Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, April 17, 2008

Work Order No.: NRC-2138 Pages 1-270

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 MEETING

+ + + + +

THURSDAY,

APRIL 17, 2008

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11555 Rockville Pike, Rockville, Maryland at 8:30 a.m., Dr. George Apostolakis, Chairman, presiding.

COMMITTEE MEMBERS PRESENT:

GEORGE APOSTOLAKIS, Chairman

DENNIS BLEY, Member

MARIO V. BONACA, Member

JOHN D. SIEBER, Member

ACRS STAFF PRESENT:

CHRISTINA ANTONESCU, Cognizant Staff Engineer

GIRIJA SHUKLA, Designated Federal Official

SERGIO GUARRO, Consultant

TABLE OF CONTENTS

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

8:35 a.m.

CHAIRMAN APOSTOLAKIS: The meeting will now come to order. This is a meeting of the Digital Instrumentation and Control System Subcommittee of the Advisory Committee of Reactor Safeguards. I am George Apostolakis, Chairman of the Subcommittee. ACRS Members in attendance are Mario Bonaca, Dennis Bley and Jack Sieber. Sergio Guarro is also attending as a consultant to the Subcommittee. Girija Shukla of the ACRS staff is a designated federal official for this meeting.

The purpose of this meeting is to discuss the progress associated with the research in digital risk assessment methods. We will hear presentations from the NRC staff and its contractor from Brookhaven National Laboratory on NUREG Report entitled "Approaches for Using Traditional PRA Methods for 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.

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

We also have two gentlemen, Bob Enzinna and Shelby Small from AREVA on a bridge phone line listening to the discussions today. To preclude interruption of the meeting, the phone line will be open one way during the presentations and Committee discussions.

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

We will now proceed with the meeting and I call upon Mr. Alan Kuritzky of the NRC staff to begin. Alan?

MR. KURITZKY: Thank you, Dr. Apostolakis. Again, I'm Alan Kuritzky with the Division of Risk Assessment -- Risk Analysis in the Office of Research. And as Dr. Apostolakis said, we're here to discuss the research that we're doing on the use of traditional PRA methods for modeling digital systems.

I'm here today also with my colleagues from Brookhaven National Laboratory, Gerardo Martinez-Guridi and Louis Chu, who have been instrumental in the main performance of the work that we're going to discuss today. In addition, Mengye of Brookhaven National Laboratory has been a major player in this work, but was unfortunately unable to attend today.

We previously talked to the Subcommittee on this topic last in April of 2007. At that time, the project was early in its work and we were able to discuss a little bit about some of the initial activities. And we're coming here today to try and bring you up to speed on where we -- what we have accomplished since that point and particularly to discuss, as Dr. Apostolakis mentioned, the NUREG/CR that was released for review and public comment a few months back and is getting ready to be published as final.

Okay. Just quickly the outline of the presentation I'm going to give you here first. And actually, just to give you an overall view, I'm going to provide an overview of the work that we have accomplished and what's in the NUREG/CR. And then

Louis and Gerardo are going to go ahead and give more detailed presentations on some of the technical topics that I'm just going to briefly touch upon.

So some of your detail questions, you may want to hold off until you hear the detailed presentations, but I'll leave it up to your discretion.

What I will talk about is initially the objective of the project and the tasks planned that we have in place to accomplish the work, where we stand on that work as of right now and also because the NUREG/CR, once it was released for comment, we went ahead and started performing the next task of the project. So even though the NUREG/CR is just getting towards its final stage right now, we actually have accomplished quite a bit of work on the next task, which is application of the traditional methods to the first example system or benchmark system, which is a digital feedwater control system.

So we're going to -- I'm going to give you a few preliminary results and insights from that work. And then lastly, I'll discuss the remaining steps of the project.

The objective of this work is to determine the existing capabilities and limitations of traditional methods for modeling digital systems. By traditional reliability modeling methods, we mean just to recap from what was mentioned in the past, is that these are well-established methods that do not explicitly account for the interactions between the plant system being modeled and the plant physical processes.

Okay. Those types of methods that do explicitly account for those interactions, we refer to as dynamic methods. And you have heard about those at other briefings. The ultimate goal of this work is to try and develop risk informed decision making guidance that can be used with -- for digital systems and applications to nuclear power plants, as well as to try and come up with guidance for inputting digital system models into plant PRAs.

CHAIRMAN APOSTOLAKIS: Now, when we say digital systems, we mean software-based digital systems?

MR. KURITZKY: Software-based digital systems, yes.

CHAIRMAN APOSTOLAKIS: You stated several times in the report that software failures are not part of this act.

MR. KURITZKY: Quantification of software failures is not part of this.

CHAIRMAN APOSTOLAKIS: Well, even identification of the failure modes of software, are they part of it?

MR. KURITZKY: What we have in this, in our study, we consider the normal behavior of software in developing the models as well as some hardware software interactions. Okay. But we do not consider or we do not quantify and we lay out a structure for which software failure information could later be input, once we have advanced to that, if and when we advance to that stage.

So we do consider software in the sense that we are actually considering the normal behavior of the software, but we don't actually quantify software failure probabilities.

CHAIRMAN APOSTOLAKIS: That's right. It's not very clear. I mean, there are several statements in the report, in particular Section 6.3, where one gets the impression that software failures are not part of this or even the failure modes, unless I misunderstood it. And then another interesting thing is elsewhere in the report it says that software failures should be included and so on, I mean.

MR. KURITZKY: Right. The report talks

about -- and we'll get to it shortly, but there are criteria that we have right up front that identify those things we feel should be in a reliable model for, you know, a digital system that's going to be included in the PRA. And that includes software, the treatment of software failures.

CHAIRMAN APOSTOLAKIS: But you are expecting someone else to do it?

MR. KURITZKY: Exactly. What we state right now --

CHAIRMAN APOSTOLAKIS: Who is that someone else?

MR. KURITZKY: That someone else, we have not decided who that someone else would be nor is it necessarily going to be our decision, but it's -- what we're saying is that the current state of the art, the scope of this project is to, again, as I mentioned before, look at the existing capabilities and limitations of the traditional methods. That's really the scope.

So the area of software reliable to quantification is considered, right now, to be too immature to be included in a PRA. There is no technical community consensus on how to accomplish that, okay, so --

CHAIRMAN APOSTOLAKIS: I mean, when one looks at the title of this project, "Risk Assessment Methods for Digital Systems," I mean, even the abstract doesn't say anything that software failures, which is really the most important thing of interest here, but they are not included. So one gets the impression that if I have a digital system and this NUREG is going to tell me how to identify failures and failure rates and all that, it's buried in Section 6.3, that the software failures are not part of it.

MR. KURITZKY: Yes.

CHAIRMAN APOSTOLAKIS: And that bothers me a little bit.

MR. KURITZKY: Right.

CHAIRMAN APOSTOLAKIS: And it seems to me the whole idea of dealing with digital I&C is to try to understand the behavior of the software, not the hardware.

MR. KURITZKY: Right. I have two points I want to make to that comment. One is -- well, first of all, I take some exception actually to the fact that software is the only interesting thing. There are a lot of aspects of digital system modeling that are not intuitive or significantly different than what is typically done in a PRA for modeling a fluid system or, you know, a low pressure safety injection or service water system.

So we want to explore the capabilities of the traditional methods to be able to account for those aspects. But I agree that the software is the, I would say, most challenging or maybe the most interesting aspect. The comments you make is -- was reputed by many people from the internal reviewers of this draft report as well as the public.

And the draft final report that unfortunately you were not provided until just about a week ago, so I understand that you probably haven't gotten a chance to look through that, but because of that comment, right now in the front of the report --

MEMBER BLEY: We did not.

CHAIRMAN APOSTOLAKIS: We don't have --

MEMBER BLEY: We didn't get this thing a week ago.

CHAIRMAN APOSTOLAKIS: Mr. Shukla, do we have the final report, the revised version of this?

MR. SHUKLA: No, I do not know.

MR. KURITZKY: Well, anyway, the staff asked for it, I believe last week, so went it. But in any case, okay, that draft report brings up into the scope section of Chapter 1. We now have a section on the scope of the study and we specifically say in that scope section that software reliable quantification is not in the scope of the work, because it's believed to be too immature and we're not advancing the state-of-the-art in this project. So we have written it out of the scope.

So your comment is valid, I agree with it. And we try to address that in the final report by bringing that up right up front into the scope section of the report.

MEMBER BLEY: Alan, may I ask a question about your earlier comment? When you said you consider proper operation of the software, it's only as a boundary condition, right? This is the way it's working. How does the hardware work given that the software is doing it's job?

MR. KURITZKY: Right. And it's an important aspect in modeling digital systems. As we're going to mention later in the presentation, the modeling of a digital system is much more complicated than at the level of detail that we believe the system should be modeled in order to account for all the digital system specific attributes that could impact reliability.

The model is a lot more complicated than typical systems that you model with fault trees or any other method. So because of that, we ended up having to use processes that require us to consider the actual software of the system in determining how various component, digital component failure modes would -- how and if they would lead to digital system failure.

So we actually have to get right in there and use the actual software, the code from the system as part of developing the models.

MEMBER BLEY: When you said you have laid out a scheme for looking at software failures, you are referring to Appendix C, correct?

MR. KURITZKY: Well, actually, Appendix C, has more, I'm going to touch on that also, because Appendix C you -- has -- and the new final report of Appendix C is being removed.

MEMBER BLEY: Oh.

CHAIRMAN APOSTOLAKIS: Why?

MEMBER BLEY: That seemed like the most interesting part.

MR. KURITZKY: Right. We had that comment from a lot of people. The basis, the reason that we are removing it is because this -- again as I mentioned, treating software reliability quantification is out of the scope of the current project. That work that was in Appendix C is actually work that was completed by Brookhaven some years ago. And in fact, that work was briefed to this Subcommittee in June of 2006.

Okay. We had included it in, but at the time that work was provided to NRC as an intro-level report, it was not made public. So we thought that this was an opportunity to take that work and get it published so that other people could see it and get it out into the community.

MEMBER BLEY: Well, again, I want to interrupt you for just a second. It seems to me it fits in with the title of your report in laying out a structure for looking at failures of software and actually identifying some specific failures. It seems like it fits very nicely the fact that you can't quantify, this doesn't say on its cover this is a report on quantification.

MR. KURITZKY: Right.

MEMBER BLEY: It seems, you know, if it's not here, where is it going to be and when?

MR. KURITZKY: A valid question. Again, I want to re-emphasize that it's not within the scope of this work, because we are only looking at what are the current capabilities and limitations of the models. It's very useful work. It's very interesting work. And we would like to have it out there in some manner. It's just not within the scope as dictated for this project.

So all we have right now is a placeholder in our model for dealing with the software, whenever that part of the analysis is mature enough that we can include it, that we feel we can include it in the PRAs.

MEMBER BLEY: It seems we are mature enough to be able to start looking for software failure modes and categorizing them.

MR. KURITZKY: Right.

MEMBER BLEY: To leave that out just seems a real shame.

MR. KURITZKY: Right.

MR. CHEOK: This is Mike Cheok.

MR. KURITZKY: It's just that -- I'm sorry. Go ahead.

MR. CHEOK: I guess my comment there is that, you know, as Alan is saying, the scope and the objective of this report is to investigate traditional methods and not to do state-of-the-art analysis. To leave the Appendix C in there as is would lead to the perceptions that perhaps you all had also that we have done more work in terms of self-reliability than we actually have done with just looked and entered the surface of it, at this point, two years ago, and it wasn't part of this task, to leave the impression that we have done a lot more would not be the correct one.

MR. KURITZKY: I guess I --

DR. GUARRO: Appendix C is a review of what is out there. And by the way, I have already, you said informally to the others in other environments, but I'll say it here on the record, I think it should be updated, because it's not updated. With respect to where this thing of the art is.

CHAIRMAN APOSTOLAKIS: But even if it is a --

DR. GUARRO: But it is a review.

CHAIRMAN APOSTOLAKIS: Of traditional methods, but applied to hardware. That's a very important point. I mean, there may be other people there that are doing correct things or incorrect things, who are trying to deal with the software and you are not reviewing those, right? So it's really focused on the hardware.

MR. KURITZKY: Right.

CHAIRMAN APOSTOLAKIS: That's a very

important thing to put even in the title.

MEMBER BONACA: What is troublesome to me about this is on page 216, there is a statement says "Probabilistic developer software, the task of assessing relevant probabilistic parameters, such as probability of software failure for complex software is enormously troublesome." And then it goes on to say that there is no generally agreed upon method to label this kind of software.

I mean, I was left -- many comments like this, I was left with impression that always you cannot tackle this issue.

MR. KURITZKY: Again, I don't want to go so far as to say that, but we do -- the point that we wanted to make was that this project, again, to reiterate what Mike had said, is focusing on just looking at where we stand right now. What are --

CHAIRMAN APOSTOLAKIS: On hardware.

MR. KURITZKY: Well, actually, hardware, see you are making the distinction. You are parsing out it into two pieces. The hardware and the software of the system. And actually, when we look at a digital system, there are many aspects of having to model that system. Software is one aspect. There are many other aspects.

I don't know, actually, I would just lump all the rest and say they are all hardware. They are actually --

CHAIRMAN APOSTOLAKIS: Well, make it clear then that the software is not included. But it seems to me that this is the main concern.

MR. KURITZKY: Well, we -- there are other aspects of this. You know, as we will discuss, there are many other aspects or at least some other aspects of digital system modeling that are also a concern. It's not just software.

CHAIRMAN APOSTOLAKIS: I'm sure.

MR. KURITZKY: Completeness and a fair amount of identification is a very important one. The adequacy or availability of data for even hardware quantification is another issue. So it's not just the software. It's not the only issue that we have to confront.

CHAIRMAN APOSTOLAKIS: Is there another arching model here where we are going? I mean, does the Agency have a model that says this work of BNL will be finished by such and such date and it deals with these issues? This other work here deals with that issue, that issue. And then at some point in the future, all of these things will come together and we will say now the Agency has a good model. Is there such a thing?

MR. SYDNOR: This is Russ Sydnor. I'm the Branch Chief of the Digital I&C Branch in the Office of Research Division of Engineering. And I believe the Committee is familiar with the digital I&C Research Plan and there have been past presentations on the overall efforts to look at software reliability and dependability.

There is a number of ongoing research projects in this area. And based on Committee past -- other Committee ACRS recommendations in the area of software failure analysis, inventorying classification, recent presentations, you are aware that we're continuing to work in that area.

So there is an overall plan. Additionally, the Digital I&C Research Plan is under review this year. We want to update it and take a look at the work that has already been done and formulate a better plan going forward, a more cohesive plan. That will involve, you know, interactions between PRA Division and the Division of Engineering.

So, you know, I think we're headed toward what the Committee's questions are probing. I think we are getting there. The ACRS will get a chance to hear what our new plan is later this year as we formulate that and get it in the right format for presentation.

CHAIRMAN APOSTOLAKIS: The Research Plan that we have seen --

MEMBER SIEBER: Right.

CHAIRMAN APOSTOLAKIS: -- did not go down to this kind of detail, as I recall. It was really a fairly high level. I mean, and if at that time you present a project that has this title here, the Committee is in no position of figuring out that software failures are not included. So it doesn't surprise me that we didn't complain when we saw that.

But some logical way that says we're going to have to do this first, this second, this third or parallel and eventually, we're going to have something, I think we need that. And if this plan comes before this Committee, I hope it will have something like this.

MEMBER SIEBER: There's a larger task description that goes on those sheets that authorize each individual job. And maybe that's what we're looking for, because I have read those for the program up to the last year. And you can -- you actually need an overall plan to put those modules together, but it sort of shows you the individual goals of each of the projects. So maybe that's what we want to look at.

MEMBER BLEY: I think so. I think the stuff I have looked at in that plan when it is talking in this area, it talks about modeling digital systems.

MEMBER SIEBER: Right.

MEMBER BLEY: Which I think all of us assumed was hardware and software. We were kind of surprised that it's not. And I don't see any. I just went back and glanced through the plan. I don't see anything in there that makes that distinction.

MEMBER SIEBER: Not only that --

MEMBER BLEY: We would like to. We would like to know when that is coming.

CHAIRMAN APOSTOLAKIS: But you actually have to read a good part of the report until you figure out that software failures are not included. I mean, Section 6.3, that's 106 pages down.

MEMBER BLEY: And it's a paragraph.

CHAIRMAN APOSTOLAKIS: It's a short paragraph.

MEMBER SIEBER: But --

CHAIRMAN APOSTOLAKIS: In passing says by the way, software failures are not included. And you stop and my God, on page 106 they are telling me this?

MEMBER BLEY: Well, I think --

CHAIRMAN APOSTOLAKIS: No, this is very important, because, you know, for more than a year now, we have been hearing that Brookhaven is looking for additional methods for digital software and we all had assumed that it included everything.

MEMBER SIEBER: Well, the staff was the one that decides what the work should be and that should be properly described in the instructions to the vendor. And that's what we ought to be looking at, I think. That it ought to be good enough to be able to tell what are the components of the task and what's the expectation for the final report. And in some cases, those sheets are good enough, in others they are wanting for detail.

MR. KURITZKY: Actually, the ones for this project, it does go to that level of detail.

MEMBER SIEBER: Yeah.

MR. KURITZKY: And specify again that we were -- that the scope of this work that BNL was performing was not to -- it was to evaluate where we stood right now and not extend to state of the art. And I think it even specifically calls out do not go into the software quantification issue, because it's not fully established.

MEMBER BONACA: Well, one thing that troubled me was here in Chapter 5 when talk about FMEAs, you say as discussed in Chapter 1, software is out of the scope of the study. And we was left with the question of, I mean, what do you -- you know, you missed a substantial piece of FMEA by eliminating those kind of software reliability. I mean, that's a fundamental element.

And so I was left, I guess, trying to understand how the pieces you discuss later on in the chapter are affected by the fact that you are not addressing software failures. And I really lost myself into it, because you are showing some, you know, casualty analysis on FMEAs. And there are pieces that will come to mind if you include software failure. And then I'm saying what's the value of this FMEA? I mean, the software failure is missing at some level below and you begin to go into the system.

And so I just -- there were lots of questions in my mind and all that.

MR. KURITZKY: You know, I think that we can have -- Louis can talk more about what's in the FMEA, because I don't think we totally dismissed software as much as you say. And I do want to reemphasize that we are very sensitive to your comments and we know that that perception was out there on the software and that's why the new version of the report right up front under the scope tells you what is and is not included.

MEMBER BONACA: Maybe I did not communicate as well as I should have. You know, by saying we are not looking at software failures, it's if you could decouple the two. And it seems to me that when you get down into the analysis like FMEAs, you cannot decouple them. At some point, they are intertwined. And so my sense would be if that be performed again, the same FMEA once you have also included information about errors, you would get probably different product, a substantially different product. Am I correct?

MR. KURITZKY: Can I suggest something though for this?

MR. CHU: This is Louis Chu, Brookhaven National Lab. Let me explain a little bit. I think we have a whole day and you are going to hear more about it. I'm jumping a little bit. In terms of modeling of software, we actually developed a simulation to that actually run the actual application software using the control system.

By doing so, we can determine the system response to postulated hardware failures. In that sense, we modeled the normal behavior of the software and that was very -- pretty well, because we actually run the cause. And in terms of modeling failure of software, we did it at a high level, in the sense that the system consist of two CPUs. We have a software failure presenting a common cause failure. And it is such failure that is now in our model.

It's just we say quantification of this failure rate is beyond the scope, because the method is immature.

CHAIRMAN APOSTOLAKIS: All right. We'll wait until you get into it, but another thought occurred to me. It seems to me that we have projects. We have presentations in this room over the years that sort of assume certain things. In the case of software, maybe the assumptions themselves should be scrutinized. Like Louis just mentioned failure rates and so on.

I think the staff should have a project, not a big one, with some competent people who will have to think about, I hate to use the word, but, the philosophical aspects of this. Can we talk about the probability of software failure? Has anyone thought about it? I mean, in this report and others, we see that if -- that software always does what it is supposed to do, given the proper inputs. If a failure is found, it's corrected.

So given all these things, can we really talk about the probability of failure of software? Somebody ought to think about it and put it to rest. Instead of starting projects, you know, use the Markov approach or use, you know, somebody else's approach. It's really very important to settle these things. I said before the Commission and I think some people got upset and if I were to talk to them today, I would say the same thing.

I am not sure I will ever get anything that will lead us to the probability of failure in software. There are digital systems included in the software. I just don't see how we can get there.

MEMBER SIEBER: I agree.

CHAIRMAN APOSTOLAKIS: So somebody has to think about it, because if that's the case, then all these projects should be focusing on the identification of failure modes, because that's important to understand. And then again, I agree with you guys when you say that if a failure mode is identified, then it's fixed.

MEMBER BONACA: You know, this is

absolutely true. And I was reading page 511 where you say even bigger issues that there is no generic standard list to find your model digital system components.

CHAIRMAN APOSTOLAKIS: Yeah.

MEMBER BONACA: And you say then that, as discussed in the report, it is possible that FMEA of the same system by another analyst might result in a different set of failure modes. So there is a lot of work to be done there it seems to me on that. There are also discouraging statements there. It's difficult additionally the FMEA to handle the complex digital systems. I was left with, you know --

MR. CHEOK: I'm thinking --

CHAIRMAN APOSTOLAKIS: Now, that you are revising your Research Plan, you will think about it and put a task in there, that really has to be completed quickly. I don't think you need more than six months to do it.

MR. CHEOK: I think we totally agree with you, George. I mean, you know -- I think the conclusion as you will see later on is that we identify several issues that need to be looked at. And we're not saying that we have to look at them all, we have to prioritize them and see how feasible they are before we even think about carrying on to the next steps.

CHAIRMAN APOSTOLAKIS: I really think that this is a number one priority to settle the issue. Maybe the answer is not what I think it would be. I'm willing to accept that. I know my colleague here may disagree. But Dennis goes before you.

MEMBER BLEY: Yeah, I want to go back to what you first said, laying out that philosophy is important, but you cannot do that without the background of having looked closely and understanding the kinds of failure modes of these systems, how the software and hardware and firmware interact. And you might fix specific causes of failure, but you won't fix the categories of the failure modes. They are going to sit there.

And when the data comes a little differently or something else is different, you're going to get a failure. But understanding what those are is crucial to even being able to come up with a philosophy.

CHAIRMAN APOSTOLAKIS: And I agree with that, but I think we have done a sufficient amount of work between the Brookhaven work, the Ohio State work, the West Virginia work, there is some understanding of what kinds of failure modes we see, the data collection work that most of the industry does and we have done. So I think we have reached a --

MEMBER BLEY: We need to organize that in a way to make sense of it.

CHAIRMAN APOSTOLAKIS: We organize it in a way that will lead us to some conclusion which may be revised five years from now, but some conclusion regarding the quantification. So if indeed my present opinion calls and we can't do it, then maybe we should focus on just the stuff we can do. If there is hope that we can do it, then we define the appropriate project.

What bothers me right now is that we are starting projects under the assumption that we're going to, you know, bring this into the PRA, do this and do that thing. Now, Sergio wants to disagree with me.

DR. GUARRO: Well, yes, only partially. I mean, first of all, I mean, I agree with both you and Dennis about the fact that understanding the failure mode should probably be the primary focus, because we have some idea, you know, but we have an idea what the failure modes may be across a large spectrum of applications and maybe we should understand better what the failure modes may be for software that is in the main nuclear power plants, for example, specifically. That's one thing.

With respect to the probability issue, what I want to say is that it is my opinion from my experience. I think the probability of software has a different meaning than what is the traditional sense that we have. I think software failure has a meaning in the context of understanding when it is that you can stop testing, because it is true that you test often. If you find the problem, you fix it.

The problem is that you cannot test everything and you cannot test forever. You need to have a metric to know when to stop. And that metric is, call it, fault coverage, which is a fraction, but, you know, it's related to probability. It's how well you explore the operation profile or how well you explore the gray area, the boundary between the design, you know, scope and what is beyond the design scope.

You've got -- sometimes that is not clear. As I have repeated several times even here, the experience in NASA is that, you know, 7 out of -- missions that were lost because software did something "wrong," was because of design errors. Not because the software had coding errors, it did what it was supposed to do. Unfortunately, it was the wrong thing to do.

Okay. Is that true also in the nuclear power plant arena? I don't know. But, you know, those are the questions we need to explore.

CHAIRMAN APOSTOLAKIS: But that's exactly what I want this task proposing to do. I'm not saying that it's impossible to forget about probabilities, but if we -- what is it that's unique about this business? What is it that we can do if what you just said, Sergio, is what we can do, great, so be it. Let's all understand it then that this is the way we want to go or one of the ways.

And I'll give you another example of where I may be wrong. In Appendix C, you have a very good discussion about the error force in context, which is an idea borrowed from ATHENA. I can see a designer identifying extreme contexts that are so unlikely that the designer says well, it's not worth accounting for this, because this has a very low probability.

Then the probability of the frequency of that particular context is part of the probability of the failure software.

MEMBER BLEY: It's an informed decision.

CHAIRMAN APOSTOLAKIS: It's an informed decision and I agree and we all understand again where we are going. But right now, I think there is this common understanding does not exist. I mean, you have expert opinions from Sergio, from Dennis and from others, but I want all of us to agree and discuss it in this room and say look, when we talk about probabilities, this is really what we can do.

Maybe one is what Sergio just said, maybe two is what I said or maybe three is what other people are going to say. But let's understand that, rather than starting with the assumption that yeah, we can bring this into the PRA, the way we bring, you know, pumps and diesel generators and so on.

So I really would like to see that and I think, you know, it's good that you are revising the Research Plan. I hope we're going to see that there.

MR. SYDNOR: Again, this is Russ Sydnor. I value your insights here. I came new into the Research Plan less than a year ago and I had similar concerns, which is one of the reasons why we are taking some of the actions we are taking to revisit the nature of the research. And I think, you know, myself, Dan Santos, who is the new STA in research, have similar concerns to what you just voiced.

And so we will -- you will be hearing from us again on that.

CHAIRMAN APOSTOLAKIS: Let me repeat something we have said many times. This Subcommittee fully appreciates the difficulty of the problem. It's not that we come in here with the notion that boy, these guys from Brookhaven, they better have an answer, because otherwise we get upset. No. We do appreciate that it's a difficult problem. Do not hesitate to whoever undertakes this task to come here, you know, with ideas that are not maybe final and so on and just exchange views, because, you know, that's what we did when Regulatory Guide 1174 was developed.

The staff didn't know how to approach it. Nobody knew what risk informed regulation meant. They came here. We had ideas, exchange of ideas and so on. So we would like to help, but at least let's make sure that we are addressing the right problems. So don't feel that oh, we have to have this task and then what are we going to say to that Subcommittee. They are going to slaughter us.

No, we do know it's a hard problem. So let's get together, you know, after you think about it a little bit and see where we can go with this. And again, I'm perfectly willing. In fact, we should do that, what Dennis said, but together the experience from collecting, failure experience, what people have said.

I was reading your stuff on what other people have done and I just can't believe that something that a lot of people are using is based on an assumption that there is a rate of 470,000 lines of code. I just couldn't believe it that somebody would seriously propose that and other people would use it.

And yet, you know, what happens. You give it a name, then somebody else is desperate to find something. Some say oh, this is, you know, called whatever, the pyramid.

MEMBER BLEY: Something we can sign.

CHAIRMAN APOSTOLAKIS: Yeah, something we can sign. And then all of a sudden, it acquires a life of its own. I mean, if you read what they are doing, you are just -- if I had hair, I would just pull it out, you know what I'm saying?

Now, where are we now? We're still on the second slide?

MR. KURITZKY: Yeah. This just ties it all back to where we are right now. We agree with the comments that the Subcommittee is making here. And I think that the staff as a whole is going to look at the various parts of this, you know, problem, this area, as Russ mentioned, as part of the update to the five year Digital I&C Research Plan.

But to bring it back to this project, we have not gone into this work presuming that we can go ahead and just include these models into a PRA, even though we haven't thought out the software issue very thoroughly. What we are doing and the objective of this work is to see where we do stand with trying to put these models in. Where are the hard spots? Software clearly is one of those. Software quantification clearly being one of those hard spots.

There are other hard spots and that's what this work is trying to do. We're trying to dig into the systems, see how we would actually model them and see where the hard spots are. If the only hard spot in the whole thing was just software reliability quantification, then we could sit there and just focus our efforts on trying to resolve that problem or decide that it's not really resolvable.

But there are other problems, too, which we are going to discuss as we go through these presentations. And so those also will need some -- look now, as far as which one you should do first and prioritizing them, that's --

CHAIRMAN APOSTOLAKIS: I would like to understand better and I'm sure the gentleman from BNL will speak when we have opportunities on this thing. I couldn't figure out after I realized that this was only hardware, although I know you complained it's not just hardware, but anyway, let's say it's hardware only. It excludes software failure and everything else.

What is it that made this analysis unique, the digital systems, I mean? Why wouldn't if one wanted to analyze say, pick a standard component with, I think it's a couple of thousand components, these are generators and you can go down to little things, could I do that? And then what benefit would I have from that? I mean, go down to the little subcomponents, sub-subcomponents of diesel and have Markov models. I think that's what you are doing now.

You are really going down to extreme detail. Are you hoping to back up at some point and start treating things in a more global sense?

MR. KURITZKY: That's what we were going to -- we can't answer that question right now. The reason that you can treat a diesel generator at a high level, even though there are many of those parts, and I have modeled into those many parts in the past, is the fact that you have data at the higher level. So you do not need to go to that level. And there are no dependencies that have to be accounted for at that level that you are not aware of and that you can't explicitly treat without going to that level.

With the digital system, there are certain features that can influence the -- that we believe might influence the reliability of a system. To get to those features, you need to go down to that level. Okay. And that's why we end up with a very complex model at the detailed level.

Now, it may ultimately turn out that those features do not really make that big of a difference in the overall number. And there is no need to go to that level of detail. We can just accept the model at a higher level, like was done in the AP1000 or ABWR PRAs and not go to that level of detail.

But we don't know that. That's the purpose of this work is to try to explore and see how important those -- how important it is to go to that level of detail and how practical it is to go to that level of detail.

MEMBER BLEY: I just want to say something on that. Four years ago or so, around the time of WASH-1400 and a little after, people started doing models at that level on things like diesels, on other kinds of equipment, because they were worried, same thing, about this wire goes through these contacts and through our B contact. Let's put all of that in and you could build models. And you could find some data. You found data from the Army and other places.

Every time that was done, every time that I saw an analysis done that way, the answers came out unbelievably high. High to the point that they were clearly not in concert with the way the real world was behaving. I've got some ideas of why that happens and probably it's when you get down to that level, the data might not fit your specific case or there are little conservatisms built in all along the way, but it just happens over and over.

I guess maybe doing it at this level might give you some understanding, but history kind of tells us you probably don't have -- get results that are meaningful at that level. And I wonder if you have thought about that.

MR. KURITZKY: Well, beyond thinking about that, as we will talk about with -- and those are very good points and I have experienced many of those same things myself in doing peer raised in the past. But as we will show later on to give you some of the insights and results from the first benchmark study that we are nearing completion on, we actually have calculated the failure probability at that detail level.

And the result is not really out of line with what -- there is not a lot of operating experience that we can bounce off against. But what limited stuff we were able to obtain, it's in the ball park. It's not coming up with an excessively conservative number when you do an exact Markov calculation on it.

So I am sensitive to that concern, because I have run into it myself, but in this case, at least so far, it hasn't shown up as a big issue. But the bigger point again is in those cases in the past, we have been able to live with the higher level. We saw that the detailed level came with a conservative number, but we were able to get enough data at the higher level that we could stick with that higher level.

The problem with the digital system was we don't have that luxury. Okay. So there may be in the future or there may be more data out there that just hasn't been all gathered up together and used in a proper way that we could avoid the need or we may decide that even if we can't get great data at the high level, it's still good enough.

MEMBER BLEY: Just two points on that and then I'll listen some more. Back at that time and actually for 10 or 15 years after that, we were getting numbers pretty far wrong, because our success data tended to be off by factors of 10 to 100 until we really got into operating plants and looked at how all the tests were done and that sort of thing. That may be a problem here.

Also, by really studying the failure records and understanding what happens in individual failures is where you've got a good understanding of those dependencies you talked about and how you might handle them at a higher level. So to me, it all comes back to that. Really understanding what has been going on can let you model at a higher level where you are looking at the big picture thing tracking, you know, the interactions.

MR. KURITZKY: Right. And I agree. And again, as we go through this example, these pilot studies so to speak, that's one of the things we're doing. We're going down that level. We're learning about the system. You're going to hear, I think, Louis will probably talk or maybe Gerardo will talk about a couple of examples where we have identified failure, you know, of system failure component failure modes that leave the system in failure that you normally wouldn't have picked up if you hadn't gone to that level of detail.

We have a couple examples of that. And it may be that you just -- that's information you want to learn about for your model, but you don't end up having to model the system down at that level. You may ultimately come back up to a higher level, but there is a lot to be learned by going to that level and at least in these pilot studies, we need to first see what that is going to tell us without just assuming that, hey, we just don't need to go to that level of detail this time. Let's not even explore it.

MR. MARTINEZ-GURIDI: Let me elaborate a little bit on what Alan is saying. One of the reasons why this analysis is unique is because for a lot of systems, since they have been operating for a long time, we know pretty well the failure modes of each component. For example, for this to generate the failure mode is first to start or first to run for its mission time. That's pretty much what it has.

For these two systems, the point that they can have a mind of their own and partly because they have software and partly because they are very complex. So there may be some failure modes that we are simply not aware of. We simply don't know how the component is going to fail. How is it that it's going to fail? And when it fails in a certain mode, what is going to happen? What is going to be the impact on the system and why it's going to be impact at all on the big picture on the other systems and the plant?

So if we don't go to a level of detail about analysis to understand why the failure modes, we simply may be missing important failure modes. And the issues, a priori, we don't know which failure modes are maybe relevant or risk significant or significant to safety of the plant and which are not.

So we have no other choice but to go to a level of detail where we can have some confidence that we have tried to catch all important failure modes.

CHAIRMAN APOSTOLAKIS: You said, Alan, earlier that the work that is presented in Appendix C had to be completed by Brookhaven sometime in the past. And yet, if you read this report, you see no reference to error force in context that you are trying to identify those. Why is that? I mean, each project has its own goal and then you forget about it and move on?

Why don't you mention then that this report is going to look for these error force in context or part of what constitutes an error force in context? Why is that different?

MR. KURITZKY: Well, the issue of -- the report right now doesn't refer to error force in context. The report right now specifies error force in context is a concept involved in quantifying software failure probability.

CHAIRMAN APOSTOLAKIS: No, because, you know, the context itself depends on the failure modes, does it not? I mean, what may happen.

MR. KURITZKY: What is the use of that context? What do we use the context for?

CHAIRMAN APOSTOLAKIS: Sorry?

MR. KURITZKY: What will we use the error force in context for? What would you use it for?

CHAIRMAN APOSTOLAKIS: To understand when the thing fails. It's the context that forces an error.

MR. KURITZKY: Right. And I'm not -- I'm no expert in this area. But in my understanding is that context is used to help us come up with, you know, quantifying the failure problem.

CHAIRMAN APOSTOLAKIS: No. It's a

necessary task before you start quantifying. It includes everything else. If you read ATHENA, for example, the error force in context is a major effort trying to identify what kind of information reaches the operators or what equipment are available and so on. And this is the context within which some action will be taken.

Now, in your case here with software, again, what kind of failure modes can be triggered by what conditions? That's really the way I see the error force in context.

MEMBER SIEBER: That's one of the more difficult processes in troubleshooting. You try to identify those oddball cases where you have a numerical error. Usually the logic errors show up first and it's the numerical errors that lay hidden. And error force and context from a troubleshooting standpoint is central.

And so your kind of analysis it should also be essential.

CHAIRMAN APOSTOLAKIS: Yeah, it is. It seems to me it is contributing to the identification of the error force in context. That's the way I see it, the way you are doing here. Is that true, Louis?

MR. CHU: In a way. I think later you

will hear about the simulation tool, which actually runs the software. And in our analysis, we basically look at postulated hardware failures. And Alan mentioned, you know, we have a couple of examples in which we identify the system behavior, which is unexpected or it's somewhat kind of a -- you can probably say it's a potential weakness of the design.

But then is this a design of the software or hardware? The software has a very big role in it. In that sense, in doing our simulation analysis, this kind of problem reveal itself. You know, I think in the same way that the EFC method is intended to do.

CHAIRMAN APOSTOLAKIS: If I take Appendix C and I say this is a great idea, I really want to apply the concept that they have there, then I read one volume with the main report and several volumes with Appendices to this one, and I see the word EFC nowhere, I'm confused now. Is this going to help me with Appendix C or not? How is it helping me?

I mean, we can't just complete projects and then start another one and ignore everything else.

MR. MARTINEZ-GURIDI: The reason there is no connection is because, as Alan was saying before, Appendix C was really done as part of another project that was kind of --

CHAIRMAN APOSTOLAKIS: And that's my compliant.

MR. MARTINEZ-GURIDI: Yeah, I understand your complaint.

CHAIRMAN APOSTOLAKIS: That's exactly my complaint.

MR. MARTINEZ-GURIDI: But that's why there is no connection. I mean, not that we are neglecting this.

CHAIRMAN APOSTOLAKIS: Do you realize what you are saying? You are saying that if you complete the project, then it's over, it's done, let's forget about it, start another project.

MEMBER SIEBER: Two or three of them.

MR. MARTINEZ-GURIDI: No, what happens is that -- what happens when we start giving you projects, the scope of the project inclusive of reliability. And then --

CHAIRMAN APOSTOLAKIS: But it's not part-- I mean, I repeat. The error force on context is not a concept that is used for only quantification. Because it's the context within which something bad will happen. And I assume that by looking at failure modes, you are contributing to the identification of that context. Maybe it's not right to evolve the concept of error force in context in this case. I don't know.

But I mean, it would be nice to see some connection. I'm sure you can make a connection. As you say, as far as I'm concerned up until two minutes ago before you spoke, the only method I knew that really identified context was this prime approach of the DFF. Now, you're telling me your approach does the same thing. That's great. Let's explore it.

MR. CHU: I think in a sense our -- the simulation tool you will hear a lot more.

CHAIRMAN APOSTOLAKIS: If I recall from some of those analyses in the past, there were situations where the variable was -- you know, variable in this interval variable why is it this and that and that and all of a sudden you have a failure and you don't know why.

MEMBER SIEBER: Yep.

CHAIRMAN APOSTOLAKIS: Because the software in between, you know, leads to a failure and that, in my mind, is a context.

MEMBER SIEBER: And it may not always lead to that failure.

CHAIRMAN APOSTOLAKIS: It may not always lead to that failure. We really have to dig into these things and understand them much better.

MR. CHEOK: And again, I think we need to go back to the beginning of the -- to find the objection of the study as to see what rave on -- becomes traditional methods. To look into the EFCs at this point and to see what fits in digital I&C is beyond the state of the art, at this point, and I don't think it's the objective of this report.

CHAIRMAN APOSTOLAKIS: Yeah, we keep hearing those things many times, not just today, scope and so on. Well, this Committee really does take into account the scope to some extent, but we are really interested in what the Agency will have in terms of useful tools at some point. So we can't just ignore the bigger issues, just because of your scope was limited. Okay.

So, you know, we really have to understand where we are going with all of this.

MR. KURITZKY: This is Alan Kuritzky. Yes, the -- Dr. Apostolakis, I agree, we agree with you and we welcome the input from the Subcommittee on these more broader issues. I think what Mike was trying to emphasize was that what we are here to present today is to work in this NUREG/CR, that's not part of that. I recognize that there are issues that are of much interest to the Subcommittee and to the staff that are beyond what the scope of this project is and we welcome feedback on them.

We are not here prepared today to debate them at length, because they are not part of the focus of this presentation from your point of view. But we will certainly take back whatever input you are willing to provide us, so we can factor into future decisions.

CHAIRMAN APOSTOLAKIS: But it really doesn't have to be part of the scope that you have to consider EFCs. I mean, that's a technical thing beyond the issue. Anyway, shall we go on?

MR. KURITZKY: Yes. Okay.

CHAIRMAN APOSTOLAKIS: Okay. You told us about the scope.

MR. KURITZKY: Right. We're on --

CHAIRMAN APOSTOLAKIS: So where are we going to go? Which slide?

MR. KURITZKY: Okay. Task plan for this project, that should actually include all the things we --

CHAIRMAN APOSTOLAKIS: We talked about this, didn't we?

MR. KURITZKY: No, we didn't do this slide yet.

CHAIRMAN APOSTOLAKIS: All right.

MR. KURITZKY: I mean, we probably touched about every slide in the presentation at some point already this morning, but we haven't actually had this slide.

MEMBER SIEBER: But not good enough.

MR. KURITZKY: That's right. Okay. The tasks involved in this project, first off, involve developing some draft criteria for what we feel should be in a digital system model. And that -- those criteria, we actually talked to some extent to the Subcommittee back in April of last year on that and we received some further feedback on those draft criteria and have since updated those criteria.

Those criteria could eventually support any type of regulatory guidance that is put out on digital system models or provide the technical basis for doing risk evaluations for either current or new reactors. In fact, I think the draft interim staff guidance on -- including digital system models and new reactor PRAs that the Subcommittee was briefed on a few weeks ago and that the full Committee was briefed on last Friday, does, in fact, take advantage of some of that work. There was some cross connection there with some input to that ISG.

The next task was to select two traditional reliability methods to do the test case, to do the example cases and apply them to two different systems. And I think as you -- as the Subcommittee has heard before, those two sample systems are a digital feedwater control system and a reactor protection system.

The two methods that were selected were the event tree/fault tree method and the Markov method. Again, this sublet is very -- well, we have beaten this one to death already. But the idea was that this project scope does not involve major advancements in the state-of-the-art. It was specifically carved out to just look at where we stand right now. What are the capabilities and limitations that exist right now in these traditional methods?

And so we were not looking to advance the state-of-the-art. We were not looking to further work in areas that we're not already well-established. And a perfect example of being software reliability quantification.

Once we complete those models for the example systems or what we call benchmark systems, we would then compare the results of those models to the criteria that were developed in the first step to see where there may be areas that further research can improve the models.

We're going to talk about some of those areas that we have identified later in this presentation and, of course, software reliability quantification is on that list.

And the last step of this work is to take those models and see how we could put them into a PRA. One of the ultimate goals of this work is to get guidance on how you would include digital system reliability models in the PRA. And for the event tree/fault tree method, we would expect that to be relatively straightforward. For the Markov method it would, obviously, require a little more creativity to get them to -- get them integrated to the PRA.

CHAIRMAN APOSTOLAKIS: Is the Markov approach, does it deserve to be called traditional PRA? Does anybody use Markov models in PRA?

MEMBER BLEY: Yanni.

CHAIRMAN APOSTOLAKIS: Huh?

MEMBER BLEY: Yanni.

CHAIRMAN APOSTOLAKIS: He used it to get the degree.

MEMBER BLEY: No, he used it since then.

He has been using it. And they have used it in -- their friends up at the same place have been using it in proliferation resistance risk analysis work.

CHAIRMAN APOSTOLAKIS: Those were transition rates. I have no idea.

MEMBER BLEY: They are never -- they are made up so far in that area.

CHAIRMAN APOSTOLAKIS: All right.

MR. KURITZKY: Okay.

MEMBER BLEY: I'm going to sound like I'm whining. I'm just going to say it once more. It's not beyond the state-of-the-art to study the failure modes and understand them. Go ahead.

MR. KURITZKY: Right, yes, that we agree. We agree. Okay. Now, where we stand with the work right now. As we have been discussing there was a draft NUREG/CR that we have put out on the initial activities for this work that involves the development of the draft criteria, the selection of the two traditional methods that can be applied to the benchmark studies.

We documented the process that we were going to use to develop those models and quantify those models and we have also come up with a preliminary list of areas that we feel additional research would help to improve the models.

That draft NUREG/CR has received a fairly extensive amount of review. It was sent over to both user offices, Nuclear Reactor Regulation and Office of New Reactors. It was looked at by both their PRA Departments and their Engineering Departments. It was -- we had a panel that we put together or a group of reviewers that we specifically tasked with looking over the report and those included a couple of members from industry, a foreign regulator and a member of another national laboratory.

CHAIRMAN APOSTOLAKIS: What does the industry think about this? Do you remember?

MR. KURITZKY: Well, we have a number of comments from the industry. And let me say the last thing also it was put out for public comment. And public comment, we also got more response from industry members from there, besides just the ones that were on our panel. And so there is a spectrum of comments as you could expect.

Many issues that you brought up have been brought up by some of the industry members also. Some, in fact, say, one particular commentor said, let's not worry about this particular modeling right now, digital system, let's focus on software, because that's the big issue. Let's just work on that.

On the contrary, other industry organizations have come back and said we don't need to -- let's not hold up using risk modeling and risk insights just to solve this software problem which may never get solved anyway. We should know enough now that we can move forward. So you get both sides of the spectrum on that.

CHAIRMAN APOSTOLAKIS: Which is an unhelpful statement. Let's not do this. Let's move forward. How?

MEMBER BLEY: Solve the easy problem.

CHAIRMAN APOSTOLAKIS: How? It depends in depth, right? Let's go.

MR. KURITZKY: Well --

MEMBER BLEY: Did you get comments? You know, this might be state-of-the-art, but is it the state-of-feasibility? Did you get comments about that?

MR. KURITZKY: I don't -- we got -- we did not get a lot of comments about that. I think one of the reasons being because software wasn't brought up a lot in the report and that's where you would get that concern more. So I think that where we have heard from initially on numerous occasions that some of the more advanced methods if we're trying to model digital systems, they are concerned about the state-of-feasibility. We did not get too many comments I don't think in that regard.

MEMBER BLEY: So they aren't troubled by the depth of modeling?

MR. KURITZKY: Well, some do. We do -- some say that they don't understand why you necessarily need to go to that level of detail. I think we did get some comments on that. But again, it's not as -- was not -- you know, because we were talking about event tree/fault tree methods, people are more comfortable with and which industry is more comfortable with. I don't think it had quite the same effect.

MEMBER BONACA: The digital feedwater control system I&C, to what degree do you have the regional FMEAs?

MR. KURITZKY: For the one that we used in our benchmark?

MEMBER BONACA: Yeah.

MR. KURITZKY: We actually had a hazard analysis from the prototype plant.

MEMBER BONACA: So all this information, it was developed for the design that is available to you?

MR. KURITZKY: Yes, it was. Right. The one issue is that we did have documents from the prototype plant of different years and they did not always match up. Sometimes one document might make you think one thing about how the system works and another document would be in conflict. And unfortunately, we weren't able to resolve those, because we were no longer -- the prototype plant was no longer supporting the work. And so we had to just make assumptions and move forward.

Being that we're just doing a proof of concept study, it wasn't that essential that we had the exact operation, but we were able to get a lot of information from the plant. Okay.

Okay. So we received all these comments back from the various sources. We incorporated them and developed the final version of the report, NUREG/CR-6962, it now has a number, and that's going to go to publication shortly. Two major differences between the final report and the draft report that I want to point out.

One of which has clearly already been made aware of is that the appendix on software failure analysis has been removed for the reasons we have already stated. In addition, there was, in the draft report in Section 2 or Chapter 2, some discussion of four applications of traditional methods, a couple of new reactor PRAs, I think, and some other methods. And we compared those against the criteria.

That whole section was removed, because it was felt that it didn't really support the work that well and was more -- causing more arguments over whether or not it was appropriate to even compare those applications to those criteria, since those applications were not developed for the purpose of what one might use those criteria for. So those have been removed from the final version of the report.

The last thing I want to mention as far as the status is, as I mentioned earlier, once the first NUREG went into review mode, we continued with the technical work on the first benchmark. We started the technical work on the first benchmark. And if so, we are actually well along and almost complete with that work. We will have another NUREG/CR that will come out on the results of that which we will share with the Subcommittee when it is available.

And we're going to also, as I mentioned, give you a few insights and some preliminary insights and results from that work later in the presentation.

The criteria that we developed for evaluating the digital I&C models, again, we talked about this April of 2007. There were 52 criteria that we came up with in about nine broad categories, which cover all of the important areas of the digital model and the documentation of those models. They are based on experience in both PRA and with digital systems of the study team and also on review of literature, looking at journal articles on probabilistic modeling of digital systems, NUREG reports on digital systems, new reactor PRAs and things like that.

CHAIRMAN APOSTOLAKIS: 52 criteria that sounds like too many.

MR. KURITZKY: It does when --

CHAIRMAN APOSTOLAKIS: 52 of anything is too many.

MR. KURITZKY: It does when someone suggests that we have a slide, a backup slide, that listed the criteria in case you wanted to discuss that. I'm not making a backup slide with 52 criteria. If I had eight of them, I could put it up on the board, but not with 52.

CHAIRMAN APOSTOLAKIS: Are you sure they don't overlap? They must overlap. I mean, 52.

MR. KURITZKY: Well, I mean --

MR. MARTINEZ-GURIDI: What happens is they are very -- pretty detailed criteria. But I don't --

CHAIRMAN APOSTOLAKIS: So what if you go to more detail, it would be 104? 52 criteria it seems, to me, is unmanageable.

MR. MARTINEZ-GURIDI: They are categorized into nine broad categories. Like for example, one is level of detail analyzed on the data.

CHAIRMAN APOSTOLAKIS: Well, level of detail. Let me understand that. What do you mean by level of detail?

MR. MARTINEZ-GURIDI: Well, basically, what we are proposing is that a model should contain enough level of detail to capture all the detail features that can affect the system reliability. Now --

CHAIRMAN APOSTOLAKIS: Which you don't know yourself.

MR. MARTINEZ-GURIDI: Which we don't know, so that's -- we agree that that's a very fussy situation. But I believe we wanted to mention that this is a very important consideration, that's why we included it.

CHAIRMAN APOSTOLAKIS: But the criteria is helping you to do what, to judge other models?

MR. MARTINEZ-GURIDI: To judge one model that has already been developed.

CHAIRMAN APOSTOLAKIS: How can you judge a model based on this criteria, if you, yourself, don't know what sufficient level of detail is? Well, you don't know, right? You just admitted that you don't know. We don't know. I don't know. So you pick up now somebody else's model and you say oh, no, no, it doesn't have sufficient level of detail. How do you know? You don't know what the sufficient level of detail is.

So I would use criteria to establish my criteria. If I don't know what the criteria is trying to say, I shouldn't include it as a criteria.

MR. KURITZKY: Yeah, I think maybe the word criteria may be misleading and that's why we mentioned in the beginning that these criteria may provide input to some guidance, because they are not that -- those 52 items is going to be a checklist and that a reviewer of some application is going to have to then check to make sure that that hits off of --

CHAIRMAN APOSTOLAKIS: I'm very skeptical about these things, because 20 years ago, Sergio and I had a research project together. And people -- some people would come and say oh, but this is too complicated. That was crazy. What is your criterion to declare this as complicated? How do you know it's complicated? Is the PRA complicated? I don't know. Now, we're doing it routinely, so to some people, at least, it's not.

But isn't the issue of how complicated the model is tied intimately to the complexity of the thing you are analyzing? If what you are analyzing is complex, then maybe your method for analysis is complex too. So just to say oh, no, no, so the message was unless you show me a secret event tree or something, this is no good.

You know, these are the things that drive researchers crazy, because people who don't really understand the problem come up with these criteria. So I'm not saying that you guys did the same thing, but we just got an example where it was not clear how you would use the criteria about the appropriate level of detail. 52 sounds too high to me. I don't know about you guys, but --

MR. CHU: What happens -- sorry.

CHAIRMAN APOSTOLAKIS: Louis?

MR. CHU: I think the criterias that we came up with, we probably can look at them as what a perfect model should satisfy.

CHAIRMAN APOSTOLAKIS: But you don't know what the perfect model is. You, yourself, don't know. So how are you going to judge --

MR. CHU: Oh, like that example, a perfect model should be developed to the level of detail to capture the detail design features of the system.

CHAIRMAN APOSTOLAKIS: But this is a model in --

MR. CHU: Yes.

CHAIRMAN APOSTOLAKIS: We believe in that, you know. I should love my mother, yes.

MR. CHU: But the state-of-the-art may not be good enough.

CHAIRMAN APOSTOLAKIS: I do, I do.

MR. KURITZKY: For the official record.

CHAIRMAN APOSTOLAKIS: Yeah, thank you, Alan. In case she reads it, right?

MR. KURITZKY: Again --

CHAIRMAN APOSTOLAKIS: Anyway, I mean, it seems to me it would be useful for you guys to go back and --

MR. MARTINEZ-GURIDI: But in some cases, it is pretty obvious.

CHAIRMAN APOSTOLAKIS: Like what?

MR. MARTINEZ-GURIDI: Like the level of

detail that is at the very high level.

CHAIRMAN APOSTOLAKIS: But it's not practical, Gerardo, that's what I'm saying. That in my mind, a very important, I don't know, feature of a criteria should be that it's practical. That somebody can use it to do something. I mean, to say --

MEMBER BLEY: And the way you know that is, in my understanding, the ways in which it has failed and the things that can go wrong.

CHAIRMAN APOSTOLAKIS: Yeah, yeah, yeah.

MEMBER BLEY: I mean, if you applied the same criteria to a circuit breaker, you would have a very big fault tree.

CHAIRMAN APOSTOLAKIS: Yeah. Anyways, sometimes, you know, when we develop these criteria, we tend to get carried away. In this case, you should revisit them. It's a natural thing to do.

MEMBER BONACA: Actually, I think it's a pretty coarse gate. I mean, it says that you should capture the design features that could affect reliability. I mean, if, you know, the model is so poor that it misses a measured feature, I can buy that.

MR. MARTINEZ-GURIDI: And actually, all the criteria help you identify whether something important is missing.

MEMBER BONACA: Yeah.

MR. MARTINEZ-GURIDI: That's why --

MEMBER BONACA: That's the way I would view the value of that.

MR. MARTINEZ-GURIDI: Yes.

MEMBER BONACA: Criteria would be the level.

MR. KURITZKY: Okay. Let's see, where did we leave off? Okay. So those criteria, again, we emphasized that they were developed based on the knowledge and experience of the team that put them together, so they were not expected to be the end all or final word on the criteria. And essentially, what things we would be looking for in a good model of a digital system. So we subjected them to some detailed review.

We empaneled a group of practitioners in the areas of PRA and digital systems. We brought them up to Brookhaven National Laboratory last May, had them go through that set of criteria. We got quite a bit of comment back on those criteria. What was in the draft report, in fact, was significantly different than what was in the initial, I think, cut -- you know, in a lot of ways different than what was in the initial list that was provided to that review team, because we got a fair amount of good input back at that meeting.

In addition, because those criteria are in Chapter 2 of this report and has gone out for quite a widespread review and comment, we have also received quite a bit more comment on those criteria from many other parties. And all that input has been used and is reflected in the final version that show up in the draft final NUREG, which, apparently, did not receive, but we can certainly make sure you get that new copy.

They are not substantially different than what was in the draft version that you have. The biggest changes occurred after the review panel and BNL in May of last year and so those were already reflected in the draft version that you have right now.

Again, to mention that those criteria have been used to provide input to the ISG for new reactor digital system PRA, digital system models for new reactor PRAs. And also, there is an activity, an Organization Economic Cooperation Development, OECD organization, Nuclear Energy Agency Committee for the CSNI Committee, for the safety of nuclear installations, have a number of working groups.

One of them is working with risk, which deals with risk activities, PRA review activities and that group has an activity under way now to look at digital system modeling and digital system reliability calculation. The U.S. NRC is the lead for that activity and there is a meeting that is going to be scheduled for later this year that is going to address this particular topic. It may have the same issues that we're discussing today. And that list of criteria was used to help frame the scope and the content for that meeting.

CHAIRMAN APOSTOLAKIS: Do you know when this meeting is?

MR. KURITZKY: It was originally scheduled for April of this year. We would have already -- it would have been last week, I think, yeah, but unfortunately, there were some problems with some international partners and we now have to go back to the --

MEMBER BONACA: That's in Paris?

MR. KURITZKY: It was going to be here. It was going to be actually in Long Island actually, which I think one of the reasons no one wanted to come. No offense. Nonetheless, we are trying to schedule it for later this year. It's going to probably be -- we are hoping to do it in the late summer. It's probably looking more like fall, at this point, but we will let you know once we get further along on scheduling that.

Okay. What I would like to talk about now quickly is just the overview of the process we used for applying these two traditional methods to the digital feedwater control system for -- to be used in the first benchmark study. Bullets 2, 3 and 4, you're going to get detailed presentations on from Gerardo and Louis, so I'm just going to touch it real briefly.

The first thing that we had to do, of course, was look in detail at the system. As has been mentioned many times this morning, a rigorous understanding of how the system works and how it can fail is crucial to any type of reliability model and that was the first step that we had to undertake. The digital feedwater control system is actually a very complex system and so it was quite an undertaking, but we needed to have a good understanding of the digital features, especially those that can impact system reliability, the various components and their dependencies for us to go ahead and do the failure modes and effects analysis.

That was the next step and we needed to

perform that in order to identify the failure modes, the component failure modes that can lead to DFWCS failure and the impact of those failure modes on the system function. Again, you will get a detailed discussion on that from Gerardo right after this presentation.

The results of that FMEA were then used, that set of component failure modes and the effects on the system were then used to develop the models, the Markov and fault tree models. And in order to quantify those models, we also had to obtain, estimate parameters for things like component failure mode, failure rates and failure mode distributions. Particular component failure modes, component failures may -- they can have different failure modes and there is a -- associated with those modes we reach component failure. And we need to get statistics or data on that also. And that's something that Louis will talk about later.

Finally, we reiterated in the last bullet, a big topic this morning, that quantitative software reliability is out of the scope of this work. It is not out of the scope of things that theoretically should be looked at. We also agree with that.

CHAIRMAN APOSTOLAKIS: And yet, you are

proceeding with the benchmark study.

MR. KURITZKY: That's right. The deal with the model --

CHAIRMAN APOSTOLAKIS: Is anybody worrying about reliability? You have a power task for, you know, as we said earlier, whether it can be done. I mean, it seems to me we are postponing the really tough issue of dealing with software failures. We are beating the stuff that we more or less are familiar with to death. No? I mean, what are we going to learn from the benchmark study? We will still have this problem that we will not understand software failures.

MR. KURITZKY: We want to learn what else we need to focus on if there was other things we need to focus on besides just software. I think we recognize that software is an issue that needs more work. So we know that. And whether or not activities are in place and ready to look at that and whether there will be future activities to look at it more, that's a valid discussion item.

The idea is are there other things in digital system line that we need to look at besides that. That one is an easy one. We know that one. Are there others?

CHAIRMAN APOSTOLAKIS: But isn't this the second five year Research Plan we have had? I think there was one before this. I think there was one, right? Steve probably remembers. Okay. So there was one in 2001, a second in 2005. We are in the year 2008. And we are still postponing the really hard problem. If you look at it from that perspective, it's not very encouraging.

I understand in the local thing what you are doing here. You want to learn more, but if I look at it from that perspective, assuming we started in 2001, which is probably not true, but let's say we started in 2001, seven years later, we are still postponing looking into the really hard part of the problem. That's not very good. So let's complete this part of the presentation.

MR. KURITZKY: Okay. All right. So the capabilities and limitations of traditional methods. As documented in the NUREG/CR that you have, both the traditional fault tree and Markov methods are well-established. They are well-understood by the reliability community. They have been used in countless applications, all the nuclear power plant PRAs use those methods, use the fault tree methods, event tree/fault tree methods.

The Markov methods have been used, I think, in a couple of limited nuclear plant applications. They have been used for many other applications outside the nuclear industry. Both of those methods are believed to be fairly powerful and flexible methods, in that they theoretically can model many of the specific digital features that are important to digital system reliability, including identifying the various dependencies of those parts of the system.

However, both of those methods do need to be supported by good engineering analyses. Things such as identifying failure modes. The FMEA as Dr. Bley has repeated a number of times, you go down to you do need to have a very rigorous and hopefully complete look at what types of failure modes are out there. And that's going to help dictate how you are going to model your system.

Also, the issue of data. You need to have good data analysis if you want to actually come up with quantifiable frequencies or probabilities. The software, the issue of incorporating software failure contribution into the model, again, another, what we could call, supporting analysis that needs to be included in the overall digital system reliability model.

Particular capabilities with the event tree/fault tree model is that it's very integratable with plant PRAs. The plant PRAs are in that use of event tree/fault tree, so obviously, that's the easiest one to add into an existing PRA. Another particular capability, the Markov method is that it can treat the order of the failures. Whereas, a fault tree whatever orders are in your fault tree cutsets, whatever component of basically event tree in your fault tree cutsets, the order of those cannot be -- is not reflected.

However, when you use a Markov method, you can actually reflect the order of the failures. And that actually is something that becomes important. It's one of the things we found out from digital systems order is important, because there could be a component failure mode in a digital system. But if it fails first, it will lead to system failure. But if there is something else that fails first and it fails second, it does not lead to system failure. So that ordering is something that should be considered in the modeling.

Then the limitations of these methods. As we stated previously, by definition, these methods do not explicitly count for the interactions between the system and the plant process, the plant physical processes or the timing of those interactions. So they have that limitation.

CHAIRMAN APOSTOLAKIS: Its that a very severe limitation?

MR. KURITZKY: Well, that's one thing that we were trying to get some insight on. They do implicitly consider those interactions in some limited fashion. For instance, event trees and fault trees based on the nodes in the event tree and the order of them or the system's success criteria, you get some approximate implicit consideration of those. But how important that is, that is really one of the things, you know, as we will mention in the -- one of the later slides.

We're going to take the results of our study. There is the parallel project looking at dynamic methods which does, in fact, address those interactions. And so ideally, we would like to be able to compare and see how important they are. Unfortunately, that comparison is not going to be that straightforward, because there is some significant differences in the boundary conditions between the two studies that were done on the DFWCS.

CHAIRMAN APOSTOLAKIS: But I mean, it seems to me, especially in your benchmark, you have a feedback on control system, you know, that inputs come from certain variables being in a certain range, right? So clearly, an event tree/fault tree in the nodes are not really helpful there. I mean, you really have to know what the temperature is in this range, the pressure is in this range, the flux is in this range.

So it seems to me that dealing with parameter values is very important here. These are input to the digital I&C.

MR. KURITZKY: It's potentially important. The question is how important is it going to be ultimately to the quantification of the system reliability or probably --

CHAIRMAN APOSTOLAKIS: Assuming we want to quantify.

MR. KURITZKY: Assuming we want to quantify. That we don't know yet.

CHAIRMAN APOSTOLAKIS: But even for the behavior, I mean, I'm surprised you are saying that. Isn't the behavior of the system the commands it is going to generate? Are they dependent on what is happening?

MR. CHU: George, this relates to our simulation model again. We ran the actual software and read sensor input. So the sensor input comes from the plant information. So the input sensor signals correspond to that of a full power operation. So in that sense, our model, you know, account for the full power calculation.

CHAIRMAN APOSTOLAKIS: But what are you simulating? I mean, are you simulating all possible values of the parameters?

MR. CHU: Well, that's a part of the FMEA presentation that you will hear more about.

MR. KURITZKY: But to directly answer that question, no, we don't. We're not looking at the whole range of parameters. That, in fact, is what the dynamic modeling, what we call dynamic modeling, is addressing. This traditional modeling does not address that whole range. Now, when we get to the software quantification, as you have probably seen in Appendix C, I mean, you talk about looking at the whole input space and there you would have to address that issue more completely.

But as far as the model that was done under -- in this project under this NUREG right now, as Louis was mentioning, we consider a set of conditions. I think it's just kind of like a snapshot of conditions that we input to the software. It doesn't go over the whole range of, you know, feedback, in the full spectrum of potential input parameters.

CHAIRMAN APOSTOLAKIS: Okay.

MEMBER BLEY: I have a question on the Markov. Markov has a very strong assumption that the transition probabilities at a particular point are independent of the path by which you got there. Are you convinced that's a reasonable model for the things you are modeling?

MR. CHU: Yes, I think I'm actually pretty happy with the Markov model and later will discuss.

MEMBER BLEY: So there's no historical impact on transition probability? You are convinced of that? Coming out of support systems that you model earlier or anything like that? Have you found a way to take care of it? And that's a basic Markov assumption, right? Where I am is what happens next is completely independent of how I got to this point.

CHAIRMAN APOSTOLAKIS: There is no memory, in other words.

MR. CHU: Right, right. But the -- we have not come across.

CHAIRMAN APOSTOLAKIS: But have you looked?

MEMBER BLEY: Have you thought hard about that one? Because that's a very strong assumption.

MR. CHU: Okay. The way we look at it, we look at not just individual failures, but we also look at the order in which failure occurs.

MEMBER BLEY: Yeah.

MR. CHU: See one say there are -- we look -- we are looking at what's the probability of system fail during the one year operation? So you can have a failure sequence in which say you have one failure mode happen in January, another one in July, but it still -- the system is still working. And a third failure occurred in August that caused the system failure. In that sense that timing in which failure occurs is accountable in the Markov model.

That is the failure effect of the first failure exists and it's always there until the second failure occurs, then you have added failure effects. Until the third failure, the combined failure of that failed system. In that sense, maybe you can say the accumulated effect is accounted for.

MEMBER BLEY: I would have to look at that. You must be going through a different place in the model then or something.

MR. CHU: I think what --

CHAIRMAN APOSTOLAKIS: Getting to a state is important, but that means you have -- you cannot collapse the states. In other words, let's say you have a simple state, four component, four element and one state says all three are down in the trivial Markov model. Not digital, I mean, generally. If what you are saying is true, Louis, that you are taking into account the order by which they fail, then you do have an explosion of the state, with a number of states, because now one state that says three are down is not sufficient.

I have to know the order in which I reach that state.

MR. CHU: Right.

CHAIRMAN APOSTOLAKIS: So this state now will be broken up into, I don't know how many combinations, A, B, C, A, C, B, B, C, A, you know.

MR. CHU: Yes.

CHAIRMAN APOSTOLAKIS: That really multiplies the number of states.

MR. CHU: We look at merely on top of that.

CHAIRMAN APOSTOLAKIS: But you're talking about the Markov thing?

MR. CHU: Yeah.

CHAIRMAN APOSTOLAKIS: Just note how strong the questions are.

MR. KURITZKY: Right. I just point over there anyway. But, yes, you are going to get a discussion on that. Okay. And the last bullet we just talked about. That there is the potential for state explosion with the Markov model, for exactly the reasons we were just talking about.

Okay. Some preliminaries or candidate areas for additional research that came out of doing this initial activities of this work, many of them we just already talked about. The identification of failure modes and how complete we are in identifying the failure modes, that's obviously a very important issue. I think everybody kind of agrees on that one.

Also, determining -- just determining the effects of the failure modes on the system. When you get at the level of detail that the models are that we are putting together, at least here, it becomes difficult sometimes to even tell if a single, a particular individual failure, a single failure actually causes system failure.

When you try to look at combinations,

doubles, triples, etcetera, it becomes almost impossible. So looking into ways by which we can identify the effect of particular failure modes, component failure modes on the system is important. My next slide when I talk about the preliminary insights we will speak more on that.

Parameter database for the hardware, just coming up with good hardware data. No doubt there is proprietary data at certain manufacturers, vendors, what have you. It's probably a lot better than what we may have in the public domain. Certainly in the public domain, it's fairly limited as you're going to see when Louis talks later on as to estimation parameters.

I don't know how good it is in proprietary databases, but it's an area where we definitely could focus more attention. The quantitative software reliability model, obviously, is the 800 pound gorilla in the room. Treatment of uncertainties in this regard, we're talking primarily about completeness uncertainty and modeling uncertainty areas where we might want to look more -- in more detail. And HRA, both because of recovery actions with the digital systems, because a lot of times digital systems are dealing with automatic functions and there may be an opportunity for recovery, as well as the whole human-system interface issue that deals with having these digital control rooms, so that's another area that may warrant some additional work.

I think, in fact, work already is going on in that area. Okay. That pretty much talks about what was in the NUREG/CR that you already have. Now, as I said, we have already gone and completed almost the first benchmark study, so I want to give you a little bit of insight on what we have come up with on that right now. Again, you will be -- the Subcommittee will be briefed later once that report is in and we have had a chance to look at it.

But the biggest insight that has come up from that work is the fact that at the level of detail that we are modeling these systems, and again, that's at the level of detail where we feel you have to go in order to identify all of the features of the system that can impact reliability, you end up with a very complex model. So complex, in fact, that it's not practical to use the traditional methods or the Markov or the event tree/fault tree to identify which component failure modes lead to system failure.

That gets us to the simulation tool, which Gerardo is going to talk about in the next presentation that we -- that BNL put together to -- and it's based on the software, actual software of the digital feedwater control system to identify what failure modes or combinations of component failure modes lead to system failure.

Now, the output of that simulation tool is, essentially, all the components -- the combinations of component failure modes that lead to system failure. And they can be thought of essentially as the cutsets of a fault tree, except that they also consider the order. As we were just discussing, as Louis was mentioning, the order of the failure modes can make a difference as to whether or not it actually fails the system or not.

And so this simulation tool will track the order of those failures and determine which order combination results in system failure. All right.

The simulation tool was an important advancement for us, because we need it in order to be able to put the models together. However, it's still very time consuming and -- it's time consuming because of the sheer number of failure modes that need to be considered. So it would be beneficial, obviously, to further simplify that process and make it somehow more, you know, faster and more efficient.

DR. GUARRO: I hate to interrupt here, but there is something that comes to mind and talk about FMEA, the guide simulation. Those are both inductive analysis models. And in my mind, there is always a big question of completeness.

MR. KURITZKY: Exactly.

DR. GUARRO: When you do using that --

MR. KURITZKY: Either one, yep.

DR. GUARRO: In other words, the inductive give you guarantee of completeness within the assumptions of coarseness of the model you use, but inductive you are totally, you know, you just say okay, I assume something and see where it goes. But what if I assume something else, if you go somewhere else. So there is a big question there.

MR. KURITZKY: Yes.

DR. GUARRO: And so I will caution, you know, to use that as an approach without having a complimenting deductive way of looking at the whole picture, so that you can at least form an idea of what kind of space you are trying to explore.

MR. KURITZKY: Yes, Dr. Guarro. And I just flip back to the previous slide, that first bullet, in addition to what you're saying the need maybe to use a inductive approach to compliment that inductive approach. Also as you mentioned, that inductive approaches how complete you are in what you are putting into that approach is going to dictate how complete you are coming out at the other end and identifying the failure modes and how complete you are in identifying the failure modes is an important aspect.

So we have to make sure of that. And, you know, I think we are conscious that not to be overconfident in the completeness of what we're doing, because of the nuclear -- being the inductive nature of the approaches. We are definitely cognizant of that.

Okay. So I'm just -- very quickly preliminary results of the first benchmark. We used a simulation tool for the DFWCS to come up with the combination of failure modes that fail the system. As you mentioned, the order of those failures does make a difference. We have cases where failure in different orders would or would not cause system failure.

As Louis was mentioning, there is -- we had quite a number of combinations that came out. Using that simulation tool for the DFWCS, we ended up with a few hundred single failures, many, many thousands of double failures, millions of triple failures. We stopped at the triple level. Obviously, we could have kept going. It was quickly becoming somewhat unwieldy. We are comforted by the fact that the contribution to a system failure probability or failure frequency tends to decrease as the number of elements in the failure paths gets larger. And as you will see, some results that, I think, Louis will show you later, you do see that decrease in contribution as the failure paths get larger.

Nonetheless, what we worked out preliminarily from the first benchmark, using the Markov modeling, was a frequency of .08 per year for loss of automatic control of the digital feedwater control system within all of the limitations of what we talked about previously. Again, this does not include software failures and many other limitations.

We also went and quantified it not actually with the fault tree code, but using what would be a fault tree type quantification using the same software that we used to do the Markov quantification and we came up with a .21 PRA failure frequency that -- the difference and again, those differences, I think, are going to be discussed more by Louis later, but primarily being the fact that ordering of the cutsets is not accounted for in the fault tree quantification method and also the mission times of the component failures is -- that's approximate.

And so that also adds something to the conservatism in that calculation. But again, Louis will talk more about that in his presentation.

Okay. The last thing, the remaining steps to this project, we're going to complete this first benchmark, which will give us insight to the liability modeling digital systems and one of the major contributors to unreliability or failure probability, based on what we have included in the model. Obviously, we can't pass judgement on what's not in there. We also further determined the capabilities and limitations of the methods. We have that preliminary list. It may change to some extent based on insights from the first benchmark or the second benchmark for that matter.

As we mentioned previously, we are going to make somewhat of a comparison between the results and insights of our study with the parallel studies and dynamic methods. Again, that's going to be somewhat limited in scope, that comparison, because of differences in boundary conditions between the system being used for those two, the different approaches.

And the draft NUREG for this first benchmark is due in from BNL sometime next month. And so once we get it internally reviewed and get it ready for public dissemination, we, of course, provide it to the ACRS and be more than happy to come brief you on it.

The next step after -- the next task after completing that first benchmark is to go onto the second benchmark where we're going to look at a protection system, a reactor protection system, in specific. The design requirements for protection systems are, obviously, very different than for operating systems. And so they may present different modeling challenges which we will explore.

In one respect, it would be simpler in the fact that we don't have to deal with the whole complex feedback aspects of a controlled system. On the other hand, we do have to consider such things as synchronization and communication between redundant channels that you would have in a protection system, which is something you don't really address.

CHAIRMAN APOSTOLAKIS: When will these benchmarks be completed?

MR. KURITZKY: The first benchmark is almost completed. The draft report, as I mentioned, will hopefully be in next month. The second benchmark -- actually, the last presentation I have today is a future interaction with the ACRS. And there I have the schedule where all the studies are being completed and delivered, so we can use that schedule to help determine when would be the best point to come, you know, and talk to the ACRS.

So if you want to wait, we can -- we'll go over all that and we can -- you know, the idea of providing that schedule is to try and identify when would be the most opportune times to talk to the Subcommittee.

CHAIRMAN APOSTOLAKIS: Now, the last bullet, can you, please, wait on that? Don't publish a NUREG that says this is a way, because people will start using it.

MR. KURITZKY: No, no, that's not -- sorry. That is maybe misleading. We wanted to see how well we could integrate these various models into a PRA. It's not to say that this is the way you should do it, it's just -- and it's not going to be a NUREG, in fact, it's just going to be going to SAPPHIRE and can we take the results of these and how easy is it to stick it into the PRA Code?

CHAIRMAN APOSTOLAKIS: But will you

investigate that again without waiting for some sort of results from the identification of software failure modes?

MR. KURITZKY: Well, that actually is not going to happen for --

CHAIRMAN APOSTOLAKIS: Pushing too hard on this thing. And there is this major thing that's missing. And I would say just drop the bullet. Don't do it. And I'm dying to learn how Louis determined the numerical values of the transition rates for millions of states. You're using operating experience. Can we stop here?

MR. KURITZKY: Yes.

CHAIRMAN APOSTOLAKIS: Okay. Now, you guys know that this is 10:00, 10:15, can you, please, use the break to adjust your remaining presentations accordingly? Like Louis may came back and say under approach to reliability modeling it cannot be done.

MR. KURITZKY: That would shorten it. That would certainly shorten it.

CHAIRMAN APOSTOLAKIS: I'm sure.

MEMBER BLEY: I think since we have already discussed many of the topics that are in your slides, hopefully it won't take quite as long.

CHAIRMAN APOSTOLAKIS: Okay. So let's

recess until 10:30.

(Whereupon, at 10:17 a.m. a recess until 10:39 a.m.)

CHAIRMAN APOSTOLAKIS: Okay. We're back in session. Dr. Chu?

MR. CHU: Actually, Gerardo.

CHAIRMAN APOSTOLAKIS: Okay. All right. Let's find out what FMEA is here.

MR. MARTINEZ-GURIDI: My name is Gerardo Martinez-Guridi. I work for Brookhaven National Laboratory. I will be presenting our work on identifying failure modes and their effects and also approach for reliability model of digital systems. I will be presenting what is done at Brookhaven by Louis Chu, Manuel and myself mainly.

First, I will present a brief description of the digital system studies, the digital feedwater control system.

CHAIRMAN APOSTOLAKIS: So have you thought about shrinking a little bit your presentation?

MR. MARTINEZ-GURIDI: And I will be moving on to the next slide. We're talking about a two-loop PWR and having one feedwater control system for the secondary loop. The feedwater control system of each loop has two main processors and three controllers.

The CPUs receive data from plant sensors and the controllers seek the data from the microprocessors and send the demand to the control devices, such as valves and pumps. There is a fourth controller which is normally on standby and takes over in case one of the normal controllers fails.

And the next slide is a diagram of one secondary loop of the digital feedwater control system. Basically, what you have in the right, upper right corner is the feedwater control system and the four associated controllers. One of them controls the main feedwater control valve, the other controls the bypass valve, the other controls the pump and the fourth one is a standby one.

CHAIRMAN APOSTOLAKIS: Is this a system that is already installed?

MR. MARTINEZ-GURIDI: That has been operating for several years.

CHAIRMAN APOSTOLAKIS: That's why everybody is analyzing this?

MR. MARTINEZ-GURIDI: I'm sure there has been --

MEMBER SIEBER: There has been a number of them.

MEMBER BONACA: Yes, very successful

system, because before when they started automatic initiation of water, you had problems simply because the feedwater would come in, collapse the level and typically they had those kind of problems in controlling it. And this system has been very effective.

CHAIRMAN APOSTOLAKIS: So all the plants have it?

MEMBER BONACA: I think all the CEs are of a certain design. There was the San Lucie generation they had this system installed.

CHAIRMAN APOSTOLAKIS: Did you have one plant in particular in mind when you --

MR. KURITZKY: Yes, but we're not supposed to mention the name of that plant.

CHAIRMAN APOSTOLAKIS: But you did?

MR. KURITZKY: Yes.

CHAIRMAN APOSTOLAKIS: Um-hum.

MR. KURITZKY: Yes.

MR. MARTINEZ-GURIDI: I suppose I am allowed to say that it's a CE plant.

MR. KURITZKY: Right. Well --

MR. MARTINEZ-GURIDI: It's a combustion.

MR. KURITZKY: Yes, we're not allowed to mention, yeah.

CHAIRMAN APOSTOLAKIS: If Dr. Bonaca starts listing them, are you going to nod?

MR. KURITZKY: Wink, he'll wink when he gets to the right one.

MEMBER SIEBER: This particular system is -- has another degree of complexity because the feed pump turbine can be controlled. And a plant with electric pumps, you only have values. But in any event, in analog controls, they -- there is a separate controller for the feed pump turbine and the control valve, so that they can oscillate back and forth.

CHAIRMAN APOSTOLAKIS: So there's one for the electric pump and one for the --

MEMBER SIEBER: There's a different instrument system.

CHAIRMAN APOSTOLAKIS: All right.

MEMBER SIEBER: These are obviously -- I think they are PWRs.

MR. MARTINEZ-GURIDI: Well, the system analyzes the fourth box again on the upper right corner and they are expanded in the next slide, which provides some more -- very simplified, but it's a little more detailed diagram of the system. Basically, it has two identical microprocessors, the main and the backup CPUs, that take input from several plant sensors. Here for illustration only two of them are presented.

One of the CPUs is normally controlling the system and the other is in a tracking mode. In other words, it follows what the system is doing when it is not really controlling. And that's why you see the dotted lines coming from the back of CPU. In case the MFV or the BFV fails, the PDI can be used to control the main or the bypass valves. And that's also where you see dotted lines coming from the PDI.

CHAIRMAN APOSTOLAKIS: Coming from the what? Explain that again.

MR. MARTINEZ-GURIDI: The -- for some of the --

CHAIRMAN APOSTOLAKIS: There is a cursor there. Can you use the cursor? Yeah.

MR. MARTINEZ-GURIDI: For the analysis.

CHAIRMAN APOSTOLAKIS: Yeah, okay.

MEMBER SIEBER: There you go.

MR. MARTINEZ-GURIDI: This is the --

CHAIRMAN APOSTOLAKIS: So tell us --

MR. MARTINEZ-GURIDI: -- main valve, for example. The main valve is controlled normally by the MFV controller.

CHAIRMAN APOSTOLAKIS: MFV stands for?

Main?

MR. MARTINEZ-GURIDI: Main feed valve.

CHAIRMAN APOSTOLAKIS: Main feedwater valve. Okay.

MR. MARTINEZ-GURIDI: Main feedwater valve controller.

CHAIRMAN APOSTOLAKIS: All right.

MR. MARTINEZ-GURIDI: So the main feedwater valve control receiver signal from the main CPU.

CHAIRMAN APOSTOLAKIS: Right.

MR. MARTINEZ-GURIDI: And basically, it forwards the signal to the valve.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. MARTINEZ-GURIDI: And its position. The valve position is -- the valve is situated by means of its position.

CHAIRMAN APOSTOLAKIS: All right.

MR. MARTINEZ-GURIDI: Okay. If the MFV fails by sending a low signal, the PDI will detect the low signal and automatically take over control of the MFRV, the valve.

CHAIRMAN APOSTOLAKIS: The BFV stands for?

MR. MARTINEZ-GURIDI: The BFV, the BFRV is the bypass valve and its positioner. And the BFV is the controller that controls the bypass valve.

MEMBER BLEY: So the PDI takes over either one if it senses a problem?

MR. MARTINEZ-GURIDI: Either one. The only difference is that it takes automatically over if the MFV fails, but it doesn't do it automatically if the BFV fails. That -- the operator has to operate them.

CHAIRMAN APOSTOLAKIS: So if you go back to the previous slide, can you tell us those valves?

MR. MARTINEZ-GURIDI: Here is the main valve.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. MARTINEZ-GURIDI: And here is the bypass valve.

CHAIRMAN APOSTOLAKIS: Okay.

MR. MARTINEZ-GURIDI: Here is the BFV controller and here is the MFV controller.

MEMBER SIEBER: I take it this plant the way it is actually laid out is you have two feed pumps and either three or four feed water regulating valves, right, with a header as opposed to straight shots into the steam generator.

MR. MARTINEZ-GURIDI: Yeah, they -- there is a head where both come --

MEMBER SIEBER: So that makes the problem more complicated.

MR. MARTINEZ-GURIDI: Some considerations in the development of the FMEA and the reliability normally is that --

MEMBER BLEY: The way you just described it, are you just modeling a single train of the system?

MEMBER SIEBER: Yes.

MR. MARTINEZ-GURIDI: We're just modeling one, yes, that's correct. But there is almost no interaction between the two feedwater control systems.

MEMBER BLEY: Except through the sensors?

MR. MARTINEZ-GURIDI: Except through the independents on the sensors.

MEMBER BLEY: The sensors are the same?

MR. MARTINEZ-GURIDI: The sensors are the same, yes.

MEMBER BLEY: So some of the things Alan was talking about this morning, there is one kind of plant dependency that you could have modeled, but you chose not to.

MR. KURITZKY: If we're modeling --

MEMBER SIEBER: It really makes it complicated.

MR. KURITZKY: -- the whole system.

MEMBER BLEY: Yeah.

MR. KURITZKY: Right. Well, with our scope, we're just looking at the one rewrite. If this were actually to be implemented in a PRA, you would have to consider that, right.

MR. MARTINEZ-GURIDI: So we can see that the plant is operating at full power and that the DFWCS is operating at high power mode, automatically controlling the feedwater. And again, we are not addressing software reliability. However, we are taking into account the normal performance of the software, as I will describe later in a little bit more detail.

And we are including some basic software failures, nevertheless, such as the common-cause failure of both CPUs.

CHAIRMAN APOSTOLAKIS: So are you demonstrating here a general methodology for FMEA using a case study? Is that what you are trying to do?

MR. MARTINEZ-GURIDI: That is correct.

CHAIRMAN APOSTOLAKIS: So if I have to -- if I want to do an FMEA say for another system at my plant, I'll have to understand first your system and how you applied it?

MR. MARTINEZ-GURIDI: That is correct.

CHAIRMAN APOSTOLAKIS: There's no way you can separate it to have some guidelines that are generic for --

MR. MARTINEZ-GURIDI: I have such in the presentation.

CHAIRMAN APOSTOLAKIS: Okay. Some of the issues with the FMEA currently is that there is no publicly available -- there is no publicly available specific guidance on how to perform FMEA for the digital system. There is -- there are quite a few publications on the status on how to do FMEA, but there is no specific guidance on how to do it for the digital system.

Furthermore, there is no well-established list of failure modes of the component, which is a major issue, because if you don't know which of the failure modes, how do you read reliability model? Furthermore, assuming that you have some how come up with a list of failure modes, then essentially what are the effects of the failure modes, of individual failure modes and combinations of them on the plan is very difficult, because of the complexity of the digital system itself and because of the internal logic of the components which is usually implemented in software. And it's even more problematic to assert the effect of combinations of these failure modes.

CHAIRMAN APOSTOLAKIS: So you are contributing to the main theme that this Committee would like to see, mainly the identification of failure modes. You're just doing it for a class for potential failure modes, namely those due to everything except the software.

MR. MARTINEZ-GURIDI: We are doing everything except software.

CHAIRMAN APOSTOLAKIS: So this is a part of it? Yeah, okay.

MR. MARTINEZ-GURIDI: I believe we are pretty much in sync with what the Committee is proposing in terms of identifying, the importance of identifying failure modes. Those were mainly issue with --

CHAIRMAN APOSTOLAKIS: You shouldn't take everything we say as criticism of your work. We appreciate these are difficult problems, okay?

MR. MARTINEZ-GURIDI: Thank you. We have received your comments, too.

CHAIRMAN APOSTOLAKIS: I'm sure you do.

MR. MARTINEZ-GURIDI: Okay. So those were the main issues with FMEA is how we are -- I'm talking about the issues about building a reliability model. And it's expected that not every failure mode of the system is going to fail the system. But the other is that lacking information about whether the effect of a combination of failure modes is very difficult to build a model.

For example, when a fault -- when somebody is trying to develop a fault tree from using a deductive approach, you don't know which combinations of failures cause a certain impact. So it's very difficult.

CHAIRMAN APOSTOLAKIS: Why not? I don't understand what you just said.

MR. MARTINEZ-GURIDI: Because when you are developing a fault tree, the way to develop a fault tree is you first define the top event.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. MARTINEZ-GURIDI: Yeah, and you find some logic for it. And then you define that in terms of some inputs and those inputs have further developed in terms of OR gates. Now, every time you have intermediate event like that, you have to know what are the causes for that event.

CHAIRMAN APOSTOLAKIS: You don't have to

know. You are exploring. You are trying to identify.

MR. MARTINEZ-GURIDI: You are exploring, but you have to have some idea. For example, if you have an AND gate, you have to say this AND, for example, is three events that in general are going to cause this event.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. MARTINEZ-GURIDI: Okay. For these systems, that is really not feasible, because the system is so complex that you don't know which combinations of events are going to lead to another. So pretty soon after you tried to develop your fault tree, you reach a point where you don't know what the combinations are going to lead to intermediate events.

CHAIRMAN APOSTOLAKIS: I see.

MR. MARTINEZ-GURIDI: And that in principle is applicable to other approaches.

DR. GUARRO: And isn't that why one needs a model of the interactions?

MEMBER BLEY: Yeah.

MR. MARTINEZ-GURIDI: Well, that's why we developed the model of interactions.

DR. GUARRO: Okay. But you think that FMEA is a way of building a model to do interactions?

MR. MARTINEZ-GURIDI: We developed a model to support the FMEA and to support the building the reliability model. And perhaps if we go a little further, perhaps we can make a more informed --

CHAIRMAN APOSTOLAKIS: But these are the kinds of insights that are really very useful, because they are telling me that what you guys are doing, even though you are leaving software out, is shedding light on some things that we have to know. I would emphasize those points.

MR. MARTINEZ-GURIDI: Well, that was the point I was trying to make earlier on was that we recognize that software was one issue and we -- there are other issues besides just software that are complicated with doing digital system models also.

DR. GUARRO: Okay. Now, you'll probably show me this, but if you can't study the system and build a top down fault tree to explain how the event above it fails, why do you think the simulation model you put together is really modeling the system correctly?

MR. MARTINEZ-GURIDI: If you don't mind, let's go over the presentation and that should be explained.

DR. GUARRO: If you're going to get there, I'll be happy.

MR. MARTINEZ-GURIDI: Yes. So this is the general approach we are proposing to address with these issues. These are the kind of the major steps and then I will elaborate on these in the following slides. The first one is to decompose the system into more detailed components.

CHAIRMAN APOSTOLAKIS: Okay.

MR. MARTINEZ-GURIDI: Okay. And basically, what we will have is the failure effects of one level of the FMEA become the failure modes of the next higher level. If you go quickly to the next slide, this is what we are talking about. This is from -- this is a drawing from Standards published by the British Standards Institution.

And what we have at top is the system level. And then each component of the system is -- well, the system is decomposed to subsystem levels and then the subsystem is decomposing to module levels and so on until a certain level of detail is reached.

CHAIRMAN APOSTOLAKIS: This is -- now, when you say system, any system?

MR. MARTINEZ-GURIDI: Any system. This is totally generic.

CHAIRMAN APOSTOLAKIS: It has nothing --

MR. MARTINEZ-GURIDI: Nothing to do with

the what they say, this is a totally separate publication.

CHAIRMAN APOSTOLAKIS: So you do not apply this to a digital --

MR. MARTINEZ-GURIDI: We are using the same concept.

DR. GUARRO: This looks to me like a fault tree in success base.

MR. MARTINEZ-GURIDI: Yeah, this is just illustrating how we are --

DR. GUARRO: It's broken down.

MR. MARTINEZ-GURIDI: Yeah, this is just illustrating how we are decomposing the system in several levels.

CHAIRMAN APOSTOLAKIS: Okay. Okay. Go, go on.

MR. MARTINEZ-GURIDI: And then if we go back to the previous slide again, we develop a deterministic computer model of the system.

CHAIRMAN APOSTOLAKIS: What does that mean?

MR. MARTINEZ-GURIDI: We build a model of the system in terms of the software of the system. So each of the main components of the system, which was in the previous drawing, by the main CPU, the backup

CPU, each of the controllers has its own software. And each of them are running the software simultaneously and talking to each other. So we have a model that actually runs that software.

CHAIRMAN APOSTOLAKIS: I don't follow that. A model that runs the software.

MR. MARTINEZ-GURIDI: Yeah.

CHAIRMAN APOSTOLAKIS: What does that mean?

MR. MARTINEZ-GURIDI: If we go, let's see, to this diagram --

CHAIRMAN APOSTOLAKIS: Right.

MR. MARTINEZ-GURIDI: -- each of these boxes basically run the software. But we have a model that reproduces this system. Each of these boxes -- there is software running in each of these boxes. So it produces how the system is working.

CHAIRMAN APOSTOLAKIS: So that's the system then?

MR. MARTINEZ-GURIDI: It's the system. It's just we don't have physically the system. It's just, we call it, simulation, because it's just running the software of the system. We don't have the physical controllers with us. We just run the software on the system.

MEMBER BLEY: So you generate the signals that would go to the controllers?

MR. MARTINEZ-GURIDI: Exactly. We feed the signals and we see how the system responds to those signals. And the basic idea, if I go out a little bit ahead of myself, is once we have that system, which is actually pretty much a reproduction of the system, then we can see what happens every time a failure comes in and how it's going to affect the whole system.

CHAIRMAN APOSTOLAKIS: If it's a reproduction of the system, then it's a copy of the system. Is that what you mean? I don't understand what you mean. I have a software that --

MR. MARTINEZ-GURIDI: What I mean --

CHAIRMAN APOSTOLAKIS: -- mimics the CPU, but it's not the CPU.

MR. MARTINEZ-GURIDI: Well, because we don't have the actual controller. We don't have the actual hardware, which is a controller, or the actual hardware, which is the main CPU. So we just have the software that runs inside those models and we run the software.

MEMBER BLEY: Did the manufacturer give you the software?

MR. MARTINEZ-GURIDI: It is the actual software.

MR. KURITZKY: We have the actual software, yeah.

CHAIRMAN APOSTOLAKIS: You have the actual software. Okay. So you run the actual software?

MR. KURITZKY: That's right.

MR. MARTINEZ-GURIDI: We run the actual software.

MEMBER BLEY: But on their own machine.

MR. MARTINEZ-GURIDI: On our own machine.

MEMBER BLEY: On their own computer.

CHAIRMAN APOSTOLAKIS: Right.

MEMBER BLEY: Okay.

CHAIRMAN APOSTOLAKIS: That makes more sense.

DR. GUARRO: Yes, it makes sense, but I guess the observation that I have here is that, you know, I think in a way, you know, the premise of this project is that you are doing traditional modeling. This is not traditional modeling. Okay. And, in fact, what are called advanced models try to do exactly what you are doing with the simulation.

They are trying to do it in a simplified way. In other words, they are, you know, simulations of the software and functionality in some paradigm and there are different paradigms, but they are essentially simulation. So, you know, it's -- I'm kind of getting a little confused about where the boundary is between traditional and non-traditional.

MR. KURITZKY: All right. Dr. Guarro, your point, that's exactly right, Dr. Guarro. And the issue here, because you're right, the line is getting a little fuzzy, but we drew the line. If you think back to my -- when I was talking about my presentation, the definition of traditional failure mode that we have, not traditional failure mode, but traditional method we defined was that did not explicitly account for the interactions between the system being modeled and the plant physical processes or the timing of those interactions.

That was the only piece that we defined to be the difference between traditional. And the other thing was that it had to be more well-established. Now, the idea of not addressing the -- explicitly addressing those interactions, we still abide -- we still meet that condition. The issue of not doing any advancements and just looking where the establish -- what exists already, you are right.

In that case, we have moved forward. And that's why I -- the statement in the report and also I think the statement in the presentation earlier was that we generally did not advance the state-of-the-art. But in this case, we came up to a situation where we could not do the traditional models, because of the complexity of the system at that level. And so we had to come up with this automated routine in order to be able to generate, essentially, the cutset, so to speak.

DR. GUARRO: But essentially, you are implicitly meaning that one cannot model this type of problem without doing some advanced modeling?

MR. KURITZKY: Some advancement at this level of detail.

DR. GUARRO: Which is something that some people, including myself have been saying for about 20 years, so I rest my case.

CHAIRMAN APOSTOLAKIS: No, the title of the whole project probably ought to be revisited. It causes a lot of headaches with traditional methods and all that. I mean, here is an example where you depart from traditional methods. Find a better title.

MR. KURITZKY: Right.

CHAIRMAN APOSTOLAKIS: That will also say or send the message that software are not part of what you have done.

MR. KURITZKY: Additionally.

CHAIRMAN APOSTOLAKIS: Well, I mean, this is really a major thing. I mean, you really get upset after a 100 pages and you realize that this is left out. Yeah, I agree with Sergio. I think here you are departing from traditional, but keep going now.

MR. MARTINEZ-GURIDI: Okay. Once we have developed a model, we simulate the response of the system to postulate combinations of failure modes of components. So given that we have come up with some lists of component failure modes, we see whether the response of the system given that each of these failure modes has happened and given that combinations of these failure modes have occurred and then where to find what other combinations of failure modes that fail the system.

MEMBER BLEY: I'm just thinking about your simulation. Your simulation is running the software that this digital I&C says to run.

MR. MARTINEZ-GURIDI: Yes.

MEMBER BLEY: But it is running it on a computer that doesn't have the same hardware register structure, it doesn't have the same firmware, so any problems that might exist in the digital I&C system that comes about, because of register overload or some interaction with the firmware, you just won't see here. But you might see some that are happening because of those things in your computer that don't exist in the other one.

MR. MARTINEZ-GURIDI: Well, the main intent in doing the simulation is to be able to reproduce how the software is going to respond to failures.

MEMBER BLEY: Okay. So we're looking at a software performance study?

MR. MARTINEZ-GURIDI: Yes. And that's why we have mentioned before that we look at least at the performance of the software.

MEMBER BLEY: Okay.

MR. MARTINEZ-GURIDI: Because given that you have a certain failure, if you don't have this kind of simulation to, it's almost -- it's always very difficult, almost impossible to find out how the software is going to respond, because the software is so complicated.

MEMBER BLEY: When you inject failures, what kind of failures are you injecting? What do you mean by that?

MR. MARTINEZ-GURIDI: We define -- I will get to this in a little more detail.

MEMBER BLEY: Okay. I'll wait if you're coming to it.

MR. MARTINEZ-GURIDI: But let me --

MEMBER BLEY: You started a couple of times, that's why I asked.

MR. MARTINEZ-GURIDI: -- say that we define certain components and certain failure modes for each component.

MEMBER BLEY: Okay.

MR. MARTINEZ-GURIDI: And then we just take each individual failure mode and try it and then we take combinations, all possible combinations.

MEMBER BLEY: But you will give us some examples.

CHAIRMAN APOSTOLAKIS: Yeah.

MEMBER BLEY: You know, of what you're talking about.

MR. KURITZKY: Appendix B of the report actually has the actual -- for the main CPU, it has all the failure modes that were developed in the main CPU.

CHAIRMAN APOSTOLAKIS: So you are injecting failures into the actual nodes?

MEMBER SIEBER: They are sensor failures.

MR. MARTINEZ-GURIDI: Yes, when they --

CHAIRMAN APOSTOLAKIS: Not sensor.

MR. MARTINEZ-GURIDI: We're injecting failures everywhere in the system depending on --

CHAIRMAN APOSTOLAKIS: Even the sensors?

MR. MARTINEZ-GURIDI: Even the -- we postulate failures of the sensors and see why --

CHAIRMAN APOSTOLAKIS: Failure does not mean a parameter value though.

MEMBER SIEBER: Oh, yeah, it goes to zero.

MR. KURITZKY: It depends on the signal, no signal, low signal, high signal.

MR. MARTINEZ-GURIDI: We characterized it, you know, in the wrong way by just saying, for example, low signal from the sensor or high signal from the sensor. We don't have a more refined description of that, as will be the reality.

CHAIRMAN APOSTOLAKIS: I'll have to understand that a little better. How is this different from VFM? It's not what VFM does?

MR. MARTINEZ-GURIDI: It may have some similarities. It may have some similarities.

CHAIRMAN APOSTOLAKIS: Yeah, but how is it different?

MR. CHU: In our model we actually used

the original source code from the actual subset.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. CHU: That is the CPU, the source code was written in C language, so it is pretty easy to just copy to a PC and make use of it. And the controllers, they have their own proprietary language. But we have to read the language and convert it into C.

CHAIRMAN APOSTOLAKIS: But in VFM, the various truth tables scattered all over the place are produced by running the appropriate software.

MR. MARTINEZ-GURIDI: The software.

CHAIRMAN APOSTOLAKIS: So how is your --

DR. GUARRO: Well, there is intermediate step, but essentially it's the same thing.

CHAIRMAN APOSTOLAKIS: It's the same thing it seems to me. Unless there is a difference someplace that I don't see right now.

MR. MARTINEZ-GURIDI: Well --

CHAIRMAN APOSTOLAKIS: You don't have truth tables, do you?

MR. MARTINEZ-GURIDI: No.

CHAIRMAN APOSTOLAKIS: No.

DR. GUARRO: And by the way, the reason why there is that intermediate thing in that family, is because that way you can do deductive analysis, which in a true simulation you cannot do.

CHAIRMAN APOSTOLAKIS: Now, let's go on.

DR. GUARRO: Just a clarification.

MR. MARTINEZ-GURIDI: Okay. Well, using this process, we can identify those combinations of failure modes that fail a system. However, we believe this approach addresses most of the issues that I described before. But there is still one major issues that remains, which is the issue of completeness of failure modes. And we believe we address that to some extent by finding out which of the failure modes and the effects of either component of the system.

CHAIRMAN APOSTOLAKIS: So because you are injecting failures, you have this issue of completeness that was raised earlier, right? Because you are only finding what is going to happen if I inject a failure here and a failure there. Obviously, you cannot figure out all the combinations.

MR. MARTINEZ-GURIDI: We do.

CHAIRMAN APOSTOLAKIS: All of the combinations?

MR. MARTINEZ-GURIDI: We do up to a certain point, because what happens is that as the number of -- for example, first we try combinations of all possible two in order, then all possible three. And I do keep increasing components. The probability keeps coming down very quickly. So now a case, for example, we only had to examine up to combinations of PRORE, because combinations --

CHAIRMAN APOSTOLAKIS: How do you know the PRORE comes down? That's a conjecture on your part, which I think is all right.

MR. MARTINEZ-GURIDI: Because we are calculating what the probability of failure and what the probability of not failing the system.

CHAIRMAN APOSTOLAKIS: Well, I'm calculating a probability.

MR. MARTINEZ-GURIDI: Yes.

MR. KURITZKY: And Louis has a table in his presentation that will give you some results at a couple of different levels. But I think to address Dr. Apostolakis' comment directly, as Gerardo was saying, for the thermos that we know, we address all combinations. The issue, as Gerardo was trying to point out, is that, and everybody had mentioned, do we know all the failure modes? What about the failure modes we don't know? That's the problem. That's the completeness issue.

MEMBER BLEY: But you don't do all

combinations. You just told us you do all singles, all doubles.

MR. KURITZKY: Right, right.

MEMBER BLEY: And all triples.

MR. KURITZKY: Theoretically, you could do all. We stopped after triples.

MEMBER BLEY: To see if there were natural combinations of those failures that might occur because of the same cause?

DR. GUARRO: Yeah, right, that's the question.

MEMBER BLEY: The single cause and, you know, maybe one cause can give you a certain set of three or four or five.

MR. MARTINEZ-GURIDI: We introduced some common-cause failures and we introduced them also as--

MEMBER BLEY: Not just as a black box common-cause, but as a --

MR. MARTINEZ-GURIDI: What do you mean a black box common-cause?

MR. KURITZKY: No, no, we didn't.

MEMBER BLEY: Well, we did do a black box, right. It just says common-cause failure 10^{-} whatever.

MR. CHU: In a sense, that's the case. That is we assume we disobeyed our factor for common-cause failure. And then for, you know, individual failure modes, we just add up the failure rates and then multiply by this data factor and we say this is the common-cause.

MEMBER BLEY: No, what I was getting at is did you do a systems analysis look at the failure modes catalog that you have and see could some of these multiple of these be induced by a single cause in the plant, something physical you can examine.

MR. MARTINEZ-GURIDI: No.

DR. GUARRO: In cause and in effect. In other words --

MEMBER BLEY: Cause and effect.

DR. GUARRO: -- is there a cause that branches out into a different -- a set of different failures in different parts of the software and/or digital system?

MEMBER BLEY: Random combinations of three or more can't be very interesting, but some --

MR. MARTINEZ-GURIDI: If there is a --

MEMBER BLEY: -- link coupling of 3, 4 or 5, would be much more likely and more interesting, that's what I was getting at.

MR. MARTINEZ-GURIDI: If that actually happens.

MEMBER BLEY: And the more failures we study, the more we will know.

CHAIRMAN APOSTOLAKIS: I am a little concerned about this role of using the failure rate to limit the number of combinations. So automatically now, you are telling us if there is such a thing as a failure rate or a rate of occurrence and we are using -- I thought we -- one of the big problems here is that we don't have that kind of information.

MEMBER BLEY: But they are generating.

MR. MARTINEZ-GURIDI: We have some failure rates and the representation is based on --

MEMBER BLEY: Well --

MR. MARTINEZ-GURIDI: -- a system of that.

MEMBER BONACA: They should call it converging, so that's different.

CHAIRMAN APOSTOLAKIS: It is.

MR. CHU: In a way it's that idea. We used the concept of, you know, cutset occasion.

MEMBER BONACA: Yeah.

MR. CHU: The more failures you have in a sequence, the lower the probability is.

CHAIRMAN APOSTOLAKIS: I understand that qualitative argument and I think by and large it's true, but then you have to worry about what Dennis and

Sergio just said, you know, the possible underlying linkage. That I would accept, but the actual numbers I'm not sure.

MEMBER BONACA: I think the application of the Markov example you use it as a means of making it possible to look at the combination, because you have so many.

MR. KURITZKY: Right. In fact, the simulation that I was describing, that's how we were able to address that huge number.

MR. MARTINEZ-GURIDI: Let me also just finally say that the bottom line is that this issue applies to everything, not only to digital systems, it applies to analog systems as well and applies to practically all methods, you know. The issue of completeness of failure modes, I think, no method is immune to practically.

CHAIRMAN APOSTOLAKIS: So why did you lead me to FMEA? Wouldn't it make sense to say for the identification of failure modes one can use the FMEA? That does some things well, some other things not very well. One could use something else, hazard or whatever. I mean, these are the standard tools of the trade.

MR. MARTINEZ-GURIDI: What happens is that the failure truths are basically the same. I mean, it has FMEA --

CHAIRMAN APOSTOLAKIS: No, they are similar. They are similar.

MR. MARTINEZ-GURIDI: -- they're the same thing.

CHAIRMAN APOSTOLAKIS: But so --

MR. MARTINEZ-GURIDI: Those are the traditional tools that -- those were the ones we were supposed to explore.

CHAIRMAN APOSTOLAKIS: Oh, I don't know.

MR. CHU: We were influenced by the hazard analysis that was available to us. And that's how we started looking at the failure modes and analysis.

CHAIRMAN APOSTOLAKIS: So what you are saying is you can't really do much on the causes? You can do on the failure mode on the effects of postulated failure modes, but not the causes.

MR. MARTINEZ-GURIDI: Well, not the modes. Not the modes of failure. There is a difference between failure cause and failure mode. A failure mode may have several different causes. Here we are talking about failure modes and failure effects. We have -- there is another issue I will get at a little bit later on, which is that what is relationship between, for example, between physical failures and functional failure modes. So I hope I didn't confuse you.

CHAIRMAN APOSTOLAKIS: All right. I guess we can move on.

MR. MARTINEZ-GURIDI: Okay.

CHAIRMAN APOSTOLAKIS: Unless there's another question. So what slide number is this, 9?

MR. MARTINEZ-GURIDI: It's 9 moving to 10.

CHAIRMAN APOSTOLAKIS: Moving to 10.

MR. MARTINEZ-GURIDI: Okay. 10 we already talked about, unless somebody has questions.

CHAIRMAN APOSTOLAKIS: Okay. Skip it then.

MR. MARTINEZ-GURIDI: Now, for the specifics of the FMEA of the system standard, we decomposed into three levels of detail there. The top level of the system, the modules, which are defined now and component level. This study defined a module as a microprocessor and the components directly associated with it. Like the example of a controller would be a module. Each controller would be a module.

We identify six modules for the FMEA. They are the main and backup CPUs and the four controllers. And the component level refers to the components comprised in each of the modules such as the microprocessors, multiplexers, demultiplexers, a lot of converters and such.

And the FMEA of the associated components such as sensors and support system was also carried out at this level. And we also found a practice that the duration between the FMEA level and the industry level is necessary. This probably true for any FMEA.

This is an example of how what a module looks like. This is the main CPU and at the center you see the actual microprocessor and then you see a number of peripheral devices, such as the random access memory. You have -- from the left you have in there the inputs to the module which may be charged both analog and digital processed through the module and then the incident taken out in terms of analog and digital outputs.

This is just for illustration purposes of what we mean by a module and what we mean by a component level. So the FMEA was done at the level -- at the three level for which is only way to the digital components shown in this diagram. Like we have an FMEA for this component and an FMEA for this component and so on.

We defined failure modes for each of these digital components. And these failure modes are the ones that we injected into two to see what would be the impact of that failure mode into the system.

This is a little more detailed description of the --

MEMBER BLEY: Oh, I'm sorry. I'm staring at that picture again and thinking if I look at that picture, you're running the software in your simulation in the CPU and all these other things are inputs and outputs from that software and it's those that you are effectively corrupting with the injecting failure modes, right?

MR. MARTINEZ-GURIDI: Basically, yes.

MEMBER BLEY: Okay.

MR. MARTINEZ-GURIDI: Yes.

MEMBER BLEY: So they are kind of black boxed from one processor to the other, but then occasionally you damage the signals that are coming through to see what happens.

MR. MARTINEZ-GURIDI: Right. Like we could define, for example, a failure mode in this box here.

MEMBER BLEY: Yeah.

MR. MARTINEZ-GURIDI: There is a failure mode here and how that is going to propagate through the rest of the system.

MEMBER BLEY: But what you do with that, you don't do any modeling of that, you just inject a bogus signal to account quickly?

MR. MARTINEZ-GURIDI: That's right.

MEMBER BLEY: Okay. Does that -- that stays a persistent signal as the software runs?

MR. MARTINEZ-GURIDI: It is persistent, yes. We assume that the failures are permanent. They just remain there. Shall we continue?

MEMBER BLEY: Yes.

MR. MARTINEZ-GURIDI: Okay. This is a more detailed explanation of the method we are proposing to do in the FMEA and building the reliability model. Again, we first develop a deterministic computer model of the system to simulate the response to postulate the combinations of failure modes of components to identify those that fail the system. Then individual and combinations of failure modes are used as input to the model and as output we obtain their effects. And the model should be as realistic as possible, so we can reproduce the behavior of the system under failure conditions.

The examination of the output from the execution of the model reveals the effects caused by the failure modes are postulated. In theory, all possible combinations of failure modes of the system have to be evaluated. That's what Dr. Apostolakis was asking before. And this truly can be something of an extremely large number of combinations.

In practice, however, the probability of occurrence of the combinations is going to be -- is going to decrease rapidly with the number of failure modes in each combination. The evaluation process may be stopped after having considered a limited number of failure modes in each combination.

MEMBER BLEY: Unless there are dependent effects, I guess.

MR. MARTINEZ-GURIDI: I'm sorry?

MEMBER BLEY: Unless there are dependent effects that couple those failure modes.

MR. MARTINEZ-GURIDI: Well, again, the only dependent effects are common-cause failures.

MR. KURITZKY: And we're inputting those directly as essentially single events.

MEMBER BLEY: Understand.

MR. MARTINEZ-GURIDI: Yes.

MEMBER BLEY: Let me just ask a peripheral question. For this single train system that you analyzed, how big an analysis effort was this? Are we talking a man month, a man year?

MR. KURITZKY: That's probably between that, right? Yes, I think you just put --

MEMBER SIEBER: Oh, really?

MR. MARTINEZ-GURIDI: Several man months.

MEMBER BLEY: Now, this is a truly simple little piece of an integrated system.

MEMBER SIEBER: Actually --

MR. KURITZKY: It's not that simple, but it is a little piece.

MEMBER BLEY: Compared to the integrated whole system or the number of combinations of things you can get to, it's very simple.

MEMBER SIEBER: There is a lot of things that you don't test when you use a little simplified layout. For example, you're going to have two feed pumps --

MR. KURITZKY: Yep.

MEMBER SIEBER: -- feeding a header. You're going to have eight valves.

MEMBER BLEY: Maybe with very different control systems, depending on the plant.

MEMBER SIEBER: Well --

MEMBER BLEY: Go ahead.

MEMBER SIEBER: -- they are going to have different operating curves.

MEMBER BLEY: Yeah.

MEMBER SIEBER: But those are the tables. And you model and control as software and you just use those tables to determine, you know, a proportional ban, reset and rate. But you've got eight valves and four steam generators and they are all connected together by a header between the valves and the feed pumps. And each one has a different operating principal. For example, the feed pump is tied to the power output which you measured by steam flow.

The valve position is a constant differential. On the other hand, the steam generator level is a combination of the difference between steam and feed flow as a proportional band and then reset action is based on level. And you can put rate action there, too. When you get down to a single train without this header effect, you have eliminated half of the logic for that operation. And so you really aren't testing the program. You get a much smaller failure rate, I would think.

MEMBER BLEY: Yeah, and where I was going is this is a reasonable thing to do the way you have done it. It's a Research Program. If this does not lead to generalizations and ways that you can model at a higher level and account for the kinds of things you discover here, this begins to be real hard to see as a practical way to model I&C in a complete integrated PRA at the plant.

MR. MARTINEZ-GURIDI: Why? Why is it hard to say?

MEMBER BLEY: Because I think it's too much work. I mean, you have spent half a man year or something doing this for, what I'll again claim is, a simple part of the whole plan.

MEMBER SIEBER: Yeah, on the other hand, you can do that along with the design of the system. You know, some engineers are sitting down saying I need this controller. I need these inputs. I need these outputs. Here are the characteristics that they need to have and even in truly analog systems, some engineer --

MEMBER BLEY: Has to do that.

MEMBER SIEBER: -- is doing that, so why not just put the same logic and the same numbers in your model and run the model and see what the failure effects are?

MR. MARTINEZ-GURIDI: Also --

MEMBER BLEY: If your model doesn't blow

up, then that's what I think is probably going to happen.

MEMBER SIEBER: You have to build the model to match the system.

MEMBER BLEY: I don't think we know yet how, you know, you can perhaps prioritize, you know, so that you don't have to do this for everything.

MR. MARTINEZ-GURIDI: I think that should be the goal.

DR. GUARRO: Yeah, exactly. That's what we should --

MEMBER BLEY: I mean, right now it reads like this is what you ought to go do for every plant.

DR. GUARRO: I think, obviously, you cannot do it for the whole plant. I mean --

MEMBER SIEBER: Well, my guess is that the more you simplify, the lower the failure numbers are going to be. You know, you just aren't -- because you don't have the components and you don't have the interaction.

MEMBER BLEY: Yes, but once you learn about those interactions, you can find -- I mean, we have done that in all other aspects of PRA. We model at a higher level and account for the interactions.

MEMBER SIEBER: Yes, but pretty soon you

get to the point of you're just counting lines or code and saying, you know --

MEMBER BLEY: That will never get there.

MEMBER SIEBER: -- programmer A makes one mistake every 5,000 lines.

MR. MARTINEZ-GURIDI: But I also should say that, you know, there was overhead time that we spent first familiarizing ourselves with the system. And then there was time spent, you know, thinking about how we were going to solve the implemented system. For somebody who is familiar with the system, like the licensee, would be a lot more straightforward.

MR. KURITZKY: And once this process is already -- it's got the first time out of the box on it, so it would be a little bit more efficient. But it also goes to the comment that I made -- I'm sorry. The comment I made earlier about how we -- this was -- we use this process as a way to identify these failure mode combinations, but there is a desire to try to make it simpler and more, you know, efficient, because, obviously, it's still quite a bit of work.

MEMBER SIEBER: For the purpose of writing this NUREG, this is good enough, in my opinion. It illustrates the principle even though you couldn't apply it to an actual plan. And so, you know --

MR. KURITZKY: It's a step.

MEMBER SIEBER: -- it's a step and I suspect that we ought to go on with the presentation.

MR. CHU: I think the approach that we develop here has general applications. The fact this is a research project will demonstrate how the -- in the longer term if you feel comfortable with the way you are doing that, some other process can be further ovulated to speed up the process. When we do the study, we started doing the FMEA manually. Three of us sitting at a conference room table with the documents spread out.

Now, in order to find a response to a postulate failure, we might go through different parts of different documents to find the answer. And then we build a table that is in Appendix B. This is very time consuming, that's the reason we came to that understanding it's just not possible to do that and to look at different combinations and different orders in looking at the effect. That's why we came at this idea of developing this simulation tool.

I guess that's why we hope people would feel as though it's reasonable doing things and then a general application we can possibly develop a little more automated tool. And related to your early question, you know, how much confidence do you have with the outcome of the simulation? Since we actually started doing this manually, so we came to understanding of build FMEA table, based on our understanding.

So when we run the simulation tool and get the result, we actually compare it with what we found manually. And in some cases we don't agree, we saw the difference. In that sense, we have reasonable comfort with the FMEA that we end up. But when it come to, you know, looking at double and triple failures, there are so many of them we can only call a spot check. We will get a few of them and see the outcome is reasonable.

CHAIRMAN APOSTOLAKIS: Now --

MR. CHU: And then we have to rely on the tool.

CHAIRMAN APOSTOLAKIS: -- the PRA guy or whoever analyzes the system will identify some failure using your work to publish these generically and so on, so they know that there is a failure mode of interest. Then they would be interested in working backwards to find out how this failure occur. Can that -- can you help there? Can your approach help?

You know, it's one thing to postulate a failure and see what happens and quite another to say now, this happens. Tell me how it happened.

MR. KURITZKY: You mean the failure causes that led to the failure mode?

CHAIRMAN APOSTOLAKIS: Failures so many. Smaller pieces that lead to a failure, the failure of the regulating valve.

MR. MARTINEZ-GURIDI: Yeah, what happens is that --

CHAIRMAN APOSTOLAKIS: I want to work backwards.

MR. MARTINEZ-GURIDI: Yeah. What happens is that using this approach and in particular this ratifying those combinations of failure mode that fail the system.

CHAIRMAN APOSTOLAKIS: Right.

MR. MARTINEZ-GURIDI: In other words, each of these combinations is a failure mode of the system.

CHAIRMAN APOSTOLAKIS: The system meaning the whole thing?

MR. MARTINEZ-GURIDI: The system meaning what is in that diagram that I show.

CHAIRMAN APOSTOLAKIS: Not just the regulating valve or, I mean, the whole thing.

MR. MARTINEZ-GURIDI: Well no. In our case, your -- for our study, it was only the valves and the pump.

CHAIRMAN APOSTOLAKIS: Okay. So now, I'm taking the point of your PRA on this.

MR. MARTINEZ-GURIDI: Right.

CHAIRMAN APOSTOLAKIS: PRA on a list keeps doing his or her work and at some point says I want to understand now how this regulating valve may fail. And Brookhaven has done all this work and I would like to identify the possible failure modes or causes, I guess, in this case. Can you help there or is it strictly forward?

MR. MARTINEZ-GURIDI: At this point, if somebody would ask that question, we would not be able to give the answer. However, if we wanted to answer that question, we would fairly easily allow Alan to answer that question.

CHAIRMAN APOSTOLAKIS: Okay. Well, that seems to me that would be a question that would be asked.

MEMBER BONACA: That would be useful.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. MARTINEZ-GURIDI: That can be done.

CHAIRMAN APOSTOLAKIS: All right. Let's

go on.

MR. MARTINEZ-GURIDI: Okay. So once we obtain the combinations of failure modes that cause the system failure, then they can be used to build a probabilistic model. And then the model can be evaluated to obtain quantitative measures, such as the frequency of failure of the system. And we consider this process to be a new approach for finding out the effects of combinations of failures of several components of a digital system. And to be applicable to any complex system.

Okay. Any more questions? Okay. Now, I will give a little bit more details about the specific tool that we developed for this study for the DFWCS. As mentioned earlier, it's based on the software of the models of the DFWCS. In this way, we account for the performance of the software of the system. Given the occurrence of one or more power failure modes, this detail more than allows realistic representation of the system on the failure conditions.

However, at this time, interactions with the rest of the systems of the plant are not included in the model. But this can be expanded to include -- the model can be expanded to include these interactions.

MR. KURITZKY: Again, just to underscore, I think, the point that I think Dr. Guarro mentioned and I think others may have mentioned, too, the more this simulation tool is enhanced, the more we're veering away, obviously, from what you call traditional methods. So I mean, that's -- we're in the gray, the uncharted gray area in between traditional and dynamic methods.

MR. MARTINEZ-GURIDI: For the case of the DFWCS with defined system failure of the loss of automatic control of the feedwater loop as associated with the system and given a combination of failure modes of components as input, the tool automatically finds out whether a system failure occurs or not using criteria provided by the analysts.

This criteria basically is to specify the conditions that cause system failure. In our particular case, the tool analyzed 421 individual failure modes; 128,779 combinations of two failure modes; and almost 37 million combinations of three failure modes. So we are basically, as I said before, analyzing each possible combination of two and three failure modes. So in that sense, the completeness is -- in this particular sense does -- is not an issue for us.

MR. KURITZKY: But not in terms of completeness of identified failure modes.

MR. MARTINEZ-GURIDI: Right.

MR. KURITZKY: Because this is the only generating combination of failure modes that we identified inductively to include. We don't know what other failure modes might be out there that we didn't come up with and therefore didn't input to the simulation tool.

MEMBER BLEY: The failure modes you have in Appendix B. Were those generated?

MR. MARTINEZ-GURIDI: The failure modes we have in Appendix B we generated manually. We ran --

MEMBER BLEY: Just looking at the system saying what if this happened, what if that happened?

MR. MARTINEZ-GURIDI: Well, we used several sources. One we had some analyses done by the licensee.

MEMBER BLEY: Okay.

MR. MARTINEZ-GURIDI: Which was risk FMEA. So as Louis was saying earlier, that was kind of our starting point. And we complimented that using other sources from the literature.

MEMBER BLEY: Of actual failures that have occurred?

MR. MARTINEZ-GURIDI: At least to failure mode.

MEMBER BLEY: For failure modes.

MR. MARTINEZ-GURIDI: Failure modes. So that's basically how we created our list of failure modes.

MEMBER BLEY: Um-hum.

MR. MARTINEZ-GURIDI: And then what the tool allows us to do is to find out what happens when a combination of them happen.

CHAIRMAN APOSTOLAKIS: So again, look at the first bullet. A guy who does a PRA now for the plant.

MR. MARTINEZ-GURIDI: Yes.

CHAIRMAN APOSTOLAKIS: Will reach a point where there will be an event failure of feedwater, right?

MR. MARTINEZ-GURIDI: Yes.

CHAIRMAN APOSTOLAKIS: And what you are suggesting is that there will be then an OR gate there that says failure due to loss of automatic control, failure due to other causes. These don't interact?

MR. MARTINEZ-GURIDI: Basically, the integration with the PRA model is something, it's a subsequent task in the priority, so that has not been studied in detail. However, what can be done is properly include it in the fault tree such that any interactions between the plant and the rest of the -- between the system and the rest of the systems of the plant will be accounted for.

MEMBER BLEY: I think --

MEMBER BONACA: But now you did not do that.

MR. MARTINEZ-GURIDI: I'm sorry?

MEMBER BONACA: Up here in this example, you did not do that.

MR. MARTINEZ-GURIDI: In this example we just looked at the system itself.

MEMBER BONACA: The system. Loss of the water control. There was --

MR. MARTINEZ-GURIDI: Yes. And actually what we -- as we describe in detail later, what we modeled is the frequency of the -- we modeled the simulation event. What is the frequency of loss of automatic control as if it was an event?

CHAIRMAN APOSTOLAKIS: Automatically.

MR. KURITZKY: Right. So, in fact, if this was actually in a PRA, if you look at a traditional, let's see, fault tree, assuming that a PWR would actually have a fault tree for a few, not all of them do, but you would have the tree that says if it's a multi train, you know, an AND gate that fails train A and train B. Train A fails, the pump fails to start, the valve fails to close.

And then you have under there various other failures of supporting system. You would have failure of the control signal or, you know, in this case, that FWP, the feedwater pump has the control signal. It doesn't really work so well without it, because we're doing an initiating event. But assuming it was a backup system, so to speak, you would have it -- that is input into various parts of the tree.

Where exactly you would input that, that's the part of the last task we would go through and see how you would actually get this into the tree, so you get all the right dependencies and it fits in properly. I mean, it's not that you just take the results of this and stick it in. One thing also, because this is automatic control, there is also let's see an AND gate above that. It's really not just a simple AND gate, because there's human recovery actions.

So at various points you would have to consider human recovery, you know, operative recovery to prevent actually having lost the feedwater system, because you lost the signal.

CHAIRMAN APOSTOLAKIS: Did you give any examples of these 421 individual failure modes?

MR. MARTINEZ-GURIDI: I have a couple of examples coming up.

CHAIRMAN APOSTOLAKIS: Okay.

MR. MARTINEZ-GURIDI: By the way, these have a total number, for example, for the individual failure modes a total of -- in individual failure modes, a subset of them cause system failure.

CHAIRMAN APOSTOLAKIS: What? Say that again.

MR. MARTINEZ-GURIDI: We have -- we are considering 421 individual failure modes.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. MARTINEZ-GURIDI: Some of them consistent failure and some of them --

CHAIRMAN APOSTOLAKIS: Not all of them lead to failure of the --

MR. MARTINEZ-GURIDI: Right. Some of them will cost a lot of --

MEMBER BLEY: Some are mobile themselves.

MR. MARTINEZ-GURIDI: By themselves, because --

MR. KURITZKY: This is the input to the

tool not the output.

MR. MARTINEZ-GURIDI: No, no, no, this is -- yes. Well, I mean, essentially, I mean.

MR. KURITZKY: Exactly, yes.

MR. MARTINEZ-GURIDI: All of these combinations were examined by the tool. As I've said all of this cause system failure. And I also said and that will be measured in Louis' presentation.

MEMBER BONACA: A lot of years of operation of this system, did you find significant information regarding performance?

MR. KURITZKY: We -- I think, Louis, you looked at, I think 15 years of -- for just the one plant and found one instance of a reactor trip due to feedwater digital -- digital feedwater control system failure. Now, the problem with trying to compare the numbers is we're just looking at the loss of the automatic control, so if someone actually had a loss of automatic control, they may not -- if they correctly -- if the operator is corrected for it, there would never be a trip and you wouldn't necessarily get it reported. So, you know, we don't have any.

MEMBER BONACA: Well, the operators were not very capable of compensating often times. The challenge you would get to when you control --

MR. KURITZKY: Right, right. And there was one case, obviously, where there was a failure of the automatic system and it, obviously, wasn't corrected in time, because there was a reactor.

MEMBER BONACA: It might not even be a failure of the automatic system. It might be the system does what it's supposed to do, but maybe he has a situation where still it doesn't catch up in time and its cram the course.

MR. KURITZKY: Yeah, I don't know if we have any details on the actual to back that up.

MEMBER BONACA: Okay.

MEMBER SIEBER: Just so I understand, you can have a fault in the system that will reposition several controls, but if you -- and that's a fault in the system. And if it doesn't trip the plant, you don't have a consequence.

MR. KURITZKY: Right. And in fact, actually, there is a little disconnect with trying to compare operational experience, because the success criteria for this model was if the system switched from automatic to manual mode, you know, a controller did, we call that a failure.

MEMBER SIEBER: Right. But when you --

MR. KURITZKY: That's right.

MEMBER SIEBER: It will self-compensate.

MR. KURITZKY: Right. It will self-compensate, right.

MEMBER SIEBER: Or, you know, a valve could -- a positioner on a valve could fail, for example, and the valve would go closed and pending on what valve it is, you might survive that.

MR. KURITZKY: Right, right.

DR. GUARRO: Would you say that, essentially, what you are doing here is a form of what in the soccer world is called integration testing? Because essentially, you are -- it's -- you know, what that involves normally is that, you know, the operational profile is explored. Here you are extending that to the fault space, which is actually something that has been suggested, you know, as a way of exploring that great boundary between the design envelope and outside the design envelope.

And the fact that you are using, essentially, the -- a copy of the software with all the modules, so that's equivalent to integration testing. In fact, in many cases that's exactly -- you know, people test software in a way with a simulator because they don't really -- you know, it's rare that people can do integration testing in a -- well, and the space system is like it's called test like you fly. But, you know, so here is the test like you operate, meaning that you have the software in the actual platform or the actual processor with the actual firmware, etcetera, etcetera, etcetera.

MR. MARTINEZ-GURIDI: I agree with your observation with one caveat, which is that in the world of software, it's very difficult, perhaps impossible test or impossible to pass, because the software, you know, is so complex.

DR. GUARRO: Well, you know, people don't do that. You know, what they do, they decide, you know, what combinations of inputs they are going to test. And you are doing the same with the combinations of inputs that are represented by this component faults. Those are system states that define the input to your estimate, simulations last testing them.

MR. CHU: Yes, Sergio, I agree with you. You point out the potential application of this kind of tool. You know, essentially, we have simulated for this incident and we can use the tool to whatever test you do. And our last test is on the protection system, that's what we are planning to go to develop something like this for the digital feedwater control system. And then use it, try to use that on a simulation tool to develop our model for the interpretation system. An application of that simulation will be, you know, using it to do other kind of testing, licensing applications possibly.

MR. KURITZKY: I think also one of our presentations mentioned directly to what Dr. Gerardo mentioned was that, you know, when you're talking about integration testing, you know, that gets used in the software world, we mentioned that using this is something that would benefit in the design phase, because we uncovered a couple of failure modes, not obvious failure modes. I think that's a couple of examples that Gerardo is going to get to, in that you wouldn't necessarily pick up unless you did that type of testing. So it probably is very similar to what you are saying.

DR. GUARRO: I guess, you know, the limitation that I see in this approach is the fact that if you wanted to use it in a design stage, rather than in a, what's called, verification stage, then you would have trouble, because you wouldn't have a definition of the software that is so detailed that you can simulate it at this level of fidelity.

MR. KURITZKY: Yes, and we couldn't do it early. Yeah, it would have to be down -- you know, in the downstream of the life cycle, I guess.

DR. GUARRO: Right.

MR. MARTINEZ-GURIDI: While the tool we consider is pretty realistic, the timing of occurrence of a failure mode is just roughly approximated. That is we only consider one failure mode, of course, after the other. On the other hand, we found out that the order of failure modes which occur was found important, because fault-tolerant features of the system cause reconfiguration of the system.

One example of this is, for example, of a failure mode of the main CPU causes system failure. So it's a single failure. By single failure we mean, there is a -- it's an individual failure mode that causes the system to fail. Then there is another failure mode of the main CPU that does not cause system failure, but it is detected, so the backup takes automatic control. And then when the first failure mode occurs after the second, the system doesn't fail any more, because the main CPU is not controlling any more.

So that's something that is -- that's another insight that we have about modeling digital systems, that the order of the failures is really relevant.

CHAIRMAN APOSTOLAKIS: I don't understand what it means when the first failure mode occurs after the second. Either it's there or it isn't.

MR. MARTINEZ-GURIDI: Well, for example, in our case, we are modeling an event the frequency happened during one year. So we are looking at what would happen with the system throughout one year. In that year, there is a possibility of system -- that the failure A happens, for example, in the first three months.

CHAIRMAN APOSTOLAKIS: Why? Why? I mean, this comes back to this error force in context idea. I thought software always reproduced the output given the same input. So something happened, some input changed?

MR. MARTINEZ-GURIDI: Right. There was a failure. There is a hazard failure mode. Remember we're talking just about hazard failure modes.

CHAIRMAN APOSTOLAKIS: Yes, but these are not due to aging, are they?

MR. MARTINEZ-GURIDI: No. I mean, it just randomly happens.

CHAIRMAN APOSTOLAKIS: Due to what though?

MR. MARTINEZ-GURIDI: Due to random nature of hardware failures.

MR. KURITZKY: Just like a pump failure or a valve failure.

CHAIRMAN APOSTOLAKIS: Right.

MR. KURITZKY: We're just talking here -- here we're just talking hardware failures.

CHAIRMAN APOSTOLAKIS: Right.

MR. KURITZKY: It could be age-related. It could be, you know, a corrosive environment. It could be whatever, you know, failure cause you have for hardware failures.

CHAIRMAN APOSTOLAKIS: And you -- by the way, another thing we have not discussed today is another major assumption or boundary condition to what you are doing is that you have excluded fires.

MR. MARTINEZ-GURIDI: Yes, this is only internal events.

CHAIRMAN APOSTOLAKIS: External.

MR. MARTINEZ-GURIDI: Only internal events, that's correct.

CHAIRMAN APOSTOLAKIS: Now, have people seen these kinds of failures that you are talking about? Have there been any failures of this type anywhere?

MR. KURITZKY: Of digital feedwater control systems?

CHAIRMAN APOSTOLAKIS: No, of the individual hardware pieces of the CPU?

MR. MARTINEZ-GURIDI: Well, I mean, certainly. I mean, there are publications on at least failure modes and even data about failure modes, so these are -- these failures have happened.

CHAIRMAN APOSTOLAKIS: But again, on the major failures due to digital systems, due to software, for instance, these are really -- I mean, there are discussion about your French Arian, and so on, are there any failures that are equally well-known due to the failure modes that you are investigating? Where hardware failed, in other words. Something in the computer failed. Are there any failures like this? Sergio, have you heard of any or is it hard to tell?

DR. GUARRO: Well, I am sure something may have happened. You know, the failures that I am familiar with and I, you know again, am more limited to this space environment than not being of this nature.

CHAIRMAN APOSTOLAKIS: More of the software?

DR. GUARRO: Software.

CHAIRMAN APOSTOLAKIS: The computer, the computer program in other words.

DR. GUARRO: Yes, the software design has been the major problem.

MEMBER BLEY: No, they tend to be those things that can of themselves or in some kind of common-cause way lead to real difficult situations where these, I think, generally take one thing out of service.

DR. GUARRO: And something that has been pretty common in complex digital systems has been, you know, what I would call contention failures. When you have overloaded the system in terms of resources, you know, memory or communication channels, you know.

MEMBER BLEY: And then things really funny happen.

DR. GUARRO: Yeah. Then these weird common-causes --

CHAIRMAN APOSTOLAKIS: But these are not hardware failures, are they?

DR. GUARRO: No. No, they are not hardware failures. Well, the hardware gets overwhelmed by too much digits coming in, essentially.

MEMBER BLEY: Which is almost -- at least some of those cases are almost a testing failure, because you didn't expect that kind of input, so you never tested to see how the system would respond to that kind of input.

CHAIRMAN APOSTOLAKIS: That I would put it in the domain of the software problems, not the hardware the way we are discussing it here.

MEMBER BLEY: It's real fuzzy. I mean, it's ending up overwhelming the hardware and that's the way the things interact. Where the software is putting it ends up taking it out of balance.

DR. GUARRO: Right. You know, I think it's software in the sense that it is the logic of the system that fails, you know, either in terms of timing or in terms of our location or execution and so forth. So in that sense, it's software.

CHAIRMAN APOSTOLAKIS: Louis, you have reviewed the operating experience.

MR. CHU: Yes, actually --

CHAIRMAN APOSTOLAKIS: Have you found any of those?

MR. CHU: Well, there is an LER for this particular system. It is hardware-related failure. It happened to, I think, an early version of this digital feedwater control system. The cause was some kind of interference like radio frequency interference, because some cable was not properly shielded. And it is a hardware failure as a result. It's suddenly like a signal was sent to the flow control valve to either open or close it.

CHAIRMAN APOSTOLAKIS: But what is it that fail?

MR. CHU: The cause incorrect signal generated.

CHAIRMAN APOSTOLAKIS: Is that a software issue?

MR. CHU: It is hardware, hardware failure --

CHAIRMAN APOSTOLAKIS: Why is this hardware?

MR. CHU: -- generating the incorrect signal.

CHAIRMAN APOSTOLAKIS: And that's my question. What hardware failure generated that signal?

MR. KURITZKY: Incorrect shielding.

MR. CHU: Right. Due to the interference some incorrect spurious signal was generated. I have to look at the LER more carefully.

MR. KURITZKY: But it wasn't a software

failure that led to an incorrect signal. It was a physical hardware failure mode.

CHAIRMAN APOSTOLAKIS: And what was that physical hardware failure?

MR. KURITZKY: The fact there was inadequate shielding and so they felt that the radio frequency environment was such that it generated a false signal.

DR. GUARRO: So more than a failure you could say that it was incorrect hardware design or engineering, because it was put there from the beginning.

MR. KURITZKY: That's the cause.

DR. GUARRO: Right. I know.

MR. KURITZKY: Right, right.

DR. GUARRO: I'm just trying to make it, you know, a little bit -- because I think George is trying to understand it was something that happened. Well, I think, you know, there was a dormant condition and then, you know --

MR. KURITZKY: Right.

DR. GUARRO: -- that this --

CHAIRMAN APOSTOLAKIS: What was shielded now, a cable or what?

MR. KURITZKY: A cable.

DR. GUARRO: A cable.

CHAIRMAN APOSTOLAKIS: And not this part of what you call hardware failures here?

MR. CHU: Right yeah, I guess the interference is the cause of hardware failure. And of course, in our model, we don't model the cause.

MEMBER SIEBER: There should be failed to perform.

CHAIRMAN APOSTOLAKIS: Yeah, shielding is the common failure.

MR. MARTINEZ-GURIDI: It was inappropriate.

DR. GUARRO: There was an environmental condition of some sort, so there was some electromagnetic wave that came in from somewhere that was not shielded property by this design and so it was translated. Now, it became a signal inside the cable that was sent to the valve.

MEMBER BONACA: A signal caused by --

MEMBER BLEY: We actually had that kind of problem 30 years ago. If you ran a welding machine anywhere near one end of the plant, it tripped, you know, just from picking up those kind of signals. There is nothing peculiar about -- I can't even say that. There might be something peculiar about the design of the control system that allowed that noise to create the --

DR. GUARRO: To become, yeah, now a digit somewhere.

MR. KURITZKY: But let me also just say a couple words about the idea of whether or not hardware failures, the type that are being discussed here, actually manifest themselves in the actual operating experience. And one thing is -- well, first of all, there have been some digital feedwater control system failures in this last year. And they generally come from failures of power supplies. And that's a hardware failure and I think we have that in our model or it should be the hardware. So there are hardware failures that do occur in the operating experience that lead to digital feedwater control system failure.

The second thing is more conjecture. I would imagine, as you mentioned, the more the significant events, the ones that come more to attention are software-related, because of the fact that the software can affect multiple trains, multiple components, so it tends to lead to what potentially could be a more serious condition.

Whereas, in general, in the nuclear field anyway, we would expect that a hardware failure somewhere in that system hopefully would not be sufficient enough to actually call it some effect that would be significant enough that it would (A) be reported LER, (B) be something that we would have a whole report written about it in the literature, because it was such a significant event.

So I think there is a tendency to see more of those occur from software just because of the design of the system, particularly in the nuclear area.

DR. GUARRO: Yeah, I think when it comes to the hardware failures of digital systems, the question is are they such that they are actually different in effects, perhaps, or in the former manifestation than hardware failures that, you know, occur with analog systems for the same function. I mean, the power supply, you know, if the power supply --

MR. KURITZKY: Right.

DR. GUARRO: -- will fail an analog or digital or whatever --

MR. KURITZKY: Right.

DR. GUARRO: -- you lose power. You know, you have a spike of power and you lose something important to your system, no matter what it is digital or analog or relay hardware.

MR. KURITZKY: Right.

DR. GUARRO: So there is nothing special about that.

MR. KURITZKY: Right. I think the two examples that Gerardo is going to get to very soon hopefully, those are hardware failure, right?

MR. MARTINEZ-GURIDI: Yes.

MR. KURITZKY: Potential hardware failures. They are not events that occurred. These are obviously, you know, potential events.

CHAIRMAN APOSTOLAKIS: This is really a good example of an error force in complex situation, in that a signal comes, it's a random occurrence entirely, then there is a condition in the system that allows that system, the signal to do hard, right? So that is a good example. The biggest problem, it seems to me, is -- not the biggest one. The big problem is identifying these deficiencies, if you want to call them that, in the system that do not protect you properly against those outside influences.

MEMBER BONACA: I mean, that's stretching, I think. You may find that an error force in the context is somewhat -- I mean, it seems to me that there is a real mechanistic dependency there. You have an adequate shielding that causes -- is initiated, I mean, which is the actuation.

CHAIRMAN APOSTOLAKIS: But you must have something from the outside to treat it.

MEMBER BONACA: Yeah, sure.

CHAIRMAN APOSTOLAKIS: Yeah, that's what I'm saying. It's a combination of something happening on the outside and then the protection wouldn't be good enough. Of course, figuring out the rate of this thing outside and what it is.

MEMBER BONACA: I guess, I looked actually at the error force and function as human-related.

CHAIRMAN APOSTOLAKIS: Well, it's borrowed from the human.

MEMBER BONACA: Yeah.

CHAIRMAN APOSTOLAKIS: But the idea of context, I think, is -- makes sense.

MEMBER BONACA: Yeah.

CHAIRMAN APOSTOLAKIS: That doesn't mean we can identify them.

MR. MARTINEZ-GURIDI: But coming back to your original question, failures of hardware have happened and the occurrence have been tracked by some organizations and published in --

CHAIRMAN APOSTOLAKIS: But are they failures that are induced by something else that happened, like in this case, or they are intrinsic failures that cause some effect?

MR. MARTINEZ-GURIDI: I think both possibilities are -- can occur.

CHAIRMAN APOSTOLAKIS: And are they more likely than software problems?

MEMBER SIEBER: That's another question.

MR. KURITZKY: One we can't answer.

CHAIRMAN APOSTOLAKIS: Well, it is certainly getting a lot of attention.

DR. GUARRO: Well, I think also well, are they more likely or are they more severe in consequences, because that's the thing, you know.

CHAIRMAN APOSTOLAKIS: Well, how can they be? I mean, we already have major failures due to software failures.

DR. GUARRO: Well, that's what I mean.

CHAIRMAN APOSTOLAKIS: I mean, the thing just failed.

DR. GUARRO: Well, yeah. What I'm saying is that they -- a software common-cause failure typically has more severe consequences than an individual hardware fault, because typically they are fault-tolerance built into the system to remedy the latter. Whereas, the first, you don't have the protection.

MR. MARTINEZ-GURIDI: But you can also have hazard common-cause failures.

CHAIRMAN APOSTOLAKIS: Sure.

MR. MARTINEZ-GURIDI: Like in our case, for example, if you have common-cause failure of both CPUs, your system is --

DR. GUARRO: Well, yeah, but that's, you know --

MR. MARTINEZ-GURIDI: I'm -- I think that has happened, too.

MR. KURITZKY: The point is right now, we don't know enough to be able to say which one it is more likely, I think. I mean, you -- maybe you have some experience that leads you to think one or the other, but we, I don't think, can tell you here which one is more likely. And we considered them -- the possibility of both and at this stage, we're just going through the concept of the modeling technique.

CHAIRMAN APOSTOLAKIS: So where are you, Gerardo? Are you --

MR. MARTINEZ-GURIDI: I am now on 19.

CHAIRMAN APOSTOLAKIS: And this is your total presentation or you have another set of slides?

MR. MARTINEZ-GURIDI: No, this is it.

This is all my --

CHAIRMAN APOSTOLAKIS: So when the schedule says --

MR. MARTINEZ-GURIDI: 11:45 it said finish.

MR. KURITZKY: My intention is -- we fell 45 minutes behind on initial presentations. So if we can gain 15 minutes back on each of the three, we will be back on track. So if we can actually finish within half an hour of the scheduled time, the 12:15, we'll be on pace to get back.

MR. MARTINEZ-GURIDI: Well, let's see, three charts, two and a half.

MR. KURITZKY: Speed up.

CHAIRMAN APOSTOLAKIS: You might even beat it.

MR. KURITZKY: Don't bet on it.

MR. MARTINEZ-GURIDI: Okay. I want to try to quickly present a couple of examples of firmware. Very interesting is a couple of single failure modes. One example is one single failure mode that were identified in these methods.

One failure mode is the MFRV demand signal from the main CPU to the MFV is low. That is the electrical signal from the main CPU to the controller is low. The MFV controller in turn sends a signal to the back to the PDI controller and provides some feedback to the main CPU. The system appears to be designed for the main CPU to detect this failure and cause of failover to the backup CPU. And in that way, the system keeps controlling feedwater.

However, the failover to the backup CPU has a one second delay. And the signal from the MFV controller to the PDI controller has no delay.

CHAIRMAN APOSTOLAKIS: So where in your analysis are you taking into account these delays? IN the simulation?

MR. MARTINEZ-GURIDI: The software, in the simulation. In the simulation we have included all these timings, so that it takes into account this delay.

CHAIRMAN APOSTOLAKIS: So how did you figure this out? The computer, the simulation said something?

MR. MARTINEZ-GURIDI: We -- during our studying the system, we learned of the one second delay and then we implemented into the simulation.

CHAIRMAN APOSTOLAKIS: And then as a result of the simulation, you concluded what's here?

MR. MARTINEZ-GURIDI: Correct.

MEMBER BLEY: I'm curious. A one second delay seems an incredibly long time for a digital system. Why did they do that? Do you know? I'm just curious. It has nothing to do with your analysis.

MR. MARTINEZ-GURIDI: I don't know. Do you know? That is the way the system is built though.

MR. KURITZKY: Unless there's a typo in the documentation we have. It could be a little n missing from that, you know, I don't know.

CHAIRMAN APOSTOLAKIS: We love taking advantage of the fact that you have the backup CPU.

MR. MARTINEZ-GURIDI: Exactly.

CHAIRMAN APOSTOLAKIS: And this is what the designer intended?

MR. MARTINEZ-GURIDI: Well, it seems to us that --

CHAIRMAN APOSTOLAKIS: But we don't know.

MR. MARTINEZ-GURIDI: -- the designer --

MEMBER SIEBER: Some we don't know.

MR. MARTINEZ-GURIDI: It seems to us that the designer intended that the backup CPU would take control of the system. That's why the bullet say the system appears to be designed for the main CPU to take this failure and cause of failure.

CHAIRMAN APOSTOLAKIS: And you will still declare this as a failure of the automatic?

MR. MARTINEZ-GURIDI: Exactly. It's a failure of the automatic.

CHAIRMAN APOSTOLAKIS: That's not a failure of the system.

MR. MARTINEZ-GURIDI: It's not a failure of the system. It's failure of automatic control.

CHAIRMAN APOSTOLAKIS: And would the operators be surprised?

MR. MARTINEZ-GURIDI: I have no idea. I can't --

CHAIRMAN APOSTOLAKIS: Because it is now controlled, supposed to be, automatically.

MR. MARTINEZ-GURIDI: Well --

CHAIRMAN APOSTOLAKIS: I mean, manually.

MR. MARTINEZ-GURIDI: -- what we probably could see in the control room is that now the PDI has taken control and they have to take manual control of the system. They wouldn't -- understand that they have to take manual control, but they don't know why the system --

MR. KURITZKY: Is telling them they have to take manual control.

MR. MARTINEZ-GURIDI: It's telling them that they have to take manual control.

CHAIRMAN APOSTOLAKIS: Okay.

MR. CHU: This is one example that our analysis, our understanding actually differs from plant hazard analysis. Plant hazard analysis, in this situation, there will be a failover, but the system must be controlled. The automatic control continues.

CHAIRMAN APOSTOLAKIS: Okay.

MR. CHU: But based on our detail, you know, and understanding of plant document and how the system works, we think there will be a -- the PDI controller will become the manual controller for the valve. So it requires very detailed analysis on the plant document to come to this kind of value.

CHAIRMAN APOSTOLAKIS: Now, could this approach that you have taken supplement it, by the only one I'm very familiar with, with DFM that deals with software failures? And it is also based on simulation. Would you put the two together?

MR. MARTINEZ-GURIDI: That is certainly a possibility.

CHAIRMAN APOSTOLAKIS: Well, I know it's a possibility, but would that be something that you would like to pursue?

MR. CHU: We have not thought about that.

MR. MARTINEZ-GURIDI: I --

CHAIRMAN APOSTOLAKIS: What?

MR. CHU: We have not thought about it. I think it's an idea to --

CHAIRMAN APOSTOLAKIS: I think there is also, I mean, I'm not -- I don't mean you, in particular, but there is a natural tendency for researchers to really push their own approach as much as they can. And I think as an Agency, we have to fight that a little bit. There is a methodology out there that deals with something that you are not dealing with, but has a hell of a lot of similarities with what you are doing.

I think it's a good idea to explore putting them together, even though you are not the developers of that methodology. Okay?

MR. MARTINEZ-GURIDI: Yes, but again --

CHAIRMAN APOSTOLAKIS: Louis is smiling.

MR. MARTINEZ-GURIDI: -- I think that's one possibility. But I think another possibility would also be extending this method to also account for software failures.

CHAIRMAN APOSTOLAKIS: I don't see how you would do that.

MR. MARTINEZ-GURIDI: Well, I think there is -- I think it's --

CHAIRMAN APOSTOLAKIS: But why? Well, of course, you can explore things.

MR. MARTINEZ-GURIDI: Yeah.

CHAIRMAN APOSTOLAKIS: But I would caution you against the natural tendency of pushing your stuff as much as you can, if other people have already spent 30 years developing something else, which seems to compliment what you are doing. You are both relying on simulation. There is this advantage that Sergio mentioned earlier that through the truth tables, you can trace back what caused the particular failure at the system level.

Now, you said earlier, Gerardo, that you can adjust your methodology to also do that. Fine. So but, I mean, there are so many similarities of, it seems to me, some effort to combine would be useful.

MR. KURITZKY: Let me speak.

CHAIRMAN APOSTOLAKIS: If you put your ego a little on the side for a while.

MR. KURITZKY: Gerardo, let me respond, because I don't think it's appropriate for BNL to respond to what work we will be pursuing.

CHAIRMAN APOSTOLAKIS: Yeah, you guys don't have to decide.

MR. KURITZKY: So we will definitely take that feedback and we will consider it as part of our consideration.

CHAIRMAN APOSTOLAKIS: That then could be some sort of an approach that combines both hardware and software failures. And there are really many, many similarities here. But this idea, for example, of the prime implicants, that might be a way of addressing the software problem. I don't know. If it does work, it does the work. But I mean, that might be something that you may want to explore, but that's really a decision to be made by the staff.

MR. KURITZKY: We appreciate the input.

CHAIRMAN APOSTOLAKIS: Because we really have to show some progress on all fronts. I mean, we can't --

MR. KURITZKY: All right.

CHAIRMAN APOSTOLAKIS: I see the SRM here. The Commission is encouraged by what it heard on April 7th. They met with the staff and the industry. They are meeting with us in June.

MR. KURITZKY: You've got 10 more minutes, Gerardo.

MR. MARTINEZ-GURIDI: Well, this --

CHAIRMAN APOSTOLAKIS: No, even less.

MR. MARTINEZ-GURIDI: -- example, I don't know if you want to go over it or I just keep it.

CHAIRMAN APOSTOLAKIS: What is your next example?

MR. MARTINEZ-GURIDI: Yes, it's example -- another example of an individual failure mode that cause the system failure.

CHAIRMAN APOSTOLAKIS: Well, you are listing issues here on the 21, you mean?

MR. MARTINEZ-GURIDI: No.

MR. KURITZKY: 20. 20 was the next example.

MR. MARTINEZ-GURIDI: 20 is the next example. It says Example 2.

CHAIRMAN APOSTOLAKIS: Well, go over it here quick.

MR. MARTINEZ-GURIDI: Well, basically, each CPU has two modes of operation. One is controlling and tracking. For the automatic control of the system, one of the CPUs has to be in controlling mode. Normally, the main CPU is controlling and the backup CPU is tracking.

And on the other hand, each controller has to modes of operation, automatic and manual. The failure mode is that the signal transmitting the bypass mode of operation from the bypass controller to the main CPU incorrectly becomes set to manual. It is normally an automatic. It incorrectly becomes set to manual. Upon receipt of this signal, the main CPU becomes automatically changes its status to become operating and tracking mode. So since both CPUs are in tracking mode, there is a loss of automatic control. There is no CPU controlling the system.

CHAIRMAN APOSTOLAKIS: Okay.

MR. MARTINEZ-GURIDI: A recap of the issues we have identified as part of this work is there is the difficulty in finding out what is the level of detail needed to model the digital features.

CHAIRMAN APOSTOLAKIS: It comes back already commenting about your 52 criteria, right?

MR. MARTINEZ-GURIDI: Those are right. There is a potential lack of completeness in the failure mode identification by this, again, a very big issue. There is difficulty in relating the function of failure modes, which is really what is used in PRA, the physical failure modes and mechanisms, which is sometimes what is reported in publications.

We have not really addressed some detailed features, such as communication, synchronization and voting, that are potential contributors to system reliability. And there is difficulty in finding out the effects of individual and combinations of failure modes.

So in light of that, I want to briefly mention some potential research which will be to do more extensive search for other available FMEAs. Sharing experience with organizations and countries.

CHAIRMAN APOSTOLAKIS: Yeah, keep going.

MR. MARTINEZ-GURIDI: Okay. I'm done.

MEMBER SIEBER: Let me ask a question about our country and mother.

MR. MARTINEZ-GURIDI: Yes.

MEMBER SIEBER: It's related to your last slide. There is a lot of ways that digital I&C systems can fail that don't result as a consequence to the plant necessarily or any big perturbation. When you do a plant PRA, how do you take the fact -- that fact into account when you have, you know, 400, 500, 10,000 potential failure modes, 90 percent of which don't cause a failure in the plant? How do you do that?

MR. KURITZKY: Let me --

MEMBER SIEBER: Do you end up with two different analyses?

MR. KURITZKY: Well, again, this is -- I can tell you how it would sound to do it here with our simple analysis. When you get to a plant, it's going to be more complicated, but right now, that simulation tool it only -- in that simulation tool, what we didn't mention was there are certain rules that are specified that define what system failure is.

In our case, it was loss of automatic control of that one thing.

MEMBER SIEBER: Right.

MR. KURITZKY: And so you have that rule in there, so the only combinations that get spit out of that simulation are the ones that call us that there is going to be the failure of the control.

MEMBER SIEBER: And that doesn't necessarily result in a threat to the plant.

MR. KURITZKY: That's right.

MEMBER SIEBER: You know, because you get that kind of thing even within loss.

MR. KURITZKY: That's right. So when you go to actually integrate this with the PRA, that's when you have to determine how it is going to interact with the other aspects of other elements of the PRA and you have to define your success criteria, such that it is going to match with that. So if --

MEMBER SIEBER: That's a hard thing to do.

MR. KURITZKY: It's not -- well, yeah,

exactly.

MEMBER SIEBER: Sure.

MR. KURITZKY: Not straightforward.

CHAIRMAN APOSTOLAKIS: In --

MEMBER SIEBER: Yeah, I understand.

CHAIRMAN APOSTOLAKIS: -- connection with the recommendation I made earlier, it seems to me that there is a third element of the error force in context. In other words, are we now ready to start integrating these ideas? Again, I'm not saying that it has to be there, but your Appendix C at least indicated that whoever wrote it thought it was a good idea.

But you guys, you don't -- how come you ignored it in this project?

MR. MARTINEZ-GURIDI: We don't have the money.

CHAIRMAN APOSTOLAKIS: Come on. So anyway, can one put together an approach that would combine this concept of error force in context? And the example you gave us is really a very good example. I mean, you have the signal, random dang do dang, something is wrong in the system and then you have the context. And then within that combine your approach with DFM or something else, I don't know what, and start talking about an approach that truly or maybe what the higher state is, I'm not -- I'm talking about DFM, because I'm more familiar with it.

To start having an approach that will address the whole problem, so we won't have this issue of oh, but this is outside the scope or this is outside the scope, because we really need to make progress on that front. And again, if somebody else has done it, guys, that's fine, take advantage of it. You don't have to develop everything yourselves.

I think that would be a good way to proceed. Okay. Trying to put everything together. And, you know, looking at 36 or 35 million, 36 million combinations is really an impressive thing. You have actually done that, Louis, 36 million?

MR. KURITZKY: The first 4 or 5 million are hard.

CHAIRMAN APOSTOLAKIS: You're the one who six years ago told me that this method or some other method was too complicated. This is simple.

MR. CHU: It's automated.

CHAIRMAN APOSTOLAKIS: Ah.

MR. CHU: It's done on the PC. It took like a week of execution to complete.

MR. KURITZKY: A week?

CHAIRMAN APOSTOLAKIS: Well, it was a cheap PC. Any other questions or comments for these gentlemen from the Members or Members, I mean, Sergio, as well? Okay. So then after lunch, we will talk about reliability modeling.

MR. CHU: Yes.

CHAIRMAN APOSTOLAKIS: We may catch an early flight. Thank you very much. The discussions were very useful. So we will reconvene at 1:15.

(Whereupon, the meeting was recessed at 12:15 p.m. to reconvene at 1:21 p.m. this same day.)

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

1:21 p.m.

CHAIRMAN APOSTOLAKIS: We're back in session.

Dr. Chu?

MR. CHU: Yes. My name is Louis Chu. I started working on digital work back in 1999 doing some literature review and since then it was on and off. I work on digital I&C related to work. It was only the past two or three years that we have increased effort on the work and we have many -- two more people, basically, becoming involved in the work.

What I'm presenting today, I have two sets of presentations. I think the subject is more traditional, it's more traditional PRA, therefore, a lot of things are pretty standard. Therefore, I tend to think I should be able to go over them pretty quickly.

The first subject is modeling of the digital feedwater control system. As you have heard, the objective is to look at the traditional methods, fault trees and Markov model, evaluate their capability and limitations. As you have heard from this morning, due to the level of the detail at which we want to model the system, it was not possible to develop these models from scratch without the use of a simulation tool.

Once you have the simulation tool, then the rest of the analysis is kind of straightforward. Fault tree, for intents of fault tree, you already have the sequences, therefore, we just used the standard quantification method to quantify it and this represents an approximation to the solution.

Further, Markov model making use of the outcome of this simulation tool, you can prepare a full model of the Markov model and it happens we can solve the Markov model analytically, such that quantification is pretty straightforward.

CHAIRMAN APOSTOLAKIS: Analytically or numerically?

MR. CHU: Analytically.

CHAIRMAN APOSTOLAKIS: But you have too many slides -- states.

MR. CHU: Well, the simplification comes into, you know, when we look at singles, doubles and triple sequences and if you look at the probability, in our calculation, we can calculate what we missed. Say if we only look at single sequences, then you can see the converged -- conversions.

CHAIRMAN APOSTOLAKIS: The interest today is not really in how you solved the Markov model. I think the real interest is in how you got the transition rates, right?

MR. CHU: That's the next presentation, that's discussed next.

CHAIRMAN APOSTOLAKIS: Well, I mean, solving the Markov model is not something that is of great interest.

MR. CHU: Therefore, I think I can go over the slides pretty quickly.

CHAIRMAN APOSTOLAKIS: Well, yeah, I mean.

MR. CHU: Unless they are -- since you are particularly interested.

CHAIRMAN APOSTOLAKIS: I would go to slide 5 or 4 right away.

MR. CHU: 4 or 5, okay.

CHAIRMAN APOSTOLAKIS: 4, go to 4.

MR. CHU: 4 is basically a summary of what we talked about in the morning. Due to the complexity of the system and if we want to develop the Markov fault tree model at the level of detail we wanted to do, we have to have this simulation tool.

Regarding the level of detail, why we choose this level of detail, there are -- is a few reasons. One is availability of generic failure rate information. And at the level of detail that we modeled, we were able to find some generic failure rates.

Another reason is we are kind of influenced by the hazard analysis. The level of detail that plants' hazard analysis was performed is consistent with this. And another reason, of course, is that software is an important part of the system. In order it will capture software in our modeling, we need to have our model at this level, such that the role software in place comes into -- become kind of -- it's included in our modeling.

CHAIRMAN APOSTOLAKIS: Again, you are bringing up the issue again of software failures being included. I thought we agreed that they are not? Because if you have a software fault that is due to some specification there, all right, I don't know that you can account for it here. You are not looking for it.

MR. CHU: I look at it from two ways. First, normal behavior of the software. That we expressly included in our simulation tool. In that sense, I think, we are doing a reasonable job.

CHAIRMAN APOSTOLAKIS: Well, yeah, and there are many tests to which the software is subjected. I mean, this is nuclear, right? We do the best we can. There is this review of the life-cycle, all that stuff has already taken place. And now we have the thing running and it's these unusual extraordinary situations the error forcing contexts that are of concern.

So, you know, to say that you simulated it under normal conditions, yeah, I mean, other people have done it, too, before you. I mean, before it was installed, I'm sure they tested it by the way. Let's not forget that these are --

MR. KURITZKY: I think Louis is referring into the model itself. There is no question that all of the software life-cycle previously have been done on anything in the plant.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. KURITZKY: It's the point I think Louis is talking about that we consider the normal behavior of the software as part of the model. It's something that has to go into the viability of the model to consider the software. So it's the quantification of software failures that we are not addressing yet.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. KURITZKY: But we still are

considering the software in developing the model.

CHAIRMAN APOSTOLAKIS: All right.

MR. CHU: Yes, I would say in some cases, as indicated in the two examples Gerardo talked about, you know, software plays a role in the -- in those two examples. The behavior of the system kind of deviates from what is expected. In that sense, you can say we have found examples in which the design of the system including the software could be questionable. In that sense --

CHAIRMAN APOSTOLAKIS: I understand the design of the system.

MR. CHU: -- in the review itself, the weakness in the design, you cannot review --

CHAIRMAN APOSTOLAKIS: Software is logic, the logic of the software, that's really what we mean. And, you know, I don't think that two failure modes that Gerardo would identify had to do with logic. I mean, you have this external interference and installation is not good enough.

MR. KURITZKY: Excuse me, that wasn't the examples that we're referring to with the two in Gerardo's presentation about the one case where the -- both the CPU, the main CPU --

CHAIRMAN APOSTOLAKIS: The timing, the

timing.

MR. KURITZKY: Yeah, the one that had a one second delay, so the other -- the PDI took over. And the other case was the one CPU went to tracking, you know, the other.

CHAIRMAN APOSTOLAKIS: Right.

MR. KURITZKY: So there is limits that we can.

CHAIRMAN APOSTOLAKIS: Well, so, okay. So you managed to get some of it.

MR. KURITZKY: Right.

CHAIRMAN APOSTOLAKIS: But I don't think you can claim that you really focused on the software.

MR. KURITZKY: No. We were not trying to claim that.

MR. CHU: All right. Again, we are considering how the failure modes --

CHAIRMAN APOSTOLAKIS: Yes, yes.

MR. CHU: -- and the software response to postulated hardware failure.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. CHU: And we have done that evaluation in a very systematic way. Okay. That's the first bullet. With the simulation tool we generate sequences that cause system failures. And these sequences are used in quantifying the system failure probability. System failure probability is used in conjunction with frequency that we lose the system.

CHAIRMAN APOSTOLAKIS: What is the size of the Markov model typically?

MR. CHU: The size of the Markov model, basically, is determined by the number of --

CHAIRMAN APOSTOLAKIS: States?

MR. CHU: -- single, double, triple sequences. Because we -- by using the cutset of truncation, we are able to --

CHAIRMAN APOSTOLAKIS: Okay. So --

MR. CHU: Okay. Only you --

CHAIRMAN APOSTOLAKIS: -- typically, what is it?

MR. CHU: I have a table that shows it. There is something I believe 11 million sequences.

CHAIRMAN APOSTOLAKIS: So it's 11 million by 11 million?

MR. CHU: Oh, no, no.

CHAIRMAN APOSTOLAKIS: Well, that's what I --

MR. CHU: We do have to spell out the full system states.

CHAIRMAN APOSTOLAKIS: Okay. So the

actual Markov model after you do all this manipulation, what size are we talking about?

MEMBER BLEY: How many modes?

CHAIRMAN APOSTOLAKIS: X by X, what is X?

MR. CHU: We only -- we didn't have to go through that kind of counting, so I don't really know. But if you look at -- in case of signal failure, we have about 100, so that's 100 states.

CHAIRMAN APOSTOLAKIS: Okay.

MR. CHU: Then double, we have, I don't know, 30,000 say.

CHAIRMAN APOSTOLAKIS: Yep.

MR. CHU: And out of 30,000, you have two failed states, so it's 60,000. And triples, we are --

CHAIRMAN APOSTOLAKIS: So these are huge matrixes?

MR. CHU: Right. But we are able to solve the sequences and alert code, therefore solving it is pretty straightforward.

CHAIRMAN APOSTOLAKIS: It's very forward.

MR. CHU: It happens the problem can be solved analytically. I think I will come to that.

CHAIRMAN APOSTOLAKIS: Yeah, keep going then. This is the kind of thing I was interested in.

MEMBER SIEBER: Well, depending on how

many faults you assumed at some point, it's not worth extra effort to find them. You know, one and two maybe are good enough.

MR. CHU: Right, right. We use the accounts truncation. If we find, you know, after looking at the double sequences, what we missed is already pretty small comparing to the system failure probability and we can stop. In this case, we stopped at triple. I think we estimated we may miss a 5 or 10 percent of the top --

CHAIRMAN APOSTOLAKIS: Do you have an actual example of what you did?

MR. KURITZKY: Yes, I think the -- oh, is it the next page or this one?

MR. CHU: I can go through the -- there is an --

MR. KURITZKY: Yes, at the end of this slide.

MR. CHU: -- example Markov.

CHAIRMAN APOSTOLAKIS: Yes.

MR. CHU: Let me see, this one, Slide 11.

CHAIRMAN APOSTOLAKIS: Okay. But that's again generic A, B, C. Well, tell us what you want to say about Slide 11.

MR. CHU: Slide 11 gives you an example.

Here we considered four components, A, B, C and D. And the left modes system state is the perfect state. That is there is no failure at all. And then the states in this column are those system states with one failure mode happen.

CHAIRMAN APOSTOLAKIS: And the order is important basically?

MR. CHU: Sorry?

CHAIRMAN APOSTOLAKIS: The order is --

MR. CHU: Yes. The way we designate the system states, actually, tells the order. Like in this case, in this state, A_1 represent failure mode 1 of Component A happened. And B, C, D here just says they are in good condition. There's no failure. And the next state will be A_2, B, C, D, A_3, B, C, D. Similarly, we have B_1, A, C, D and I guess C_1, A, B, D and D_1, A, B, C.

So this column represent all the possible states with one failure.

CHAIRMAN APOSTOLAKIS: Okay.

MR. CHU: And our simulation tool tells us all of these -- I think there are some 400 failure modes altogether we look at, about 100 of them failed the system. For those system states in this column that failed us, we just stopped. These are of trouble state. And we can easily solve for the probability of those states. And then --

CHAIRMAN APOSTOLAKIS: There is no repair here, right?

MR. CHU: Right. That's the critical thing that makes the model solvable analytically.

CHAIRMAN APOSTOLAKIS: So let's say that on the right hand side there all the way to the right.

MR. CHU: Yes.

CHAIRMAN APOSTOLAKIS: Yeah, that the second where you are now.

MR. CHU: Yes.

CHAIRMAN APOSTOLAKIS: That's a failed state?

MR. CHU: Yes.

CHAIRMAN APOSTOLAKIS: What kind of calculation would you do?

MR. CHU: Okay. You will follow the path coming to this --

CHAIRMAN APOSTOLAKIS: Well, there may be many paths, right?

MR. CHU: No, there is only --

CHAIRMAN APOSTOLAKIS: There's only one?

MR. CHU: -- one path. There has -- it is defined by these four failures.

MEMBER BLEY: And their order.

CHAIRMAN APOSTOLAKIS: And the order is important?

MR. CHU: Yeah, the four failure modes are defined by these four designated. And it happened, in this case, you can -- we actually derive a general solution for say a sequence with n failures.

MEMBER BLEY: Now, all of the permutations of that one exist in here somewhere. In your simulation, did you determine that the ordering decides whether it has failed or not? Whether the system failed?

MR. CHU: Yes, that's the -- that's what the simulation is for.

MEMBER BLEY: So it defines the failure state?

MR. CHU: Right. So it's spelled out, I don't know, 50, 60 million sequences and out of those 11 million since correspond to system failure.

MEMBER BLEY: Okay. And somehow these are all generated automatically by some kind of rule system or something?

MR. MARTINEZ-GURIDI: The simulation tool has the rules defined by the analyst of what comprise the system failure.

DR. GUARRO: What happens if you have now a system that has recovery? In other words, you get--

MR. CHU: Then the solution will be much more difficult. If you have to solve it numerically, then it will be hard.

DR. GUARRO: Because I know that that is actually not something that uncommon. In other words, you have situations in which you may go to a whole state and then there is a reboot and you come back in certain systems. And I'm not -- you know, how that applies again to the nuclear power control systems, that's a different story. But when you talk about digital system in general, there are a lot of systems that have such characteristic. In fact, all fault-tolerate, you know, systems more or less work in that mode. So you see a serious complication of the --

MR. CHU: That's --

DR. GUARRO: -- following this approach.

MR. CHU: For example, in the next system, reactor protection system, we don't know what the, you know, situation is. I think when it happens, then we try to tackle it.

DR. GUARRO: Well, especially -- okay.

MR. MARTINEZ-GURIDI: But let me say that in this case, the fault features are accounted.

Because, for example, if one component fails, such as the main CPU, that will be failed, but the system will continue operating with a backup CPU.

DR. GUARRO: Now, that -- yeah, yeah.

MR. MARTINEZ-GURIDI: That would be captured by this.

DR. GUARRO: Yeah, no, that I understand. That's --

CHAIRMAN APOSTOLAKIS: So all you need then is radio rates that's going that way for the failures that are in that combination?

MR. CHU: Well, not -- because the definition of these system states include successes, that is, for example, in this state, B, C, D didn't fail. So in the solution for this state, you have to include, you know, failure rates of many components, almost all of them.

CHAIRMAN APOSTOLAKIS: So the question is now how do you get those?

MR. KURITZKY: That's the next presentation.

CHAIRMAN APOSTOLAKIS: So the complexity here of the Markov approach is handled by the fact we don't have restoration for failure, correct?

MR. CHU: Right. That's an important

factor that --

CHAIRMAN APOSTOLAKIS: If you are handling thousands of these, right, or millions you said --

MR. CHU: Right. I think later I have a table that will show you the numbers, something like another million triple sequences.

CHAIRMAN APOSTOLAKIS: It takes you how long to do that?

MR. CHU: The simulation takes -- took like a week. But actually, you can split the job on two different PC and run them parallel, because each simulation is by itself. So you can breakdown the jobs. The quantification, you know, you have 11 million triples, it doesn't take long, because you have another solution in 15 minutes, I was told.

MEMBER BLEY: There's really nothing about what we are doing here that is Markovian, it looks like. This is kind of a one pass through with transition probabilities and with no repair and no settlement. It's just a multiplier.

CHAIRMAN APOSTOLAKIS: Leave your case of Markov.

MEMBER BLEY: I mean, it doesn't even have the Markov assumptions.

CHAIRMAN APOSTOLAKIS: Well, they still

assume constant rates, right?

MR. CHU: Right, right. You know the order in which the failure occurs is automatically accounted.

CHAIRMAN APOSTOLAKIS: Okay. So the interesting discussion is deferred until we start talking about the estimation. All right.

MR. KURITZKY: Right. But also to set expectation levels appropriately, the quantification-- we came up with numbers for demonstration purposes for this proof of concept model. We in no way want to insinuate that the numbers that we are going to use in our example are the numbers that other people should run and stick in their models. So it's just a demonstration.

CHAIRMAN APOSTOLAKIS: Well, that's my problem.

MEMBER BLEY: Given that, if that's true--

MR. KURITZKY: Yes.

MEMBER BLEY: -- I think that's reasonable. Have you worried at all about having old numbers in your report that this is going to become the Bible of numbers to use?

MR. KURITZKY: I hadn't thought about that, so I hadn't worried about it.

MEMBER BLEY: It will be.

MR. KURITZKY: But now that you bring it up, I hope it will not be.

MEMBER BLEY: NRC says use these and those tables will get disconnected from any text you have.

MR. KURITZKY: Right.

MEMBER BLEY: This will be the database for a lot of people who were running off doing this stuff.

MR. KURITZKY: That's a good point.

CHAIRMAN APOSTOLAKIS: That's why --

MR. KURITZKY: I had not thought about it.

CHAIRMAN APOSTOLAKIS: -- I'm very skeptical about all this.

MR. KURITZKY: Yes.

CHAIRMAN APOSTOLAKIS: I'm not sure you should publish any numbers.

MEMBER BLEY: Unless you believe them, and I don't think you do.

CHAIRMAN APOSTOLAKIS: It's really a problem. I told a story to my colleagues when I was at UCLA that I found a number for the probability of hot shorts and the fire, which is something that is also very difficult to evaluate. So immediately we called the guy who wrote the report and he said, no, no, no, this number -- I was told by this other guy. It was Sandia and some consulting firms.

And anyway, after three or four, this other guy gave me this -- this other guy gave it to me. They gave me a name at Sandia. So I called the guy at Sandia. And I said, hey, I think it was John, I realize -- I understand that you have a number for hot shorts that you gave to this organization and so on. And where did you get the number and he said from you. And then I knew how.

MR. KURITZKY: Oh, so you have the answers for us.

MEMBER SIEBER: Yeah, well, you can be free now to use those numbers.

CHAIRMAN APOSTOLAKIS: So, you know, these numbers because there are no data, no numbers anywhere, the moment they see a NUREG with numbers, that's it man, NUREG/CR.

MEMBER SIEBER: Even better.

CHAIRMAN APOSTOLAKIS: So --

MR. CHU: In our report, we need to say a lot of qualifying things.

MEMBER BLEY: Well, I think more importantly --

CHAIRMAN APOSTOLAKIS: Qualifications

won't do it. Dennis is right.

MR. KURITZKY: Well, we will have to make a decision on how we're going to deal with that, but one thing it won't be qualified. It will have to be in the actual table itself, so that it can't be disconnected from the text. Okay. Thank you for that caution.

MEMBER BLEY: And you have lots of different sources of numbers, you get lots of numbers. You know, a table somewhere that says these are examples --

CHAIRMAN APOSTOLAKIS: Only.

MEMBER BLEY: -- only and they are only here to illustrate the calculation might be okay. But anything else will become -- whatever you put in there, you will see again sometime.

MR. KURITZKY: Yeah, yeah. Good point.

MR. CHU: Since we are already at Slide 11, the next one is probably --

CHAIRMAN APOSTOLAKIS: Yes, we discussed this, didn't we?

MR. CHU: Yeah.

CHAIRMAN APOSTOLAKIS: Oh, you want to say something about it again?

MR. KURITZKY: Just move to the --

MR. CHU: Well, except maybe I'll talk about two simplified quantification method. One or the second one is already discussed. It's the standard quality cutset quantification. So if you have two failure in a sequence, we use mission time of one year for both of them, so it's conservative.

CHAIRMAN APOSTOLAKIS: Yes.

MR. CHU: The first quantification, I call it rare event approximation. Basically, we assume the failure modes in the sequence are the only failure modes. So there is no competing effects. The competing effects on other failure modes are ignored.

CHAIRMAN APOSTOLAKIS: What? I don't understand what that means. What do you mean by that?

MR. CHU: If you look at the earlier transition diagram, they want to find a probability of this state.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. CHU: In this state, failure mode one or Component 8 take place.

CHAIRMAN APOSTOLAKIS: Right.

MR. CHU: And no other failure mode occurred. So if you solve the equation for this state, you account for the success being that other failure modes never take place in this state, that reduce the probability of the state.

CHAIRMAN APOSTOLAKIS: Why is that an approximation? I mean, it's not an approximation.

MR. CHU: Well, because there is a competing effect. Say they think of -- there are only two failure modes, two transitions from this state. They are competing over each other in the sense -- say if the failure rate for the first one is very low, then chances are --

CHAIRMAN APOSTOLAKIS: Which one will occur first?

MR. CHU: First.

CHAIRMAN APOSTOLAKIS: So what you are saying is that you follow one path and you ignore all other paths?

MR. CHU: Right.

CHAIRMAN APOSTOLAKIS: Okay.

MR. CHU: Right. That's all. So you get a somewhat of a conservative result.

CHAIRMAN APOSTOLAKIS: So then, wait a minute, you are then -- I mean, as you said, you are calculating the probability of a state where order is important, right?

MR. CHU: Yes.

CHAIRMAN APOSTOLAKIS: But in terms of the whole system, can you still prioritize the failure modes according to their probability with this assumption?

MR. CHU: Yes. I don't see why not. I mean, we look at all the -- we identify all the singles, all the doubles and the triples.

CHAIRMAN APOSTOLAKIS: I don't know. I have to think about that, but maybe you are right. Okay. Keep going.

MR. CHU: Next, I think this was discussed.

CHAIRMAN APOSTOLAKIS: Yes, we discussed that.

MR. CHU: Out of 400 some single failure modes, 112 of them are system failure and they have a probability of .05.

MEMBER BLEY: Altogether?

MR. KURITZKY: Yes, altogether.

MR. CHU: Yes, altogether.

CHAIRMAN APOSTOLAKIS: That's pretty high, is it not, $5X10^{-2}$? That's a high number for PRA folks.

MR. CHU: But remember --

MEMBER BLEY: Not all of those failed the system.

MR. KURITZKY: Now, the .05 is the sum of those that do fail the system.

MEMBER BLEY: That do fail the system.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. KURITZKY: I mean, if you remember the slide we had early on we had a .08 as the total failure probability --

CHAIRMAN APOSTOLAKIS: Yeah.

MR. KURITZKY: -- failure frequency for the system. But in reality, that's actually only four automatic, loss of automatic. So, you know, there is operator recovery involved, too. And frequency for loss of digital feedwater system, loss of feedwater system is an initiating event. We are in that ballpark. I mean, it's not --

CHAIRMAN APOSTOLAKIS: But if this number means anything, how many years of experience do we have?

MR. CHU: Well, I think that --

CHAIRMAN APOSTOLAKIS: Reactor years.

MR. CHU: -- the digital feedwater control system probably has been operating since -- probably has been operating for like 10, 12 years.

MEMBER BLEY: Times the number of trains. Times the number of trains.

CHAIRMAN APOSTOLAKIS: And at how many

plants? Yeah.

MEMBER BLEY: So then all they are saying is once in 20 years on a single train you would expect to have to take manual control of it.

CHAIRMAN APOSTOLAKIS: Right.

MR. KURITZKY: Right.

MEMBER BLEY: It would be kicked in the manual controls.

CHAIRMAN APOSTOLAKIS: Do we have this kind of --

MEMBER BLEY: So we should have had some cases where people then kick in the manual.

MR. KURITZKY: And we actually even have cases where the plant tripped.

MEMBER BLEY: Because of it.

MR. KURITZKY: And they did take the manual control, right. So I mean, again, we don't have all the data. We don't have an inventory of which plants have which systems and for how long to do an actual calculation. But we did look at, as I mentioned earlier, that the data for the prototype plant, which is around 15 years of experience, and they had one actual trip of the system, a very small data sample.

CHAIRMAN APOSTOLAKIS: That is consistent.

Is that what you are saying, that the experience is consistent with this?

MR. KURITZKY: I think so, yeah.

MR. CHU: Yeah.

MR. KURITZKY: The very limited experience that we looked at.

MEMBER SIEBER: As compared to no trips with the analog system, right?

MR. KURITZKY: Is that the case? I don't know. Is that the case?

MEMBER SIEBER: Well, the only thing that can fail is the sensors and the sensors are the same regardless.

MR. KURITZKY: Yeah.

MEMBER SIEBER: Sensors and the operators.

MR. KURITZKY: In any case, so yeah. So I think that we have no reason to believe that this is inconsistent with operating experience. That's about all I can say.

CHAIRMAN APOSTOLAKIS: And the operating experience, I mean, one part of the operating experience is the number. The other part is how it happened. Is that hardware related?

MR. KURITZKY: Well, the one event that I mentioned was the shield, the improper shielding.

CHAIRMAN APOSTOLAKIS: This is it, yes.

MR. KURITZKY: The shielded cable, right.

DR. GUARRO: Which was totally different from what you are modeling here.

MEMBER SIEBER: That's right. But that's okay.

MR. KURITZKY: Well, I don't know whether or not when we stick in -- see the values that we have quantified here, we've gotten the so-called suspect data table that's in there, you know, the data that went into that table, I don't know what the source of events were for that data. An event just like this one may be in that table as one of those failure events. So I can't say whether or not that event is or is not part of this calculation.

MEMBER BLEY: I keep trying to think of which of your failure modes from Appendix B, which are what you are modeling --

MR. KURITZKY: Right. We never --

MEMBER BLEY: -- with that case.

MR. KURITZKY: Right.

CHAIRMAN APOSTOLAKIS: Right.

MEMBER BLEY: I read through it. I can't remember that there was one.

DR. GUARRO: It is not important. It was

built for --

CHAIRMAN APOSTOLAKIS: I think this will make much more sense to put it in the bigger study that I suggested there, because we always have this question. I mean, is it included? It's not included. Is it something else that's outside the scope? If you tried to put this whole thing together by identification of failure modes using this and something that deals with software, I mean, maybe talk about context, then I think things will become much, much clearer.

I'm surprised by the numbers you are getting, but, of course, it all depends on the inputs. .05, I mean, wow, that's pretty high, Sergio, isn't it?

DR. GUARRO: That's not for loss of feed though.

CHAIRMAN APOSTOLAKIS: No, but in terms of software failures, I mean, the logic I think the probability -- this probably dominates.

MEMBER SIEBER: It's pretty high.

CHAIRMAN APOSTOLAKIS: Yeah. Don't you agree, Sergio?

DR. GUARRO: Well, and if you look at, you know, should I also infer that in reality the total system is, you know, you've got sum of the single, double and triple.

MR. KURITZKY: Right. So there is --

DR. GUARRO: So it's like four times .05.

MR. KURITZKY: No, it's --

DR. GUARRO: Or .02.

MR. KURITZKY: .08. And the last column of that --

CHAIRMAN APOSTOLAKIS: The very last one is .08.

MR. CHU: This number is .08.

CHAIRMAN APOSTOLAKIS: They add these things up. Triple failures, including single you are saying?

MR. KURITZKY: Yes. The last column is cumulative.

DR. GUARRO: Yes, this is cumulative.

MEMBER BLEY: Oh, okay. All right. All right.

CHAIRMAN APOSTOLAKIS: Well, this is only for one loop?

MR. KURITZKY: Yes.

MEMBER BLEY: Yes.

MR. CHU: Yes.

MR. KURITZKY: Automatic.

CHAIRMAN APOSTOLAKIS: But there is two involved.

MR. CHU: The loops.

CHAIRMAN APOSTOLAKIS: Then it's this square? Is that what it is?

MR. KURITZKY: No, because they are not redundant loops.

MR. CHU: They are doubled.

MR. KURITZKY: I would double.

MEMBER SIEBER: Double.

MEMBER BLEY: Double.

CHAIRMAN APOSTOLAKIS: Oh, why? They're not redundant?

MR. KURITZKY: No.

DR. GUARRO: Because if either one -- no, no. They are two loops so either one --

(Multiple people speaking at once.)

MEMBER BLEY: And what they are calculating, you have to take the --

DR. GUARRO: Either one you have to --

MEMBER SIEBER: Of that, no one can understand.

MEMBER BLEY: That loop.

MR. KURITZKY: Right.

MEMBER BLEY: You can take manual control of one leg.

CHAIRMAN APOSTOLAKIS: So from the singles then it's .1, that's what you are saying if I consider both loops?

DR. GUARRO: 1 in 10.

CHAIRMAN APOSTOLAKIS: 1 in 10, wow.

MR. KURITZKY: For automatic, loss of automatic.

DR. GUARRO: And the total is like -- more like .2.

MR. KURITZKY: Now, again, this is preliminary results. This is -- when we do the -- come up with this next NUREG, we will have looked into the dominating contributors. You know, when you go to look -- when we go to the next presentation, you will see that table of numbers, which could get misused, but in there, there are going to be certain failure rates for certain components. And maybe one of those is dominating, because there is a particularly high failure rate for any particular component, which is showing up in this list of singles.

I don't know whether we have any insight on that at this point, but that could be one of the things driving it. But even so, at .1 for the two loops, it's not an outrageously -- it doesn't obviously look like it's inconsistent with operating experience. But if it's a little bit high or low, I can't say, but it's not totally inconsistent.

CHAIRMAN APOSTOLAKIS: Okay. What else do you have here?

MR. CHU: The next one will show comparison of, you know, quantification using different methods.

CHAIRMAN APOSTOLAKIS: Exact method? There is an exact method?

MR. CHU: It's exact solution of the Markov model, an analytical solution giving you that.

MR. KURITZKY: Excuse me, just in context, when Louis was showing that slide a couple slides ago where he talked about the rare approximation.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. KURITZKY: This is what he was talking about. So the exact method is using the Markov quantification whereas compared to just doing that mere approximation.

CHAIRMAN APOSTOLAKIS: Well, that's a pretty significant difference, right, 50 percent?

MR. KURITZKY: Yes.

MR. CHU: Yes. And the fault tree method in general is just too conservative. And it happen to be relatively close, because single failure dominates. In case of single failure the fault tree quantification is pretty good. But if you have a system with high redundancy, then the error of the fault tree cause will be much higher.

MR. KURITZKY: Well, may be. We will have to wait and see how it is going to come out.

CHAIRMAN APOSTOLAKIS: All right. So are you ready to move on to the estimation?

MR. CHU: I just want to say a little more about quantification. Using our model, we're also doing some sensitivity calculations. We are calculating what's the benefit of having redundance. There is the specific calculation removed backup CPU. And we calculate another sensitivity calculation to see what's the benefit of the watchdog timer. Again, we go into the model, remove the credit from the watchdog timer and see what we get.

Another example we look at outer range check that is within the software it does some kind of outer range check of the input data and it handles that accordingly. And we take away that feature and see how the bottom line number changes. So in that sense, you know, developing this model can -- you can use to do certain evaluations.

MEMBER BLEY: I'm a little -- I didn't see all the details. When you include the watchdog circuit in your analysis, are you putting both its main purpose in responding to a timing problem and the chance that it shuts off the system when it shouldn't? I think that's what this is, right? It's a failure in the watchdog, which turns off the automatic system?

MR. CHU: It's both, yes.

MEMBER BLEY: So you have both?

MR. CHU: Yes.

MEMBER BLEY: You have both of them in there?

MR. CHU: Yes. But our model of the watchdog timer is -- let me explain that. That has -- it's hard -- basically, the watchdog timer periodically receives signal from the CPU.

MEMBER BLEY: Right.

MR. CHU: But it's operation, we are not able to really simulate it. The way we model it is that when we look at the individual failure modes, based on our judgment in determining -- given this failure mode, is going to crash the system. Then it should be detected by the watchdog timer. Then in the simulation tool for this particular failure mode, it just simulate the effect that the watchdog timer detected the crash and proceed forward.

And in other cases certain failure mode happens, in our judgement, it will not be detected by the watchdog timer, then simulated accordingly. So it's more of right out of our judgment, based on our understanding of the data mode.

MEMBER BLEY: Okay.

MR. CHU: So that's kind of, you know, a limitation of it. Really, that's all I --

CHAIRMAN APOSTOLAKIS: Keep going.

MR. CHU: On to the next.

CHAIRMAN APOSTOLAKIS: Whenever we adjourn again.

MR. CHU: Okay. Outline of the presentation, basically, I'll try to describe the failure parameters that we need in our model and where we get the numbers from. We look at some available sources of failure parameters. And in one case, we performed hierarchical Bayesian analysis on raw data. This is a piece of work that kind of represents our more original work. In other situations, we, basically, take the failure of parameter from whatever sources we were able to find.

CHAIRMAN APOSTOLAKIS: Without evaluating the credibility of those sources?

MR. CHU: Right. I would say yes.

CHAIRMAN APOSTOLAKIS: Why?

MR. CHU: But the sources are -- these are the only source we can get our hands on.

CHAIRMAN APOSTOLAKIS: Well, there is also an answer that there is nothing available that we can use.

MR. CHU: There might be -- I think the vendors' manufacturers tend to claim they have data.

CHAIRMAN APOSTOLAKIS: Oh, I can claim a lot of things myself. Now, this is -- you know, we have to have convincing evidence of --

MR. CHU: Yeah, therefore, you can't say this is the best available.

CHAIRMAN APOSTOLAKIS: I mean, the stuff you describe in your report that some well-known organizations have done is just incredible to me. 1,000 lines of code. My God.

MR. CHU: That's on software.

CHAIRMAN APOSTOLAKIS: Don't -- I don't know. There is a general reluctance on the part of people to say there is nothing out there I can use. They feel that they have to put it in where, you know, what's his name, Rick Arndit? Sergio probably knows.

DR. GUARRO: The Roman bandit.

CHAIRMAN APOSTOLAKIS: Oh, it will come. Keep going.

MR. CHU: Yeah. In case -- the data I will look, we actually have more description, so kind of in that sense there is some sense of the quality of this data. And I will talk a little bit about issues associated with failure.

CHAIRMAN APOSTOLAKIS: A little bit about issues, no.

MR. CHU: There are issues.

CHAIRMAN APOSTOLAKIS: A long list. All right.

MR. CHU: Well, this slide gives you an overview of all the failure data that we use.

CHAIRMAN APOSTOLAKIS: So this is from where?

MR. CHU: This is a database developed by the Reliability Analysis Center. It's based on --

CHAIRMAN APOSTOLAKIS: Who is running that center? Whose center is it?

DR. GUARRO: Well, I --

MR. CHU: It's the Department of Defense. They are -- I guess they are probably contractor of Department of Defense.

MEMBER BLEY: Probably under the

Automotive Handbook.

DR. GUARRO: Well, actually, what it is is, you know, the Automotive Handbook 217 was produced in Rome or developed and sent to Reliability Analysis Center. It was officially banded with the Acquisition Reform Initiative of infamous Darlene Drulian.

CHAIRMAN APOSTOLAKIS: After how many years of use?

DR. GUARRO: Seven years of use. But it has been discontinued. The last update of 217 came out in 1992. Okay. So it's totally out dated. The organization that was contracting to DoD, essentially, was an FFRDC, who tried to continue to maintain these, but I think the way they had been able to do it was, essentially, introducing process factors to modify. I don't think there has been a real sustained -- at least that's to my knowledge, because we were looking at that for application in the space systems, not a real continuation of the data collection at work, because there was simply no funding for that.

So they have introduced factors based, essentially, on expert opinion and so forth to modify the old rates and modernize the database. But the database really has not been updated since way back then. That's my understanding of it.

CHAIRMAN APOSTOLAKIS: I don't remember whether it is your report or another report, but I remember seeing statements that affect the applicable, you know, or data produced by one system of not transferring to another system. Are you guys saying that or somebody else said that? That for digital systems --

MR. MARTINEZ-GURIDI: Again, that's for software.

CHAIRMAN APOSTOLAKIS: So I don't know that, I mean, you can go to such generic sources for two reasons. One is we really don't know the basis of the numbers we have. And second, why are -- would these numbers apply to a nuclear plant?

MR. CHU: Yes, the data that we use are actually raw data in form of, you know, number of failures and number of --

CHAIRMAN APOSTOLAKIS: Oh, you found those?

MR. CHU: But their applicability to nuclear plant certain is a question. You know, maybe they were outdated data.

CHAIRMAN APOSTOLAKIS: I am --

DR. GUARRO: The original 217 data was mostly from the automotive industry. And then 217 had all the --

CHAIRMAN APOSTOLAKIS: Strict review criteria, right?

DR. GUARRO: They had all this environmental factors that were added on to transform it into other environments, okay, and those factors --

MEMBER BLEY: Are suspect.

DR. GUARRO: -- are very suspect. Because when you ask how did you get them, it's kind of oh, tradition and, you know.

CHAIRMAN APOSTOLAKIS: So the data, when we were reviewing the Shuttle PRA, there was information like that. That so many failures were observed in so many trials, but that's it. No more information about what is failure, what is --

MEMBER BLEY: Exactly. That's the part.

CHAIRMAN APOSTOLAKIS: Yeah.

MEMBER BLEY: But there is no access to the descriptive things on which these data are based.

CHAIRMAN APOSTOLAKIS: So that immediately makes that case.

DR. GUARRO: You know, one has to agree with Louis' statement that that's the only stuff that exists that's publicly accessible, but whether the fact it exists justifies --

CHAIRMAN APOSTOLAKIS: Yes.

DR. GUARRO: -- giving a lot of credit, I don't know.

CHAIRMAN APOSTOLAKIS: Okay. Keep going, Louis.

MR. CHU: Okay. So in some cases, we extracted raw data from PRISM and did our phasing analysis. In other cases, there wasn't raw data and the -- in most cases used the PRISM method to come up with a data rate as to it.

CHAIRMAN APOSTOLAKIS: Now, does PRISM itself use hierarchical Bayesian or no?

MR. CHU: No.

CHAIRMAN APOSTOLAKIS: You are using it?

MR. CHU: Right. The principle of their approach is that they just don't account for uncertainty. They give you a point estimate. At one point, I remember asking them what was certainty? They said the uncertainty is so large they cannot consider it.

CHAIRMAN APOSTOLAKIS: Yes. It's not --

DR. GUARRO: Yes, I can vouch for that, because I asked exactly the same question back in 1995 or so to these people and I got exactly that answer. So that's what they say.

CHAIRMAN APOSTOLAKIS: But can you describe briefly what you do with the hierarchical Bayesian?

MR. CHU: Yes, I'm coming to that.

CHAIRMAN APOSTOLAKIS: You're coming to it.

MR. CHU: This is just an overview.

CHAIRMAN APOSTOLAKIS: So your third bullet it seems to me you're going to find yourself in the same situation I found myself with the short circuits.

MR. CHU: Yes, this is --

CHAIRMAN APOSTOLAKIS: A few years from now, somebody is going to come back and say common-cause failure is .05. We say great, who gave you that?

MR. CHU: But --

MR. KURITZKY: It was at an ACRS meeting in 2008.

CHAIRMAN APOSTOLAKIS: Whoa, whoa.

MR. CHU: The ALWR.

CHAIRMAN APOSTOLAKIS: Huh?

MR. CHU: ALWR utility requirement document, this is an industry document.

CHAIRMAN APOSTOLAKIS: Oh, and that's a

great source of that.

MR. CHU: They say they pick a number.

CHAIRMAN APOSTOLAKIS: I don't doubt it.

MR. CHU: But in general, we recognize, you know, there is no real --

CHAIRMAN APOSTOLAKIS: You recognize it, Louis, but you remember the discussion earlier. I mean, once the NUREG is out, it's NUREG.

MEMBER BLEY: The report doesn't quite recognize it, I think, but I'm not sure the report makes that clear.

CHAIRMAN APOSTOLAKIS: Oh, the caveat is there.

MEMBER BLEY: Not in the one you are looking at. The next one.

CHAIRMAN APOSTOLAKIS: Oh, okay.

MR. CHU: You understand?

CHAIRMAN APOSTOLAKIS: How many forms of this report are there? There is a current version.

MR. KURITZKY: Let me, if I could, Dr. Apostolakis, clarify that, because we had some confusion earlier. There was a draft version of the report that we supplied to the Subcommittee back in, I think, October of last year. We had a -- after it went out for comments, we have a draft final that BNL incorporated the comments and submitted to us a few months ago. Okay.

MEMBER SIEBER: March 18.

MR. KURITZKY: And that -- what's that?

MEMBER SIEBER: We got it March 18^{th}.

MR. KURITZKY: March 18^{th}, okay. But that version which we would then supply -- we got it in and we actually started making some changes to it. Okay. That modified version is what you have. Actually, you have the one that BNL submitted in. Then since that time, we started incorporating internal review for some additional management, with the management reviewing and some other comments that have got put in later.

That version is the one you don't have. So when -- and that's going to be what is going to be, essentially, the final version. Okay. So you have a version that is beyond the draft, it's close to what the final version will be, but not exactly the final version. And I think that Christina has the version that is almost the final version. It's in between the one you have and what's going to be the final, just because she wanted to have what we had at that day and time. But I called her and she recognized that it's not the final, so I tried to --

CHAIRMAN APOSTOLAKIS: Are you going to modify it or revise it as a result of today's discussion?

MR. KURITZKY: Originally, we were not going to make any changes, because it was supposed to actually be in publication by now. Because this schedule has been pushed off by a couple of weeks, we have an opportunity to make some changes to it. So we are going to try and take some of the feedback and things that we can work in in the short-term we will try and incorporate.

CHAIRMAN APOSTOLAKIS: Is that a plan to have a full Committee briefing on this, Christina?

MS. ANTONESCU: I'm not sure.

CHAIRMAN APOSTOLAKIS: Do you guys know that?

MR. SHUKLA: I found out about it an hour ago. It's on Thursday, May 8 from 1:30 to 3:30.

CHAIRMAN APOSTOLAKIS: Two hours, wow. When is this, May what?

MR. SHUKLA: 8th.

MEMBER SIEBER: Be there.

MR. SHUKLA: And Christina will give you all the information.

MEMBER SIEBER: When will we get the final version of the NUREG?

CHAIRMAN APOSTOLAKIS: Yeah, we should have the very -- what you consider final.

MR. KURITZKY: Right. When it's final, you know.

CHAIRMAN APOSTOLAKIS: But don't worry, I wouldn't go -- I wouldn't rush and publish it.

MEMBER SIEBER: Appreciate that.

CHAIRMAN APOSTOLAKIS: Before the meeting. They will still publish it independently with a letter because this is a NUREG report. That's not a very good idea.

MR. KURITZKY: In the last presentation for a few minutes I discussed interactions. I'm going to go over the schedule to publish opportunities to incorporate it.

CHAIRMAN APOSTOLAKIS: Good. Let's let Louis complete.

MR. CHU: Regarding modeling software failure in our model we do have high level of software failure modes. I'll explain a little bit. Earlier you questioned if we made use of what is in Appendix C. In Appendix we have developed some high-level software failure modes.

CHAIRMAN APOSTOLAKIS: Appendix C?

MR. CHU: Right. There we have some high-level software failure modes and separate causes. In our modeling we have two kind of software failure modes included in our model. In one case it's a software halt. Basically the system crash. This kind of failure can be detected by the botchel type so that is how it is modeled.

In the other case we say software is running but it's just not generating the right answer. This is a failure mode that goes undetected and, as a result, it's going to lead to a system failure. This kind we modeled.

CHAIRMAN APOSTOLAKIS: Again, you are going to use failure rates for these kinds of very specific failure modes that's running but is not detected?

MR. CHU: High-level failure modes that seem reasonable to include.

CHAIRMAN APOSTOLAKIS: But did you put rates?

MR. CHU: We use 10 to the minus 8 per hour.

CHAIRMAN APOSTOLAKIS: That's right. Sources of failure perhaps.

MR. CHU: Liability prediction method is

the main publicly available data sources, military handbook, Telcordia, and PRISM. We make pretty extensive use of the PRISM database.

CHAIRMAN APOSTOLAKIS: Which is suspect to begin with. Right? Is that right, Sergio?

DR. GUARRO: I would say so, yes.

MR. KURITZKY: Unfortunately it's what we have available in the public domain.

CHAIRMAN APOSTOLAKIS: No, but the point is you could actually say we don't use any of this

MEMBER BLEY: We are just exercising the model with failure numbers.

CHAIRMAN APOSTOLAKIS: And focus on the failure mode identification. Then the next guide will cover a series of bullets like this and the last bullet will be NUREG/CR such and such.

MR. CHU: Other sources of failure data, LER and COMPSIS. LER document U.S. operating experience is not designed to be used for failure. Especially in the case of digital component or system it's hard to find out how many of the same components or systems are in operation. The same issue applies to COMPSIS which is an international effort in sharing operating experience.

It's only at an early stage of collecting nuclear experience. We have come across some technical paper and technical report that performs a serious study and contains some kind of estimate of digital components. This slide talk about the failure prediction methods.

CHAIRMAN APOSTOLAKIS: Would you say then that your numbers are basically your judgment as shaped by what you saw in the literature of various sources? That's what you say in the first bullet, modified by pi factor.

MR. CHU: That is the reliability prediction method. If we have raw data from PRISM and we use the raw data.

CHAIRMAN APOSTOLAKIS: Without modification?

MR. CHU: Without modification.

CHAIRMAN APOSTOLAKIS: I asked you earlier about the Hierarchical Bayesian. Did you actually tell us what you did?

MR. CHU: Yes. It's pretty much the same as two bases analysis.

MR. KURITZKY: The next slide is going to hit it.

CHAIRMAN APOSTOLAKIS: Okay.

MR. MARTINEZ-GURIDI: My understanding is that the data were not modified using this pi factor but rather they were updated using the Hierarchical Bayesian method.

MR. CHU: Some criticism of the military handbook. I think there is a professor of University of Maryland who published quite a few papers criticizing the accuracy.

CHAIRMAN APOSTOLAKIS: Yes.

MR. CHU: Also, of course, they don't have treatment of uncertainties.

A little bit about the PRISM database. It has two methods for estimating failure rates. RACData is a more traditional pi factor method and it contains raw data. It is this raw data that we use in our basing analysis. Then they also have --

MEMBER BLEY: And this kind of raw data is just counts. Right? It's no underlying information.

CHAIRMAN APOSTOLAKIS: That's correct.

MR. CHU: Right. Right. It's the explanation of what failure means.

MEMBER BLEY: X failures and Y trials.

CHAIRMAN APOSTOLAKIS: And numbers on the order of 10 to the minus 8 per hour. What is the best way to present what you have done? I mean, is it to say -- first of all, why did you need several weeks to limit?

No, you don't. You look at single failures, double failures, triple failures. You can say it makes sense but a triple failure is less likely than a single failure. You may have underlying causes but overall that is a reasonable thing to say so I don't need probabilities there.

I'm just invoking a qualitative argument. You can still do everything you have done, everything, with the failure modes and identification of these things that you showed us, blah, blah, blah, done. You're done and you don't need anybody's failure rates. Then you have a second stage where you start now doing these exercises. My view is that you should separate the two completely.

Make it clear that one can do the failure mode work without any reliance on these reliability rates. Then the second one personally I wouldn't present at all. If you want to present it, make sure you put all these qualifiers up front but I really think it's going to be misused and it doesn't deserve to be in the NUREG.

Now, the calculation of stuff that you did with the Markov, I think that's interesting to put there to have a record. Somebody else might use it. But then when you start putting numbers in, I don't know, you need boldface letters or something. This is not an exercise in fatigue.

Let me repeat, you are not responsible for the state-of-the-art. You are not responsible. Nobody is forcing you to come up with numbers. The state-of-the-art is such that the numbers are not credible. Don't take it until you fail. It's not your responsibility to come up with numbers no matter what.

MR. KURITZKY: I think the issue here is that we are not looking to come up with numbers. What this study is doing is not trying to come up with a value for the failure of automatic control of the digital feedwater control system. What we are trying to do is demonstrate the methods and see where the weaknesses are.

We recognize that the data we are throwing in is not the data that someone should use. In fact, in our criteria we say you should use specific data for your system. We don't have that data. We are just demonstrating what the process is. If someone wants to use this process, they should be using the appropriate data.

The method of using HBM is such that if the applicant or whoever is going to use this method does not have beautiful data to stick in that they would want to use some method such as this to account for uncertainty. We would not necessarily want them to use that arbitrary data we pick but whatever data they do use, we still may think it's appropriate to use something like HBM to account for it.

CHAIRMAN APOSTOLAKIS: HBM is what now?

MR. KURITZKY: Hierarchical Bayesian Method.

CHAIRMAN APOSTOLAKIS: I would separate that and maybe present it at the conference. It's really very different from the rest of the report. I think the way I understand it now, the way we are going there will be a major effort on the identification of failure modes. Not just by you. I don't know but we are going to recommend it to the commission.

Failure modes, failure modes. Let's understand it. Let's have an integrated approach. I think you are contributing to it. That is a stand-alone document. Your Markov stuff you may or may not want to include in the same report, or maybe you do because it's an interesting exercise without numbers.

The last part that you do with this I think is a very risky proposition because it's going to be abused. It weakens the report. It weakens it and takes away from the quality of the report, I think. Naturally people will focus on this, I mean, unless somebody else has a different view.

I mean, we are perpetuating this business of numbers. We are taking them from somebody else and say, "It's all very good but this is what it is." Then the next guy reads it in NUREG and, therefore, you know.

MEMBER BLEY: I guess I would go just a little further. This is going back to search through places in the report. There are sentences and paragraphs in the report that make it sound like this is pretty darn good data and takes care of the stresses and other things that are important. I don't remember any caveats and in a quick search I don't see any.

MR. KURITZKY: In the PRISM data, you mean?

MEMBER BLEY: Yeah. And some of the others fall in there, too, but PRISM crops up most often.

MR. CHEOK: I think those are fair

comments and we will take them under serious consideration and we will certainly think about them.

CHAIRMAN APOSTOLAKIS: You are not responsible for the state-of-the-art. Don't feel that it is bad to say that there are no numbers.

MEMBER BLEY: But you could be if this comes out.

CHAIRMAN APOSTOLAKIS: Yes. Okay, Louis. Oh, this is an example of the Hierarchical. Yeah, good.

MR. CHU: It is desirable to assess the uncertainty of failure parameters. Therefore, since we were able to extract the raw data from the PRISM database, we used the extracted data with the Hierarchical Bayesian Method. This basically accounts for the variability of data sources since the data came from a variety of sources.

CHAIRMAN APOSTOLAKIS: I see what you're getting at. But there is an assumption here that all the sources are equally present. Right? In a plant-to-plant variability in reactors, yes, they are. It's just different data. In this case I think the credibility of each source is a very important consideration.

MR. CHU: There is information about the

source of data. For example, one source just might say warranty data from a certain manufacturer. Later I have a slide showing an example of data extracted from PRISM.

CHAIRMAN APOSTOLAKIS: The purpose of this Hierarchical Bayesian was really to deal with the issue of source-to-source variability, plant-to-plant variability. Even that you believe the information you get from each plan. For the nuclear application it made perfect sense, but here we have a bigger problem than before. We just don't trust the data. Again, having a method like this out in the literature may give people the wrong impression that because it sounds sophisticated we do have something that is believable.

DR. GUARRO: I'll just make an observation that you may take or leave here because I don't know if it applies. You are using this to construct a prior. Right?

CHAIRMAN APOSTOLAKIS: Yes.

DR. GUARRO: There was some work that we did years ago for spacecraft risk assessment. We had the issue of different sources and different applicability. We thought that it was applicable but not applicable in the same way. We used what is now known as the weighted likelihood way of combining the data. Perhaps you could address George's situation in terms of credibility of the data and explore something like that. It's just a suggestion.

MR. CHU: We have no information to judge.

CHAIRMAN APOSTOLAKIS: What do you really think, Louis? Come on. How much do you believe this?

MR. CHU: Well, we come up with a distribution that is --

CHAIRMAN APOSTOLAKIS: No, no, no, no. Not your analysis, your original inputs.

MR. CHU: I don't know. It's what happened in the --

CHAIRMAN APOSTOLAKIS: You're taking the easy way out. You are taking the easy way out. Keep going.

MR. KURITZKY: First let me say because I think this is an important issue and after this meeting as we consider on the completion of the report and finalizing it, as Mike Cheok mentioned, we will take into serious consideration the comments we received.

One thing, though, and I'm not trying to defend the data because I think we all recognize that we are just using this as placeholder data because that is what's there and we want to make sure it's not misused regardless. We are looking at the scope of this work, the objective of this work is to explore the capabilities and limitations of using the current methods to model these systems and quantify them.

Okay. It's kind of incumbent on us to see where that state of quantification exist. We recognize all this ourselves and, as has been reinforced by the comments today, the state of quantification is not good. That is probably an understatement but the idea being we don't want to go out and say to people in the absence of better numbers just use these in the meantime.

That is not our intention. Our intention is to go through this exercise to see where there are problems. The argument could be made that you don't need to actually stick in arbitrary numbers to know that --

CHAIRMAN APOSTOLAKIS: But what problems have you identified? You haven't identified any problem. What problems? You just found a number for the probability of automatic control failure. So what? People don't have to see that. I don't see what insights you are gaining by using numbers that are worth announcing to the world that you wouldn't get by dropping the whole subject.

MR. KURITZKY: That's my point. I don't think I would go so much as dropping the subject. I think the report needs to look into the estimation parameters. That's part of our scope. What we may want to do is say not published numbers. Say we looked for numbers and we couldn't find any numbers that were of real value and, therefore, our conclusion is that the state-of-the-art --

CHAIRMAN APOSTOLAKIS: As long as you are criticizing the existing databases that's fine with me but the moment you start saying, "Now I'm going to assume .05 for the failure rate," and all that, that's not okay.

MEMBER BONACA: I think the report makes the point to the weakness of the data. I think you can make it in a harsher tone, too, by saying that just simply -- I mean, when you read it through, in fact, you look to the same villains all the time, LERs. We know what you get from the LERs. You get very selective information or other pieces of information or sources. As long as you communicate, as you did, I think, the limitations of the databases, that's fine.

MEMBER BLEY: I guess I didn't read it the same way. I've just been re-reading Chapter 8 while we sit here and I would urge you guys to go back and re-read Chapter 8 as if you are seeing it fresh. Mostly it's saying positive things about the sources of data that are being mixed together and it's identifying what is good. I don't see much here identifying what's bad.

MEMBER BONACA: I guess I read it differently in the sense that I know enough about some of the sources of data.

MEMBER BLEY: Yeah. I think that's the way I read it the first time, too.

CHAIRMAN APOSTOLAKIS: Alan says they have to address the issue of estimation. I think it makes perfect sense to critique the existing sources. Take into account what Dennis just said and Mario and maybe change your language here and there and then stop. You don't have to go and say, "Now I would assume this number and I will assume that number." I think that is perfectly acceptable.

MEMBER BONACA: One thing is this information was not collected with the intent of using it for the uses we are trying to make here. It was for traditional systems in a way. That's a fact. That's the past.

The question in my mind what are we going to do about modifying some of the collection systems that we have today to make them more amenable to support, in fact, this kind of simulation. You need to have information from an LER about the performance of the digital system and you don't get it the way it's being written today. What are we going to do?

CHAIRMAN APOSTOLAKIS: I would go back to my comment this morning that we really need this quotation, philosophical stuff. What role should probably be displayed in this field? We are going with the standard assumption that the way we have been doing it here applies here as well and I think it doesn't.

What exactly -- I mean, if we are to use probabilities here, what is their proper utilization? Sergio mentioned one possibility. I mentioned another possibility. Some smart guys sit down and think about it and debate it for a while. In six months they can have a nice piece of work that says, "In the context of digital INC, this is what we believe makes sense to talk about probabilities." There is a fundamental problem. It's very different from what we have been doing in the last 30 years. Very different.

MEMBER BONACA: Again, I would like to --

CHAIRMAN APOSTOLAKIS: You are talking about design errors. Where do we account for design errors in the standard PRA? We don't.

MEMBER BONACA: I would like to complete my thought process before --

CHAIRMAN APOSTOLAKIS: Yes.

MEMBER BONACA: Somewhere in this report there has to be some statement about the expectations that you would have for the EPIX system, some of the systems out there, the kind of information that needs to be provided to support this work. There is nowhere a statement that says that something has to be done about this collection of databases.

Yet, I think unless we have the industry in some way start a different kind of way of selecting that information, etc., they are going to go beyond this kind of information. They will consider the databases to be inadequate.

CHAIRMAN APOSTOLAKIS: I think even that will require some prior thinking along the lines I just described. If I am after this kind of probability, then what kind of information would I need?

MEMBER BONACA: I agree with that. I'm

talking about the opportunity to make a choice.

CHAIRMAN APOSTOLAKIS: I mean, you have a chance here to make an impact and that is what we are trying to do, even at the expense of delaying the publication. Really you need to do that. I mean, this idea of rates of transition and this and that I get confused every time. Somebody has to put the issue at rest.

I have other comments in the ACRS letter two or three years ago hoping that would instigate something like this but I guess it didn't happen. I ask questions. People have to ask themselves what does a rate mean and so on and it didn't happen. All right?

So now we go to Alan or are you done or what? I think we pretty much understand what you did.

MR. CHU: Okay. I'll show you an example of the data we extracted.

CHAIRMAN APOSTOLAKIS: Okay. That is slide what?

MR. CHU: Nine. This is the kind of information we have. Each row represent one source of data. In the first case they had 12 failures in 633 million hours.

CHAIRMAN APOSTOLAKIS: What component are you talking about here? It says Quality, Environment, Number of Failures. What component?

MR. CHU: Those are the terminology used within PRISM. Quality means when it's for commercial application or military application representing different requirements, different design requirements.

MR. MARTINEZ-GURIDI: It's the same component with different sources of data for the same component.

MR. CHU: This is data from memory from different sources. GB means ground benign. AIF means airborne inhabited fighter.

CHAIRMAN APOSTOLAKIS: The numbers range from 1.4 to 1.210 to the minus 3, three orders of magnitude. So if I said without looking at this based on my experience it's between 1 and 10 to the minus 5, I probably would be right.

MEMBER BONACA: But you're sure you captured the uncertainty?

CHAIRMAN APOSTOLAKIS: I am sure, yes.

MR. CHU: The next slide shows the result. One way of looking at it is look at the error factor obtained.

CHAIRMAN APOSTOLAKIS: Obtained from where, from these sources? Oh, the Hierarchical

Bayesian Analysis.

MEMBER BLEY: What did you start with in the Bayesian Analysis as the underlying fire before you mixed all these databases, some kind of noninformative grid?

MR. CHU: We assume it is lognormal with the parameters uniform.

MEMBER BLEY: Uniform.

MR. CHU: Actually, there is some sensitivity calculations like using gamma distributions or some different type of fires. We eventually still end up with lognormal and uniform. We actually recognize there is an issue with the gamma distribution. It was shown by Hofer that in Bayesian Analysis that likelihood function is unbounded.

That is, when you implement numerical you always have to truncate. Therefore, you miss things. The implication is that people who have been assuming gamma distribution and perform this kind of analysis you can question the validity of the results.

DR. GUARRO: I think we can go back to the more fundamental issue. I don't think mathematical issues with the gamma are the problem here. Look at the processing unit and add a factor of 339. That means, you know --

MEMBER BLEY: We have that stuff Louis showed before we don't know where it came from.

DR. GUARRO: If we mention the whole universe.

CHAIRMAN APOSTOLAKIS: I remember when we started dealing with this issue several years ago and the staff came, I think it was NRR, and they said in preparing for digital INC they visited organizations like Boeing and other places where digital had been used. One common message they got from all the organizations was do not pay any attention to the variability models.

It was a flat statement dismissing everything. There was a reason for that, I think. The real designers and the real users just couldn't see how these models would be helpful in any way. I think we are making progress here in the failure modes. I think that is very important. Since you managed to get them without really using any numbers, that's great. That's really great. Let's emphasize the positive part of your work and de-emphasize the negative.

Okay. So are we going to Alan now?

MR. CHU: There is a little more, failure mode distributions. That is, when you have failure rates estimated. In our model we don't just look at failure rate but we break it down into different failure modes.

For example, in the case of the microprocessor it has two failure modes normally running but sending incorrect results and it stop sending outputs so we have to break down the failure rates into the contributors. There are two sources that we used to estimate this breakdown. The first one is published by the Reliability Analysis Center. The second one is a book by Meeldijk.

In some cases we have to make some kind of judgment and the component we are interested in may not be exactly in these sources so we make some interpretation of using the failure distribution.

MR. KURITZKY: Okay, Louis. Before you start this slide, I think I want to emphasize that because -- particularly because of the feedback we are receiving today and the intention to de-emphasize the quantification or the estimation of the parameters, this particular -- the next slide that Louis is going to talk about I think this is one that we would definitely be looking for feedback from the subcommittee right now because this has got to play a more prominent role in the report. If we are no longer going to have quantification I'm not coming to that but that is what we are considering.

CHAIRMAN APOSTOLAKIS: That is legitimate.

MR. KURITZKY: We are going to have to lay out exactly why we feel that we are not in a position right now to be able to quantify so this is some of the ideas that we have come up with as things where there are issues with trying to quantify. I think we would be well served if we could get as much --

CHAIRMAN APOSTOLAKIS: I believe the main issue is all these databases they do not provide a technical basis of whatever they are giving you. Something that will convince the reader that there is some connection to reality, some connection to experience, some connection to something that will give credibility to these numbers. That is my main problem with it.

Sergio.

DR. GUARRO: Yeah. The lack of real traceability to the source of the data from today to when the origin because these are numbers that were dug up 20 years ago and then massaged and modified, etc. The history is not there so you don't know what you are dealing with.

I think anybody knows that between a

microprocessor today and a microprocessor from 1980 something, which the data was probably collected in 1992, you know, it probably referred to something before. We are looking at something 30 years ago. The technology has gone light years ahead in those 30 years so what is the applicability of that data?

Also, in terms of feedback, I think, Alan, you can look at the result of your own assessment to make a judgment. When you start looking at those error factors, it is your own analysis that tells you that the probability is so large that essentially the data means nothing. I mean, an error factor of 140, 300. Even the smaller factors here are big.

CHAIRMAN APOSTOLAKIS: That could be an argument.

DR. GUARRO: It is an argument. We did an analysis and we looked at the variability. The variability is so large that the data cannot be used. That is what I would say.

MEMBER BLEY: But the data must not have been collected on the same things we're looking for and the same environment.

DR. GUARRO: These are cats and dogs thrown together.

CHAIRMAN APOSTOLAKIS: Make sure that you don't say that the uncertainty is large so we don't use it because we can deal with large uncertainty but this is different. This is so large in the source-to-source variability so it creates this suspicion.

MEMBER SIEBER: That we don't believe it.

CHAIRMAN APOSTOLAKIS: They are not dealing with the same components. I think that is a very --

PARTICIPANT: Or even the same failure mode.

CHAIRMAN APOSTOLAKIS: We just found some use for your Hierarchical Bayesian. Those numbers are a justification of the conclusion. Once you go over this threshold that I'm not responsible for the lack of numbers, then it's easy to write.

MR. KURITZKY: One thing also you should keep in mind, though, clearly the numbers that we had to use out of the public domain have great variability and we have no traceable basis for them. However, we are trying to talk about a process and an applicant, someone who works for a manufacturer, a vendor, may have extensive data on their particular system. The idea of quantification, I mean, we can't take that step maybe in a generic sense but it doesn't mean that someone else may not be able to do the quantification if they have the data.

CHAIRMAN APOSTOLAKIS: I don't think we said anything that would discourage an organization like that to come forward with this kind of data. We haven't said anything. What we are saying is that the data sources we have looked at don't convince us.

MEMBER BLEY: And your own principles up front say the data need to be applicable to the things you --

MR. KURITZKY: Right, right. That's the way we want to couch it is that we would couch it not that the state-of-the-art doesn't support doing quantification right now necessarily. There is no generically or publicly available data that we can use right now but we don't want to rule out the fact that someone else may have data.

DR. GUARRO: That's true but this will also underline the fact that someone else will have the burden of proof to show that data is valid because you clearly say what is publicly available is not really useful. In fact, it's not useful at all. I think we can go even that far so don't grab some number from a lot of these databases and come and tell me that is the reliability. If you have something better, show that it is better.

CHAIRMAN APOSTOLAKIS: You are sending a very explicit message as to what we did and why. The language here is extremely important and I think you should go back to the report, the main body of it. As I was reading it I had a lot of notes, "Wow, how did you get this? Where is this coming from?" I think you got the message. I think Dennis was right. You tend to be more positive than you intended to be.

MEMBER BLEY: And I think you will see that if you go back and read it again, especially Chapter 8.

MR. CHU: Since we have this model and we have quantified that, we are just demonstrating the method. We are putting a lot of qualifiers saying the numbers are not good but the --

CHAIRMAN APOSTOLAKIS: You don't need to quantify anything. I think your model --

MR. CHEOK: We will discuss that after this meeting.

MR. KURITZKY: We understand the subcommittee feedback and we will make a decision as to what --

CHAIRMAN APOSTOLAKIS: You don't have to give any numbers. The numbers are the third part which is different.

MEMBER SIEBER: You could use variable names just to show the methods.

CHAIRMAN APOSTOLAKIS: Yeah, put it down there. Somebody may take it and improve it because I believe in the foreseeable future the regulatory decisions will be really within the traditional defense and diversity, but to risk inform this is something way into the future.

All right. You still want to show something?c

MR. CHU: Just this bullet. I think you touched upon probably most of the other bullets. In looking at the PRISM database and PRISM data we came to the thought that when something like PRISM give you a failure rate, some other feature quite likely has started building in the failure rate estimate. Therefore, when you develop a model you don't want to credit that feature again. Otherwise you will be in trouble. In general, the failure parameter is an area that a lot more effort is needed with applicable data.

MR. KURITZKY: Okay, next slide. I guess here, too, because of the discussion we just had, it would be good to have an idea. We had picked up some candidates for further research in this area based on our work. Based on the opinions and feelings of the members here where do you think would be the most promising candidates for further research in the area of data? Or is this something that should be left to the applicant to deal with and it shouldn't be something the NRC take on?

CHAIRMAN APOSTOLAKIS: I wouldn't do anything on data until this philosophical study is done but I know what I'm after. You don't look for data if you don't have a model in your mind. You guys do that and come back and say, "Here is where we believe probability might play a role and these kinds of probabilities will be needed." Then you will decide how to get them.

Although the guys who will say it will also have to think a little bit about the feasibility of getting some data regarding this. I really think it is an important step to think hard about how much of this can be risk informed and what probabilities can be usefully used. As I say, I don't think it will be more than six to nine months to do this. There is already in the literature the subcommittee will be happy to meet with whoever is doing it even at the beginning to throw out some ideas and take it from there.

Sergio's comment, for example, you decided this is really something which actually, Sergio, what you said about guiding the testing is a little related to what those guys are doing with the one failure, two failures, three failures. Right?

DR. GUARRO: Yes.

CHAIRMAN APOSTOLAKIS: So, you know, put that together and say here is a place we can actually do this. You also have to include in this consideration the actual software failures, the logic, not just the hardware. That's my view. I mean, other people may have a different view. Right now as an agency it seems to me we have to focus on the identification of failure modes for the total system, not just the hardware.

MEMBER BLEY: That's No. 1.

CHAIRMAN APOSTOLAKIS: That's No. 1.

MEMBER BLEY: Really not in parallel where this philosophical thing will drive both of them. Maybe you're right. Maybe we'll never have data, or not for a long time, but you've got to have that before you can even plan how you would get the data.

CHAIRMAN APOSTOLAKIS: We are not going to tell you how to manage this. These are just ideas.

MR. KURITZKY: We appreciate it.

CHAIRMAN APOSTOLAKIS: We are very careful not to cross the line but let me tell you how I would punish you.

MEMBER SIEBER: We don't actually know how you are going to do this but we heard the comments.

CHAIRMAN APOSTOLAKIS: Okay. How do we proceed?

MR. KURITZKY: Okay. I guess that wraps up that.

CHAIRMAN APOSTOLAKIS: Do you have any slides, Alan?

MR. KURITZKY: Just two slides.

CHAIRMAN APOSTOLAKIS: Okay. Future interactions.

MR. KURITZKY: Okay. You can go to the next slide, Louis.

Just to try and get some feedback on where we should be interacting with the subcommittee, this is the schedule that we have right now with the project, the main milestones. We have the draft NUREG/CR in the first benchmark that's going to come in next month. We'll send that out -- currently planning to send that out for public comment in August, a few months after that.

Then we will get the draft final back in to incorporate those comments in October. The second benchmark actually the work on that is going to be starting almost as we speak. We will get a draft NUREG/CR from BNL on that in December of '08, send it out for public comment in March '09, finalize it and get the draft final back from BNL in May of '09. That's the general schedule tentatively right now.

Given that those are the target dates that we are working towards, Louis, just slip to the next one.

CHAIRMAN APOSTOLAKIS: You don't have anything on the existing NUREG.

MR. KURITZKY: Because the existing NUREG, as I mentioned before, is supposed to be published next month.

MR. MARTINEZ-GURIDI: That's the first bullet.

MR. KURITZKY: The first bullet is actually that first benchmark. The existing NUREG/CR is supposed to go to publication. It was already supposed to be in publication. Now it's been pushed off to the beginning of next month. That is something we will have to take back and reconsider if we are going to adjust that schedule.

CHAIRMAN APOSTOLAKIS: I think that is a good idea.

MR. KURITZKY: That's what I said on this slide because it's theoretically supposed to be out by the time we had this meeting. Now the question is where would be the most useful points to meet with the subcommittee. Certainly input on the draft NUREG --

MEMBER BLEY: I'm sorry. You'll have to put the old slide up. One thing that is not on your plan that is really close to our hearts is something on failure modes that might be Appendix C or some successor to Appendix C.

MR. KURITZKY: You mean for software failure modes?

MEMBER BLEY: For software failure modes. Is that anywhere in this schedule?

MR. KURITZKY: It is not in the schedule. Again, I repeat that the scope of this project is not addressing software.

MEMBER BLEY: And your schedule is this project.

MR. KURITZKY: Is this project only.

MEMBER BLEY: This is a project in which Appendix C or a successor could be published sometime soon, or not so soon.

MR. CHEOK: Russ is not here but let me attempt to speak for him. In the fall of this year he is going to come and talk to this subcommittee on the five-year plan and in it he may discuss the possibility of doing this software reliability. At that point I think that would be a good point to question and ask when the next steps would be for software reliability.

MEMBER BLEY: One last word. There is a lot of work that has been done here already. It's a start and it's a shame for it to languish when just getting into a plan six months from now.

MR. KURITZKY: Honestly it's been languishing for over two years.

MR. CHEOK: Russ has a copy of that report and he is taking that report into account as he is formulating his plan.

CHAIRMAN APOSTOLAKIS: Repeat the name again. Who?

MR. KURITZKY: Russ Sydnor. He's the Branch Chief of Digital I and C.

MR. CHEOK: And that report has been used to help him formulate his plan to go forward.

MR. KURITZKY: So given that the schedule for this project, the comments from the subcommittee on the two NUREG/CRs for the two benchmark, the first benchmark will go out for public comment sometime in the summertime. Late summer or early fall would be the opportunity to meet with the subcommittee to get feedback on that document. By the same token for the second benchmark in the spring of 2009 or that ballpark will be the time to get feedback on that document as they are both released publicly.

However, if you want to influence the technical direction of the work, that we need input much sooner. Today, as we have been getting some, or anytime shortly after because the work for that second benchmark is undergoing now.

See, the technical work for the first two activities, the initial activities and the first benchmark, is essentially done. We can modify the report to some extent but the work has been done. The second benchmark has yet to be done so we are more flexible in being able to maneuver based on feedback for the second benchmark.

CHAIRMAN APOSTOLAKIS: Maybe we can try to find the date somewhere in late May. Would that be good for a subcommittee meeting?

MR. KURITZKY: The question is what would be the topic. What would you be commenting on?

CHAIRMAN APOSTOLAKIS: Well, your first benchmark.

MR. KURITZKY: Oh, the first benchmark. The first benchmark it would not be until late summer because the first benchmark we are going to get in May the draft report. Before we can even release that to the ACRS we have to go through -- it has to be reviewed by myself and internal RES management.

CHAIRMAN APOSTOLAKIS: You just said you wanted advice early on to affect the --

MR. KURITZKY: Right, on the technical work. It's more like we don't have anything to present to you now. You have been presented how we are going to go forward. The first benchmark we will give you some more information on how we have actually implemented it. We have discussed a lot of the insights and results already.

MEMBER BONACA: Are you saying late summer would be the time?

MR. KURITZKY: That would be the time that we can come and brief you on what is in the first NUREG/CR. The question is if you have input that you want to give us to steer the direction of the second benchmark.

CHAIRMAN APOSTOLAKIS: Of which study?

MR. KURITZKY: The second benchmark.

CHAIRMAN APOSTOLAKIS: When would you like that, this June?

MR. KURITZKY: Yes. We would like to have it as soon as possible. There is not a briefing per se that we have to give you on that. It's more like --

CHAIRMAN APOSTOLAKIS: I understand. I said several times today that it's okay to meet with us before you have concrete things to present. You can say, "This is the way we plan to approach this," and then we'll start debating. That's great.

MR. KURITZKY: If that is what you would like to do is have us -- it has to be at least somewhere down the line that we have established how we are going to do that second benchmark. The stuff that is documented in the current NUREG/CR tells you how we are going to go do things. Now you know how we are going to do it so you can comment on it based on that explanation.

However, because it's a new type of system, things may be a little bit different so once BNL gets into the design of that system and it starts to play out how they are going to have to model the system differently than the DFWCS, then we can kind of some up and give you a more updated briefing on how they are going to model that system as opposed to what they have done already. At that point we can get feedback.

CHAIRMAN APOSTOLAKIS: So the next subcommittee then you will brief us on the first benchmark and what you plan to do on the second?

MR. KURITZKY: Yes, unless we can get to you earlier without doing the first benchmark and just tell you how we are doing the second. Again, that depends on how far along we are on the work at that point in time.

CHAIRMAN APOSTOLAKIS: The question is what timing you want because I'm confused now what exactly you have in mind.

MR. CHEOK: I think what Alan is trying to say is we are about to start on our second benchmark and the comments we got from you today on the methodology itself I think we will apply that also to the second benchmark. If you have anymore comments on the general methodology we spoke on today that you think we should apply to the second benchmark at this point, it would be useful.

CHAIRMAN APOSTOLAKIS: Additional comments? I can't think of any.

MEMBER SIEBER: Actually, there weren't a lot of comments on the methodology. The comments seemed to focus on the data which there isn't very much of. We don't know exactly what it means and it's very broad.

MR. KURITZKY: Right.

MEMBER SIEBER: I would consider that sort of a setback as far as reissuing this NUREG because it's going to take a fair amount of editing to remove that. Then what will the PRA practitioners do because you're right. That's where they will go through their failure data and there won't be any. I don't think there's a lot out there.

MR. KURITZKY: We should really be so worried about that concern. I mean, we didn't intend PRA practitioners to go get the numbers.

MEMBER SIEBER: But that's what they'll do. That's what I would do.

MR. KURITZKY: No, but if we take them out I wouldn't worry about that.

MEMBER SIEBER: What it does is setback the whole process for perhaps a year or more.

CHAIRMAN APOSTOLAKIS: Do you think trying to set up a subcommittee meeting in June would be useful?

MR. KURITZKY: I don't know.

CHAIRMAN APOSTOLAKIS: Is it too late?

MR. KURITZKY: My intention really is just to have -- I wasn't envisioning another briefing because I don't know exactly where we'll be. I understand the subcommittee's interest to discuss these topics before we have a NUREG/CR, before we have a formal report that we can submit to you for review. What I don't have right now is a good timeline on when we'll have at least a minimum amount of stuff that would make it worthwhile.

CHAIRMAN APOSTOLAKIS: Okay. So you can coordinate with the ACRS staff.

MR. CHEOK: One proposal is that Russ Sydnor is, again, going to come and talk to you about the overall plan and you could maybe get an hour or two at that time to talk to the subcommittee on our first results of our first benchmark.

CHAIRMAN APOSTOLAKIS: You're saying this will happen in the fall?

MR. CHEOK: And it would be in the September/October time frame.

CHAIRMAN APOSTOLAKIS: That is kind of late.

MR. KURITZKY: Yes, that's the issue.

CHAIRMAN APOSTOLAKIS: Now, we also have to prepare for the full committee meeting. When are you going to present?

MR. KURITZKY: I didn't know there was one until a couple of hours ago.

CHAIRMAN APOSTOLAKIS: Well, a condensed version of what --

MR. KURITZKY: Right.

CHAIRMAN APOSTOLAKIS: One thing you may want to add is a discussion of how you plan to respond to comments you receive today. That's probably the only new thing, a condensed version of what you are doing.

We have a new version of the report, Christina, so I can --

MS. ANTONESCU: I think we need another version.

CHAIRMAN APOSTOLAKIS: Oh, there's another version coming?

MR. KURITZKY: There's not a final version. What you have is how it stands as of last Tuesday.

CHAIRMAN APOSTOLAKIS: Oh, okay. The members don't have that, do they?

MR. KURITZKY: It's not much different than the one that you do have.

MEMBER BLEY: And it's still got the

appendix in it and all of that.

MS. ANTONESCU: The appendix is still there.

MR. KURITZKY: Until we finalize the report, there is not really a new version.

CHAIRMAN APOSTOLAKIS: Okay. That's okay.

MR. KURITZKY: Then, of course, now we have other things that we are going to work with on that report.

MEMBER BLEY: Back to your question of a get-together. George has said just have a discussion. There have been some other subcommittees I know of that just come together with staff with a set of questions laid out to guide the discussion rather than full presentations. Something like that might be appropriate.

CHAIRMAN APOSTOLAKIS: I repeat, when we started doing the NUREG Guide 1174 staff didn't want to come here. Finally they did come and they started saying, "We are thinking about this or that." The subcommittee gave its views. Then the staff found that useful and they requested the second meeting. It was really a very significant change in attitude.

MR. SHUKLA: One thing I would like to make clear that this has to be a published subcommittee public meeting. Some staff members get confused and they said they can just come in for two hours and talk one on one but that is not what we are talking about.

MR. KURITZKY: Okay. Also going back to what we would present to the full committee besides adding a discussion of how we plan to respond to the comments we had today, I think one thing I would consider is pulling out the discussion of the estimation of parameters. Identifying the issues and the limitations that we have encountered but pulling out a discussion of numbers and the details of quantification. I think it was pretty much agreed by people here.

CHAIRMAN APOSTOLAKIS: Well, you tell us how you see the final NUREG coming up.

MEMBER SIEBER: Well, even before that. Would you ever expect to put forth some kind of effort to come up with better numbers or are you going to wait for the industry to do that?

MR. KURITZKY: Again, something like that would have to be considered within the update to the five-year plan. This project does not have anything in it asking to do that so that would have to come from --

I guess outside of that it would just be, like you said, a condensed version. Mostly the overview presentation. The overview presentation that I gave took two hours.

MEMBER SIEBER: Good job.

MR. KURITZKY: It would be probably something very similar to that.

MEMBER SIEBER: You want two hours for the introduction.

MR. KURITZKY: And then another project will come up and speak. Okay. I guess that's pretty much all we have.

CHAIRMAN APOSTOLAKIS: Do we want to go around the table or have we all expressed our --

MEMBER SIEBER: I think they did a good job but there's a lot of changes now. All this effort is not for nought. It's a worthwhile effort.

CHAIRMAN APOSTOLAKIS: But the report has to be modified drastically. I don't think you can publish it in May but it's your business.

MEMBER BONACA: I think it was very valuable about the FMEA because I was familiar with it. I thought it was great to see at least an example of an application.

MEMBER BLEY: I think I've said everything

I want to say.

CHAIRMAN APOSTOLAKIS: Have you said everything, Sergio?

DR. GUARRO: Yes, I said everything.

CHAIRMAN APOSTOLAKIS: Okay. Staff? Thank you very much. It was very informative and the meeting is adjourned.

(Whereupon, at 3:13 p.m. the meeting was adjourned.)