS: Do you think you are skipping something that's very important? It's late in the day.

PROF. ALDEMIR: Not really, because I

stated, like you said, I stated most of them. I am trying to condense them, basically, from 11 to 7. That's all there is to it.

CHAIRMAN APOSTOLAKIS: 22.

PROF. ALDEMIR: Now, what I am trying to show you here is how the process couples failure events or, actually, stochastic and it demands events that may take place on demand. So what we have here is, I guess, a real system from a BWR/6 and this is supposed to provide core cooling in case the RCIS, the reactor core insolation cooling system, becomes incapacitated.

And I'm not going to go through the system description in detail, because I'm sure everybody is more familiar with it than I am. But the key point is that there is a high pressure core spray system consisting of many components, and there are three sets of safety relief valves. What we will try to do is to just concentrate on one of them.

So the incident that we have in mind is the following. There is a small break which incapacitates the RCIC system. In this situation it so happens that the enthalpy lost through the break is larger than the enthalpy addition due to decay heat. So the level goes down, pressure goes up. So you can get the HPCS pump started through two signals, either the first low level signal or the high radiation signal in the containment.

The HPS pump starts, but nothing happens, at this point, until the level hits the low, low mark, I think it's the second low mark, in which case the injection valve opens and water is sprayed, so the level starts. In the meantime, of course, it reduces the pressure a little bit, but not sufficiently, so you may need to -- the SRV, which is pressure-activated, SRV 1, safety relief valve 1, opens and it relieves pressure, so the level comes -- it starts spraying water, the level starts going up.

When you hit the high pressure mark, this valve closes, pump doesn't stop, keeps circulating water heat through the jockey pump. And when the pressure comes down, the set point and the safety valve closes, so you feed, you try to cool the core through a feed/bleed cooling mode.

Now, it is desirable, I have been told, to operate like this with using one SRV, because it takes less time to start up the reactor again in the future. So the top events that we defined -- oh, before I go into that. The system, as you see, is very complex.

CHAIRMAN APOSTOLAKIS: This is not

software.

PROF. ALDEMIR: No.

CHAIRMAN APOSTOLAKIS: This is just Type I dynamic.

PROF. ALDEMIR: No, Type I, Type I interaction. There is no example of Type II interactions, none in the literature that we have seen.

CHAIRMAN APOSTOLAKIS: So you will consider software here in Type I interactions?

MR. ARNDT: This is just an illustration. Go ahead.

PROF. ALDEMIR: An illustration of how Type I interactions tie up, coupled failure events. Type II, there are two effects of the digital aspects. One of them is the closer communication between the devices, which makes the Type I coupling much worse than this one and two on top of that, you have Type II coupling or Type II there. There is no model. There is no application of Type II interactions, so that's why I'm showing this one.

So you try to control the water, I mean, cool the reactor through feed/bleed cooling mode and although this is a complex system, as you see, for modeling purposes we can make it simpler. This comes to the one-input, one-output model that I was talking about, even if it's a digital controller inside. As long as they are within the shaded area, I can regard it as a single controlled, single structural unit or micro component, which is what I'm doing in the next picture.

And since I am using one safety relief valve, I am regarding it as a single component, in spite of its intricate construction. Either I have data or I'm modeling it through conventional techniques to get failure data. So this is how it looks for modeling purposes. Then these are the set points and we are talking about -- okay, sorry. Let me go back here.

We are talking about four set points. Either I go below a certain level or go above a certain level, sorry, high level, low level possible failure mechanisms and the high pressure/low pressure. Now, these don't have safety implications obviously. What the low level signal will do is it initiates the RPCS system, but the point is that it will affect the demand frequency of the RPCS.

So although this is not a safety-related issue, it has safety implications from a PRA viewpoint, because if you do a PRA, you are going to change the demand frequency on the RPCS. And again, the pressure, of course, you know, if SRV 1 does not respond, then you have the other SRVs and you can go for manual operation and so forth.

So the incident that we had here, I looked at, is a 1 percent double-ended guillotine break. Pressure reaches whatever in two minutes following the loss of --

CHAIRMAN APOSTOLAKIS: What do you mean by 1 percent?

PROF. ALDEMIR: Of area.

CHAIRMAN APOSTOLAKIS: So double-ended at the largest pipe and you are considering 1 percent of that?

PROF. ALDEMIR: No, no, we are talking about a small, small break here, small instrumentation break.

CHAIRMAN APOSTOLAKIS: I don't know. What does --

DR. BONACA: You mean 1 percent of the double-ended --

CHAIRMAN APOSTOLAKIS: If the largest pipe has an area A, you are considering a pipe that has area 1 percent of that?

PROF. ALDEMIR: Yes.

CHAIRMAN APOSTOLAKIS: And that breaks?

PROF. ALDEMIR: That's right.

CHAIRMAN APOSTOLAKIS: Okay.

PROF. ALDEMIR: Level reaches whatever in two minutes following the LOCA, so these are your initial conditions and we're assuming that the major contributor to the HPCS failure is the failure of the injection valve.

Now, this is the results of the analysis using the cell-to-cell mapping technique. I don't know if I should read this through, but the point is that the failure mode of the system depends very much on the exact timing of the failures and exact location of the system variables at the time of the failure. That's what comes out of this picture.

CHAIRMAN APOSTOLAKIS: Give us an example of the exact time.

PROF. ALDEMIR: Examples. Low level, which is minus 148 inches, occurs. If only HPCS fails or only SU2, which is the SRV, fails to open. High level occurs if SU2 fails closed after SU1 fails after.

CHAIRMAN APOSTOLAKIS: After?

PROF. ALDEMIR: After. So high pressure occurs if the level at the time of the SRV failure is such that it takes longer for the level to reach the low level point, 100 minus 148 inches, than the time it takes for the pressure to reach 1110 psi. And there are two other examples how this exact timing is important at the time of failure. This was a study we did a long time ago. It has been now, what, 15 years.

CHAIRMAN APOSTOLAKIS: But you know how the event tree guys would model this if they realized it. They would have SU1 fails. Well, that's easy. Yes, SU1 fails and then ask does SU2 fail afterwards? Put it on the right of the event tree and then you would have a number of consequences. If they put it on the left, you have another kind.

I mean, there are good ways of doing these things and, as you know, that's why the people have not embraced the dynamic methodologies, you know, since you guys started screening because, you know, the same thing with electric power. You remember how they model. Even in the Reactor Safety Study they say what is the probability that off-site power will be recovered before the diesels fail, and they have a crude equation with an integral there and it's not very accurate, but it's good enough.

PROF. ALDEMIR: But remember here, you know, there are two types of situations. I mean, if it were just sequence dependence, I would agree with you, but it not just sequence dependence.

CHAIRMAN APOSTOLAKIS: Okay. What else is there?

PROF. ALDEMIR: This bullet here. It's the exact timing.

CHAIRMAN APOSTOLAKIS: Okay.

PROF. ALDEMIR: This one. This one. All three exact timing, not sequenced. These are sequenced.

CHAIRMAN APOSTOLAKIS: So why aren't they listening to you?

PROF. ALDEMIR: Because two reasons.

CHAIRMAN APOSTOLAKIS: This is not just software.

PROF. ALDEMIR: I will give you two reasons.

CHAIRMAN APOSTOLAKIS: Okay.

PROF. ALDEMIR: The first reason is that it is hard to follow this methodology. The second reason is that they say, you know, from the workshop, that's what Stefan Hirshberg said, so what? So if you are right, what do I care if it is not very significant? In fact, the same comment was made earlier. You know, if the digital I&C system failure is not significant to core malfrequency, what do I care?

Now, nothing has been done so far for a full PRA to show that and I think this is an excellent opportunity to do it, which we are proposing to do, by the way. So that is why we haven't been listening and I'm very happy that, you know, we have such an occasion to look at it and see if it is really significant or not.

Okay. I just summarized it, but I want to mention these two here, which are going to be important. You see, we are overestimating the low pressure probability by a factor of 3 and overestimating low level probability by a factor of 2. Now, if we had digital controllers in place, because of tighter coupling I would have expected much larger differences.

And you see the other interesting result, and that is part of the controversy. High level/high pressure results are very close to conventional methodology results. So sometimes it's okay, sometimes it isn't okay, and that is the other argument that people have raised. So as a regulator, for example, in the old days, NRC would say what do I care? You know, it's safe, no problem, but I don't think in today's risk-based environment.

So anyway, conclusions. No single methodology satisfies all requirements, namely for DFM, for example. The only thing that is really missing is the data business, but of course that is true for everything. Data, even if we had data, it's not going to be convincing. It's not going to be credible to a significant portion of the technical community. We need to show that DFM is capable of describing the system dynamics properly and the alternative is Markov approach.

Oh, I have two more. And what happens when you don't use dynamic event trees? Well, we don't have any evidence on digital Type II interactions. What we have is only evidence on Type I interactions, which says that, which implies, not says, but implies, part of it is a little bit conjecture, that if the system is a single failure mode, if it doesn't have logic loops, if it doesn't have substantial time delay with respect to the system time constants between the initiation of the fault and system failure, then the likelihood is high that the event tree/fault tree approach is going to give good results.

Now, if we extrapolate this evidence to

the digital I&C systems, what we can say is the following. The ET/FT approach may yield satisfactory results as the conventional one when a digital system does not interact with a process that has multiple top events, logic loops and so forth is basically a repetition of these three, rely on sequential circuits, which have memory, have tasks which compete for the I&C system resources and anticipate future states of the controlled/monitored process.

That's why I said RPS system is the most likely one that can be modeled using the static event tree/fault tree approach, but I don't know exactly how this system works. If there is extensive communication within the system, you know, some of these, and I think Bill mentioned earlier or somebody mentioned earlier, that there is a computer in there and you are looking at future states, so I'm not sure in that respect. So what we were proposing to do is first --

CHAIRMAN APOSTOLAKIS: Now, before you go to that, you are focusing here on dynamic stuff, which is important and so on, but another dimension, and I'm not sure it's a truly different dimension, but in the spirit of helping, you are aware of this thing that we're talking about that a failure of a software should be looked at in the context in which the software is used.

PROF. ALDEMIR: Yes, right.

CHAIRMAN APOSTOLAKIS: That there is a classic example with the landing gear of an airplane that Chris used as an example.

PROF. ALDEMIR: Yes, I read the paper.

CHAIRMAN APOSTOLAKIS: Where the airplane was on the ground and the pilot ordered the system to raise the landing gear and the system obeyed. There should have been something there forbidding it to do that if the plane is on the ground. So the question that was raised is is that software now faulty? I mean, can you say that the software -- no. One school of thought says the software did what it was supposed to do. It's the designer who screwed up.

PROF. ALDEMIR: Yes, specification error, specification error.

CHAIRMAN APOSTOLAKIS: With the requirements, requirements actually, not the specifications. So what is the failure of the software sometimes is not obvious, because the software did it.

PROF. ALDEMIR: Yes, that's why --

CHAIRMAN APOSTOLAKIS: He wanted me to

raise the landing gear. I am going to do it. You know, so the context is very important. I mean, if it's flying, it's good. If it's on the ground, it's not good and that's a trivial example, of course, but it happened actually. It happened. So I don't know.

And then, of course, the example we have been using here is the abnormal events, external events that require the software to do something extraordinary, and that's when you see that there is a problem. So should you make context as another dimension of all this and how does that fit into what you are describing?

PROF. ALDEMIR: I'll let Steve comment and then I will comment.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: Yes. The concept that you are putting forth is a very important issue and how context-specific, if you will, are certain situations is also a big issue.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: And that drives us to the kinds of questions we were asking last night. What kind of modeling is necessary? What level of detail of modeling not only in terms of how many circuits and things like that, but how much of the process, how much of the specification, what kinds of issues do you have to deal with?

As I go back to what I talked about yesterday, one of the big issues in developing both guidance for what is acceptable from a licensee PRA, as well as what we want in our own PRA, and asking these kind of questions and that's part of both developing the methodologies, as well as understanding what the requirements need to be, what level of information do you have to embed in the process model. And one of the toughest ones, as you have pointed out, is how do you deal with specification issues.

CHAIRMAN APOSTOLAKIS: Yes, and requirements.

MR. ARNDT: And requirements.

MR. KEMPER: The integration, what you are trying to do is model what you don't know. Right?

CHAIRMAN APOSTOLAKIS: We are very good at that.

MR. KEMPER: There may or may not be.

CHAIRMAN APOSTOLAKIS: We are very good at that.

PROF. ALDEMIR: This is what we are planning to do. You know, as has been clear so far, not only we are taking software and hardware jointly, but we are also taking the process as part of it. So what you are --

CHAIRMAN APOSTOLAKIS: And the process may create contexts.

PROF. ALDEMIR: Right.

CHAIRMAN APOSTOLAKIS: But we didn't say anything about --

PROF. ALDEMIR: But you know, what we are going to do is when we come to -- okay, maybe not I think enough time here, but what we are going to do is basically take this. If we can get a good description of the feed water control system, which we are sure to get --

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: -- then we are going to couple it to a system simulator.

CHAIRMAN APOSTOLAKIS: No, no, no, but you are now going into the details of how to do it.

PROF. ALDEMIR: But that's what will happen.

CHAIRMAN APOSTOLAKIS: But you gave us a presentation where you said, you know, there are certain needs. I have to recognize a few things and so on. And what I'm saying is shouldn't you also recognize somewhat there that the context is important?

PROF. ALDEMIR: Oh, you mean the conclusions?

CHAIRMAN APOSTOLAKIS: And even before.

MR. ARNDT: Yes.

PROF. ALDEMIR: Okay, okay.

CHAIRMAN APOSTOLAKIS: When you have your requirements and all that.

PROF. ALDEMIR: I see, I see. Okay. Sure, sure.

CHAIRMAN APOSTOLAKIS: It seems to me --

PROF. ALDEMIR: Yes, yes, yes.

CHAIRMAN APOSTOLAKIS: Do you mention it in the NUREG, draft NUREG?

PROF. ALDEMIR: No, no, good point, good point.

CHAIRMAN APOSTOLAKIS: And what I'm saying is that maybe it's something.

PROF. ALDEMIR: Good point.

CHAIRMAN APOSTOLAKIS: I thought that example by Chris was very, very illuminating.

PROF. ALDEMIR: No, no, that's a valid point.

CHAIRMAN APOSTOLAKIS: Yes. All this applies to your work, too.

MR. ARNDT: Right. And where this is going to be particularly important, and why we're looking at particular kinds of methods, is how do you develop a state-based model or whatever model you use to feed the particular reliability models.

PROF. ALDEMIR: But in the report we -- what I think Professor Apostolakis is saying, that we should make it a separate point.

MR. ARNDT: As explicit.

CHAIRMAN APOSTOLAKIS: Discuss it.

PROF. ALDEMIR: Good point, good point.

CHAIRMAN APOSTOLAKIS: I know you know about it.

PROF. ALDEMIR: Yes.

CHAIRMAN APOSTOLAKIS: But good point, good point. And we see all this stuff.

PROF. ALDEMIR: Right, good point.

CHAIRMAN APOSTOLAKIS: Because you see, when you talk about state space, a new context may create new states.

PROF. ALDEMIR: Right.

CHAIRMAN APOSTOLAKIS: There is a defined support. Can you hear him?

MR. CHIRAMAL: The example, there is something missing in the examples. My name is Matt

Chiramal, NRR. It starts off with a loss of off-site power and the feed water pumps have tripped, everything is tripped and it initiated with a large break or a small break?

PROF. ALDEMIR: Small break.

CHAIRMAN APOSTOLAKIS: Small break.

MR. CHIRAMAL: So you mentioned the loss of off-site power.

PROF. ALDEMIR: No, no loss of off-site power.

MR. CHIRAMAL: Then the feed water system would be working.

PROF. ALDEMIR: The break is such that it incapacitates the reactor core isolation cooling system.

MR. CHIRAMAL: Yes, but the thing is if the feed water is running already, it supplies water already.

PROF. ALDEMIR: Oh, you mean the -- oh, yes, off-site power.

MR. CHIRAMAL: So you are missing a lot of initials.

PROF. ALDEMIR: Okay.

MR. CHIRAMAL: Plus when it happened, the second HPC pump also, high pressure injection pump, tripped. There should be two, at least two or three sometimes. You are looking at a system a lot more better than when you read an example like that.

PROF. ALDEMIR: But the point is that the paper is not here, so I'm not sure if I am capturing all the assumptions that we had in the paper here in this transparency. And you may be right. We might have missed them in the original paper. But the point is that the dynamics is not going to change very much.

CHAIRMAN APOSTOLAKIS: No, because the feed water is an entirely different situation.

MR. ARNDT: Yes, we'll clean it up. The point is that there are certain scenarios that when you have competing events, the dynamics drive you to the different conclusions.

CHAIRMAN APOSTOLAKIS: And I think another thing you should do, Tunc, is nobody disputes what you say, but what you really ought to do, as well, and maybe you plan on some of it, is look at those crude models that people use to handle these situations and then draw some conclusions that the crude model is way off or something like that.

PROF. ALDEMIR: We tried to do that.

CHAIRMAN APOSTOLAKIS: Because people are aware of these things. I mean, even in the Reactor

Safety Study, as I said, they do. They do it.

PROF. ALDEMIR: And this came up again in the --

CHAIRMAN APOSTOLAKIS: Not happily perhaps or satisfactorily, but they do it.

PROF. ALDEMIR: In the workshop it came again. You know, if we try to do that analysis, the conventional analysis, people become skeptical. They say well, of course, you know, how do you know, we could have done -- Stefan Hirshberg was saying that oh, I could do anything you can do with event trees/fault trees.

CHAIRMAN APOSTOLAKIS: That's a song from something.

PROF. ALDEMIR: But what he ends up doing is exactly what we are doing, except not so methodical. He uses a simulator. He generates multiple event trees, multiple fault trees.

CHAIRMAN APOSTOLAKIS: I don't know what you are trying to say now, but the truth of the matter is that you are not identifying a situation that people are completely unaware of. They are aware of the fact that sequencing sometimes is important and they have proposed very crude methods for handling that and the classic case is loss of off-site power and when it is restored. Okay?

So if it is restored after the batteries are exhausted, then I'm in trouble, right? So people say well, gee, you know, I had to do that. Okay. How long are the batteries going to last? 11 hours. What is the probability that we will restore off-site power in 11 hours? So they break it up into pieces that they can handle.

Now, of course, you might say but how do you know it's 11 hours? It might be something else. And they will reply well, I don't need that kind of detail, because I have already gotten my order of magnitude number and that is good enough.

PROF. ALDEMIR: But there are two different issues here. One of them is the sequencing timing and subjectives, the phasing of mission, so to speak, as you describe it. The other one is interaction. They are different issues.

CHAIRMAN APOSTOLAKIS: No, I'm with you. All I'm saying is that your arguments will carry more weight if you acknowledge that other people are doing something about some of these.

PROF. ALDEMIR: We did that in the NUREG.

CHAIRMAN APOSTOLAKIS: Okay.

PROF. ALDEMIR: It is in the NUREG. We

did talk about phase missions and how people address that issue. You are right. I mean, we did that. That was Curtis Smith's --

CHAIRMAN APOSTOLAKIS: So what you are telling me is I should read the NUREG?

PROF. ALDEMIR: No, no, there was no implication, no.

CHAIRMAN APOSTOLAKIS: I started, by the way. So can we go on now to the happy end, next steps?

UNIDENTIFIED SPEAKER: Backwards.

PROF. ALDEMIR: Oh, backwards, okay. Sorry. We are proposing to develop two benchmark problems that will capture important features of the existing I&C systems, and they have digital counterparts. We want to do an analog. This was also mentioned yesterday, that we should do that or somebody should do that. We are planning to take an analog system as is and if we can find -- the ideal situation is to find something that was there earlier and then that is there now and then compare the exact systems as they are and if we can get access to the data. I'm not sure if we can.

But anyway, we're going to come up with two systems that will try to capture all these features that I mentioned, and we will use dynamic flowgraph methodology and the Markov approach with a common set of failure data to compare just the capabilities, not necessarily data sensitivities or --

CHAIRMAN APOSTOLAKIS: What do you mean "common set of failure data?" I mean, their needs may be very different. I mean, if you give them the failure data, you are forcing them to use it.

PROF. ALDEMIR: No, no, no.

CHAIRMAN APOSTOLAKIS: I mean, the failure models that they are considering may be different. Why don't you do it in pieces? First, ask the Markov guys to come up with a state space and ask the DFM guys to come up with the equivalent.

PROF. ALDEMIR: That's what --

CHAIRMAN APOSTOLAKIS: And then compare.

PROF. ALDEMIR: That's what we --

CHAIRMAN APOSTOLAKIS: Forget about failure rates. When you say failure data, I don't know what you mean.

PROF. ALDEMIR: Well, it could be --

CHAIRMAN APOSTOLAKIS: Don't give it to them.

PROF. ALDEMIR: No, no, no. I'm sorry. This is the situation. When I say "common set of failure data," the current plan is that the University of Virginia is going to come up with the failure modes of the system. Then we are going to use the same failures. We're going to take those failure modes and then try to see if the dynamic flowgraph methodology, given the system description, how it operates, is going to come up with the same failure modes, because there may be a discrepancy. It's not clear at this point.

CHAIRMAN APOSTOLAKIS: Yes, but that doesn't mean that Virginia is right.

PROF. ALDEMIR: No, no, but we're going to do comparison.

CHAIRMAN APOSTOLAKIS: So you're just making part of it.

PROF. ALDEMIR: We are looking at both failure modes. But what I'm trying to say here in this bullet is we need to quantify.

CHAIRMAN APOSTOLAKIS: Yes.

PROF. ALDEMIR: So if we need quantification, we'll try to make sure that both sets are using the same data.

CHAIRMAN APOSTOLAKIS: Yes. I disagree with your statement. We need to quantify no matter what.

MR. ARNDT: We need to try to quantify.

PROF. ALDEMIR: It has to go into a full PRA. I have to have numbers.

CHAIRMAN APOSTOLAKIS: Yes. Okay. Are we going to have another chance to look at the benchmark exercise?

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: After the fact or during the fact or before the fact?

MR. ARNDT: It's entirely up to you.

CHAIRMAN APOSTOLAKIS: Well, if I were you, I would ask for it as early as possible, because clearly there are some disagreements here.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: And I think it's too late to resolve them today.

MR. ARNDT: Okay.

PROF. ALDEMIR: Okay. But anyway, the intention is that if DFM and if we have agreement, and I'm not sure if it's going to be that easy to resolve at this point, I mean, from what Professor Apostolakis said. And then we are going to take the results and try to see how we can incorporate them into a full PRA. And with dynamic flowgraph methodology, it's fairly clear, because it gives prime implicates which can replace the minimal cut sets within the PRA, so it should integrate fairly easily.

If it turns out that we need more detail for more physical process detail, then we'll also try to see how we can get the Markov Model out, but then try to put it in a mechanical fashion into an existing PRA such as SAPHIRE. And also, we are doing it kind of independently of this project, but we are also looking at the feasibility of developing a dynamic methodology on the SAPHIRE platform, but this is another project.

(Whereupon, at 5:00 p.m. the meeting continued into the evening session.)

E-V-E-N-I-N-G S-E-S-S-I-O-N

5:00 p.m.

CHAIRMAN APOSTOLAKIS: Thank you very much. Do you have anything else to say?

PROF. ALDEMIR: Oh, any questions?

CHAIRMAN APOSTOLAKIS: Steve, do you have anything to say that you really think is important?

MR. ARNDT: I guess not.

CHAIRMAN APOSTOLAKIS: Okay. Maybe we should go around. I don't know. Are there any questions?

MR. THORNSBURY: We have representatives from NSIR here in case they wanted to comment on the research process.

CHAIRMAN APOSTOLAKIS: Anybody who wants to speak? No. Okay.

MR. MORRIS: On this topic, no, or on any topic?

CHAIRMAN APOSTOLAKIS: We have one topic. Okay. Thank you very much. This was very, very helpful both yesterday and today and yesterday's speakers. I believe the Subcommittee has a much better idea now what's going on. The plan is to have another Subcommittee meeting to cover the rest of the plan, right? Then in October maybe, September, October, sometime --

MR. SNODDERLY: October.

CHAIRMAN APOSTOLAKIS: October. You will come and brief the full Committee, at which time we will write a letter on the plan. Now, today maybe if the Members are willing, they can give us preliminary thoughts. If you are unwilling, that's fine, too. What?

MR. ARNDT: The NSIR staff wanted to be available to make comments on the overall plan.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: Not this particular presentation.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: Do you want to hear from them for a minute or two?

CHAIRMAN APOSTOLAKIS: Okay. Go ahead.

MR. MORRIS: I mean, I wasn't available yesterday. I'm Scott Morris.

CHAIRMAN APOSTOLAKIS: Can you go there, please?

MR. MORRIS: Yes.

CHAIRMAN APOSTOLAKIS: We have a microphone.

MR. MORRIS: I'm Scott Morris from NSIR.

I'm one of the Section Chiefs in the Division of Nuclear Security. I couldn't be here yesterday, unfortunately. It's my understanding that the NRR folks had an opportunity to comment as well. We only looked at the cyber security portion of it, which I think is Section 3.4. The research folks, Bill Kemper and his staff, asked us to take a look at it and see whether or not we had any heartburn with it or thought we could make it do more.

CHAIRMAN APOSTOLAKIS: And you wrote a memo, right?

MR. MORRIS: And we wrote a memo and I think it summarizes it fairly well, but I guess the point that I wanted to raise in this discussion is that we -- you know, from a security standpoint, I mean, you look at everything differently when you do it from a safety standpoint, because it's not random failures. I mean, it's bad people trying to do bad things and take advantage of vulnerability, etcetera.

And so from our standpoint, we're interested in any research that would help promote an understanding of the vulnerabilities that exist and how they could be exploited. Now, we are fairly far down a path of devising a process, an approach. We have issued a couple of NUREGs already you may or may not be aware of that define a mechanism by which licensees at reactor facilities or any facility, for that matter, can employ this process and help determine where their vulnerabilities exist.

It's a very well-articulated process and it doesn't really -- from a big picture standpoint, we really don't care what happens inside of the box. We just want to know of a box that may control a safety system. We don't really care.

CHAIRMAN APOSTOLAKIS: Are these Official Use Only?

MR. MORRIS: Yes. They haven't been widely disseminated.

CHAIRMAN APOSTOLAKIS: But we can have it?

MR. MORRIS: Absolutely.

CHAIRMAN APOSTOLAKIS: Yes.

MR. MORRIS: I'll make those available to you. But the point is it's not so important to us to know how all the inner workings of the -- we just want to know, number one, look out, look at your site. Figure out what systems are important to you from a safety standpoint, then figure out how those systems are controlled, operated, monitored, whatever and how they can be exploited from an external adversary or even an internal.

And figure out if this is the box, how is it connected to the outside world, and to take a look at all those connections and make sure that you're satisfied that they are either secure through a system of barriers or protocol, whatever. And if they are, fine, but to figure out what they all are and then use a risk-based approach to determine which ones you need to do something with or not.

And we have, as I said, been -- we have prepared these detailed methodologies. We were aided by the industry, because we have piloted it at four different sites. We had PNNL help. Pacific Northwest National Lab helped us devise this with their expertise. And now, we're working with the industry themselves, Nuclear Energy Institute, and their own Cyber Security Task Force to develop a program management document.

They currently have it published, it's NEI 04-04, that they use, but it's to take what we have developed as a staff, to use this cyber security self-assessment methodology and then put a programmatic overlay over the whole thing to help individual licensees identify it and manage the risks of cyber security at their facilities.

And we're working very closely with them, commenting on that whole thing. So with all of that as a background as to what NSIR is doing, a very non-detailed description, we looked at the research plan, from what they wanted to do or what they had proposed to do, and of course our overriding comment was hey, anything you can do to help us implement this process, that's our top priority.

But we understand there is benefit to doing some degree of anticipatory research to look inside the box, you know, to enhance our understanding of what's actually out there and to do some research to look at validating what we think we know, but do we really know it, you know, and how some of the software works.

All that is legitimate, but it doesn't directly help me necessarily. It may add credibility to the overall, what we're doing, but it doesn't -- so our comments were all based on we're doing this. Anything you can do to help us implement this is great. We understand there's a need to do these other things at some good level. You know, NRR can weigh in on that and I think they have.

CHAIRMAN APOSTOLAKIS: But you said you went to PNNL for help.

MR. MORRIS: Yes.

CHAIRMAN APOSTOLAKIS: Why shouldn't that activity be part of the plan or maybe there is no reason for it to be part of the plan. But I mean, does PNNL know -- would PNNL benefit from interactions with Steve and Mike and their contractors, because that's really the question. I mean, if it's an isolated activity that is really very different from what the rest of the guys are doing --

MR. MORRIS: I'm not sure. I think Eric can tell you better.

CHAIRMAN APOSTOLAKIS: I mean, you create a plan usually because there are activities that have a common goal and there may be synergies. You know how it is.

MR. MORRIS: Yes, I understand.

CHAIRMAN APOSTOLAKIS: But if your needs are so different that really you are not going to benefit from anything that these guys are doing, then maybe what you did is good enough. Otherwise, the question is why weren't PNNL part of this?

MR. KEMPER: Well, let me try to address that. Our approach in the cyber area is to take an inside and outside approach. We're looking at what's the vulnerability of safety-related digital control systems and other things are connected to from an inside threat as well as an outside threat. So that's why we started from the inside. It's important to understand the protocol and communication lessons between one process over another to get a better appreciation for what the vulnerability is.

As Todd said, we're trying to assess the vulnerability, not the threat, that's up to -- the threat. So until we actually start taking these systems apart and looking at their susceptibility to cyber attacks --

CHAIRMAN APOSTOLAKIS: But you are not looking for those, are you?

MR. KEMPER: Oh, yes. We haven't explained it to you yet.

CHAIRMAN APOSTOLAKIS: Oh, okay. This is one of the next meetings.

MR. KEMPER: This is the next meeting, right.

CHAIRMAN APOSTOLAKIS: Okay. Okay. Maybe you should come to the next meeting.

MR. MORRIS: We'll be there.

MR. KEMPER: Okay. So that's the inside part. And then, of course, there's the another --

CHAIRMAN APOSTOLAKIS: I understand that.

MR. KEMPER: -- which is the outside.

We're going to look at a typical, you know, configuration of connectivity of power plants and try to see what's the vulnerability of that.

CHAIRMAN APOSTOLAKIS: Even with that though, NSIR says that you are not really helping.

MR. WATERMAN: Well, to interject, when we received NSIR's comments and follow-up comments --

CHAIRMAN APOSTOLAKIS: Okay.

MR. WATERMAN: -- into the research plant, additionally, the NUREG 6047, as I've read it --

COURT REPORTER: Sorry, when you speak, move the microphone over.

MR. WATERMAN: Oh, okay.

CHAIRMAN APOSTOLAKIS: We were whispering, but --

MR. WATERMAN: Mike Waterman in research. As I understand 6047, it is designed to look at installations in nuclear power plants, right now look for vulnerabilities in installed systems. It's our research plan to address more of that. However, the other area that we're looking at is guidance for developers of new networks that haven't been installed in plants yet to tell if these are the things you ought to be considering when you are thinking about designing a secure network to put into a plant, so we can sort of head off some of the issues that Scott is trying to deal with right now.

Instead of having bad networks installed in the plants and then having 6047 and tools deal with those issues once they are in, we're also trying to provide guidance that have --

CHAIRMAN APOSTOLAKIS: It seems to me that all this really should be discussed at the next cyber meeting.

MR. MORRIS: Well, I just wanted to say that this is premature.

CHAIRMAN APOSTOLAKIS: It's a little premature, yes, but especially --

MR. MORRIS: Yesterday you guys talked about some of this stuff.

CHAIRMAN APOSTOLAKIS: Yes.

MR. MORRIS: It happened then.

CHAIRMAN APOSTOLAKIS: Okay.

MR. MORRIS: But I think you do need to be aware of --

CHAIRMAN APOSTOLAKIS: Yes.

MR. MORRIS: -- that there is a fairly significant level of activity going on.

CHAIRMAN APOSTOLAKIS: Yes, the next meeting will be probably some time in August perhaps.

MR. THORNSBURY: Or September.

CHAIRMAN APOSTOLAKIS: September is hard for some of us.

MR. THORNSBURY: It will be in one of those two.

CHAIRMAN APOSTOLAKIS: Is that okay with you guys?

UNIDENTIFIED SPEAKER: It would be okay with us. August would be --

MR. KEMPER: I won't be able to participate.

CHAIRMAN APOSTOLAKIS: August is --

MR. KEMPER: Because I mean, in August I'm away on vacation.

UNIDENTIFIED SPEAKER: In July?

CHAIRMAN APOSTOLAKIS: After the middle?

MR. KEMPER: Oh, after the middle.

DR. BONACA: After the middle we're going to transfer me, right? So then we have a couple of good preparation for the full meeting. We have --

MR. SNODDERLY: Mario, was there a subcommittee scheduled yesterday for September for Browns Ferry? I think there was.

CHAIRMAN APOSTOLAKIS: Probably was. Actually, we scheduled something.

MR. SNODDERLY: So you may want to tag it on to that.

CHAIRMAN APOSTOLAKIS: Yes.

MR. SNODDERLY: Because you never know when the time --

DR. BONACA: And that's going to be probably involving most members.

MR. SNODDERLY: Right.

DR. BONACA: Because of all the mix.

CHAIRMAN APOSTOLAKIS: Visit where?

DR. BONACA: It's going to be here, but we return subcommittee on Browns Ferry.

MR. THORNSBURY: Okay. We'll work that out.

DR. BONACA: We talked to the staff.

MR. SNODDERLY: So Eric will work with Steve --

CHAIRMAN APOSTOLAKIS: Well, remember that the --

MR. SNODDERLY: -- to come up with an agenda.

CHAIRMAN APOSTOLAKIS: Right. I mean, it's hard for me to -- Monday, Wednesday is going to be very hard to get it.

DR. BONACA: The trouble now, you know,

with meeting July 20th and then the summer is getting all scheduled with meetings.

CHAIRMAN APOSTOLAKIS: Anyway, Tom, you want to say a few words?

DR. KRESS: Yes, I can give some impressions.

CHAIRMAN APOSTOLAKIS: Yes.

DR. KRESS: First of all is I'm awfully glad to see research doing this. I think it's stuff that we have called for in the past and it's going to be badly needed and it's going to be, I think, very helpful. I like the idea of up front looking for modes of failure first, types of failures you have by searching out. I'm afraid you won't find very many out there though.

I like the thought that the EPRI guy, he's not here now, suggested that have you thought about looking at whether or not you can declare all digital systems, I&C systems better than analog and therefore you could either say that the risk is not that significant or you could just use the analog value and say you've bound it. I like that thought.

One thing that struck me is that basically everything we are doing in terms of looking at digital software failure rates, failure probabilities seems to imply that the failure is a random event and we know they are not. And I think the one unique failure probability, I think it will be sequence dependent, and maybe even time dependence within the sequence. I think you have a problem looking for a failure probability.

I think you need -- that's why you need these failure modes and how they fail and how they interact first, because I am very doubtful you will get a unique failure probability. Other than that, I'm sure glad that you guys are doing this, because it's something that, I think, will bear fruit and be very useful.

CHAIRMAN APOSTOLAKIS: Thank you, Tom. Mario?

DR. BONACA: Yes, I'm commenting also on some presentation we had yesterday morning. I felt that Reg Guide 1.97 endorsing actually policy standard, I think, is good. It is going in the right direction. I don't know, however, about the possibility of backfitting that Reg Guide to older plants. That's an issue that is not submitting to us it seems to me, at this stage.

We heard about the preliminary validation of the methodology for assessing software quality. We had a presentation yesterday morning. I was, I guess, confused about what is in that report that was presented, so --

CHAIRMAN APOSTOLAKIS: Which one is that one?

DR. BONACA: It's the --

MR. SNODDERLY: Maryland.

CHAIRMAN APOSTOLAKIS: Maryland?

DR. BONACA: Yes. Maybe it was my problem in digesting all the information in that document. But I wasn't too convinced about that work. In so far as the plan, the role plan, I think I totally agree with you, Tom, that, you know, I really had an appreciation developed yesterday and today for the need for this work. I mean, clearly, I came out of this meeting with increased concern with the use of digital systems, although we know that they will be here. And they will be used.

So, you know, one thought, we certainly would like to get involved with the Oconee upgrade.

CHAIRMAN APOSTOLAKIS: Oh, yes.

DR. BONACA: As a means of learning more about those issues you are bringing up, which is time dependency, for example, that may mask certain faults at first view. And, you know, my thought is that you wanted to couple the design from the platform. But in this case, it may be very well that the platform itself or the process that you are using for the digital design it seems to create the opportunity for mistakes on the part of the design. There is that kind of feedback there.

I thought that the plan was quite significant and I hope that they can resolve their differences with NRR. Clearly, I think that NRR is writing and being involved in the finding of need, but I think that we have to look forward and far on this issue, because there are significant implications for safety.

DR. KRESS: I hope that the apparent negative reaction of NRR doesn't put a damper on this, because, you know, I think this is anticipatory research and might not even need a user need.

DR. BONACA: Yes, I mean, I don't see, you know, given all we have heard, you have to get to it and study and try to understand it and these are pressing issues.

DR. KRESS: I mean, I thought NRR had the feeling that they know how to do these reviews already and they don't need this. But I think that's very short sided.

CHAIRMAN APOSTOLAKIS: But it's also --

DR. BONACA: I think --

CHAIRMAN APOSTOLAKIS: -- important to know that the attitude of the NRR people this time around was very different than the first time we met.

DR. KRESS: Yes, there is change.

DR. BONACA: Yes, there is better communication.

DR. KRESS: Somebody must have jumped on them.

MR. SNODDERLY: Well, I think, Mario makes a good point that we need to be very involved in the Oconee review, because that will demonstrate NRR's concern.

DR. KRESS: On how they --

MR. SNODDERLY: Right. Do they have the tools, do they have the capability to do that?

CHAIRMAN APOSTOLAKIS: And we can --

MR. SNODDERLY: So we will have to --

DR. BONACA: Yes, I think that's great.

MR. SNODDERLY: -- have follow-up and find out when that schedule is and where and make sure we schedule that.

DR. BONACA: Remember, designing this upgrade for Oconee.

CHAIRMAN APOSTOLAKIS: Framatome.

DR. BONACA: Okay. But, you know, I mean, I think we will learn a lot from them.

CHAIRMAN APOSTOLAKIS: Oh, yes. Anything else?

DR. BONACA: No, nothing.

CHAIRMAN APOSTOLAKIS: Good. Well, I think my views were made clear more or less, but I want to say that yes, I'm very pleased myself that the staff is doing this. By and large, it is a very good program, plan and I'm looking forward to seeing the revised schedule that you gentlemen are working on now. I also have serious doubts about the usefulness of all this metric thing that was presented. It was yesterday. Actually, I have more than doubts, but I just want to say doubts. I don't think it's useful at all.

DR. KRESS: The fault density?

CHAIRMAN APOSTOLAKIS: What?

DR. KRESS: The fault density, you meant?

CHAIRMAN APOSTOLAKIS: No, the other one with -- I don't know, the Maryland one.

DR. BONACA: Yes.

CHAIRMAN APOSTOLAKIS: The metrics. I don't see how that can help a decision-maker. Well, I have problems with the fault injection when they start developing failure rates, but I think a good thing about this meeting and the last meeting we had, but especially this one, is I think we are beginning to understand each other much better. But there are some fundamental issues that bother me. And, you know, you gentlemen showed some appreciation for some of them anyway.

DR. KRESS: I thought they needed a better definition of fault and a specific comment.

CHAIRMAN APOSTOLAKIS: Yesterday?

DR. KRESS: Yes. You know, you're trying to determine the number of remaining faults by some process, which I thought might be reasonable. But it's the denominator that goes into that that bothers me. And I think you need to think about that denominator.

CHAIRMAN APOSTOLAKIS: Any time anybody does a historical to determine the number of remaining faults, you should be awfully skeptical.

DR. KRESS: Yes, but it's -- you know, the numbers --

CHAIRMAN APOSTOLAKIS: But it is a difficult issue.

DR. KRESS: The denominator worried me

more than that.

CHAIRMAN APOSTOLAKIS: So I think today's presentations were -- not presentations, the substance of it was much better. Some of the stuff was presented yesterday, not all of it. A lot of it was good, too. So I think we are on our way and we're going to review the rest of the plan and then write a letter on the plan itself. But also, what is not clear in my mind is how we're going to comment on the individual projects now.

So, at some point, I mean, you know, this is research. Do they have to come to us? They don't have to, do they? Professor Aldemir finished at present three new reports to issue. I don't think the staff is -- there is a mandatory for them to come to us, unless we request it.

MR. SNODDERLY: For review, right, unless we request to review the new reg reports.

CHAIRMAN APOSTOLAKIS: Steve?

MR. ARNDT: You're right. It's a decision of the staff whether to issue publications or not. Now, not necessarily Professor Aldemir's work, but any of our work. If it goes into regulatory implementation, a Reg Guide or a revision of the SRP, then you need to come to. The point, however, is, as we mentioned earlier in the day, there are certainly times where we would want your input on decision points and directions and things like that.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: Either in this forum or in another forum and we'll work with Eric to try and do that.

CHAIRMAN APOSTOLAKIS: So it would be sort of a participatory review.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: Which I think is fine with the Committee.

MR. KEMPER: Can I ask a specific -- Bill Kemper here. Yes, what I would like to do is we're going to get together and kind of discuss our projects and maybe identify those milestones where another engagement with you all would be appropriate. Okay?

CHAIRMAN APOSTOLAKIS: Sure.

MR. KEMPER: So we're going to have to take this to heart.

CHAIRMAN APOSTOLAKIS: Very good.

MR. KEMPER: And really value the interaction here. You have given us some real good things to think about. And, obviously, it makes us feel a lot more comfortable knowing that we're on the path that you all are comfortable with.

CHAIRMAN APOSTOLAKIS: Yes.

MR. KEMPER: As opposed to violently opposed to, you know, before we go public with that.

CHAIRMAN APOSTOLAKIS: Wonderful. Anything else? Well, thank you gentlemen again. This has been very useful and this meeting of the Subcommittee is adjourned.

(Whereupon, the meeting was concluded at 5:23 p.m.)