Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards Open Session
Docket Number:	(n/a)
Location:	Rockville, Maryland
Date:	Wednesday, July 8, 2015

Work Order No.: NRC-1731 Pages 1-161

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

626TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

WEDNESDAY

JULY 8, 2015

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:32 a.m., John W. Stetkar, Chairman, presiding.

COMMITTEE MEMBERS:

JOHN W. STETKAR, Chairman

HAROLD B. RAY, Vice Chairman

DENNIS C. BLEY, Member-at-Large

SANJOY BANERJEE, Member

CHARLES H. BROWN, JR. Member

MICHAEL L. CORRADINI, Member

DANA A. POWERS, Member

JOY REMPE, Member

PETER RICCARDELLA, Member
MICHAEL T. RYAN, Member
STEPHEN P. SCHULTZ, Member
GORDON R. SKILLMAN, Member

DESIGNATED FEDERAL OFFICIAL:
CHRISTINA ANTONESCU

ALSO PRESENT:
ZAYNA ABDULLAHI, ACRS
SUSHIL BRILA, RES/DF
DAN CIFONELLI, Exelon
BOB CLOSE, Exelon
KEVIN COYNE, RES/DRA/PRAB
MICHAEL DUDEK, NRR
DALE GOODNEY, Exelon
BRIAN GREEN, NRR/DRA/APHB
MAURICIO GUTIERREZ, RES/DE
GEORGE INCH, Exelon
CHRISTOPHER JACKSON, NRR
MOHAMED KHAN, Exelon
KENNETH KRISTENSEN, Exelon
MARVIN LEWIS*
MING LI, RES/DRA/PRAB
JOSE MARCH-LEUBA, ORNL
DIEGO SAENZ, NRR/DSS/SRXB
RICH STATTEL, NRR/DE/EICB
TRAVIS TATE, NRR
GEORGE THOMPSON*, GE
RAY TOROK, EPRI
BHALCHANDRA VAIDYA, NRR

*Present via telephone

TABLE OF CONTENTS

P R O C E E D I N G S

8:32 a.m.

CHAIRMAN STETKAR: The meeting will now come to order. This is the first day of the 626th Meeting of the Advisory of the Committee on Reactor Safeguards. During today's meeting, the Committee will consider the following: Digital Instrumentation and Control Probabilistic Risk analyses, assessment of the quality of selected research projects, Nine Mile Point Unit 2 Maximum Extended Load Line Limit Analysis plus -- I always like saying that -- license amendment, preparation of ACRS reports.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Ms. Christina Antonescu is the Designated Federal Official for the initial portion of the meeting.

We have received no written comments or requests to make oral statements from members of the public regarding today's sessions. There will be a phone bridgeline. To preclude interruption of the meeting, the phone will be placed in a listen-in mode during the presentations and Committee discussion.

A transcript of portions of the meeting is being kept, and it is requested that speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume so that they can be readily heard. And I'll ask everyone to check your little portable communications devices and please turn them off.

As a matter of interest, after seven years of service on the ACRS, six years on the Advisory Committee of Nuclear Waste and Materials, and as Chairman and final Chairman of the ACMW, I'd like to thank and congratulate Dr. Michael Ryan on his retirement for the ACRS. Mike, congratulations.

(Applause.)

And with that, we will proceed with the first item on our agenda, which is the Digital Instrumentation and Control PRA. I'll lead us through that session.

I went back and looked at our history on this topic, and it's a long history. As best as we could determine, the last full Committee briefing we've had on this topic was May 8th, 2008, which precedes a good fraction of the current membership of the Committee. Michael will remember it but few of the rest of us. You don't remember to turn your mic on, but that's okay.

We've actually -- in seriousness, we

followed the subject at the subcommittee level, and we've had pretty much a meeting once every year or so. We missed a meeting in 2012. We had a two-day meeting last November, which was, in my opinion, very, very productive. And at that meeting, the subcommittee decided that it was probably time for the full Committee to get briefed on the status of this. As we all know, digital instrument and control systems remain a thorny, if I can use that word, issue for new reactors and, to some extent, retrofits of existing reactors. The methods and data and approaches that people use to model and evaluate the reliability of those systems, especially considering the behavior of the software, in the context of probabilistic risk assessments are challenging, and we decided that the Committee should hear an update on both the staff's and the industry's progress to date.

And with that, I will turn it over to Kevin Coyne, I believe.

MR. COYNE: Okay. Thank you very much, Chairman Stetkar. I'm Kevin Coyne from the Office of Nuclear Regulatory Research in the Division of Risk Analysis. Thank you very much for the opportunity to brief the full Committee today.

The timing of the meeting is very

fortuitous for us. We're in the process of updating our five-year digital I&Committee research plan, so we're looking forward to feedback from the meeting to help us with that plan update.

As you had stated, we have had numerous subcommittee briefings on the topic of digital I&Committee over the past several years, and the Committee has expressed some concerns with the degree of alignment between the research activities being conducted by the Research Division of Engineering and the Division of Risk Analysis, essentially the deterministic and probabilistic research activities we're doing. And we've taken those comments to heart and have done a number of activities to further improve the alignment between our research efforts, including more frequent periodic meetings between the staff working in these areas, review of each other's products and particularly early reviews as products are being developed, and having joint meetings, such as this, which we hadn't routinely done in the past but we're trying to make an effort to brief the Committee together, rather than doing separate briefings. And I think all these things have helped us make sure that our research activities continue to be complimentary and well aligned and going in a unified direction.

There are still some big challenges we're facing. One of the big ones is vocabulary. The words people use to describe various aspects of digital systems is still a challenge. There's a different set of vocabulary that an I&Committee engineer would use versus a PRA engineer, and the vocabulary depends on the level of detail you are analyzing the system at.

We continue to work in the area. We think that we have a pretty good understanding of the core concepts that we're investigating, and we're continuing to work on trying to smooth out the vocabulary so that we have good communication between the I&Committee engineering community and the PRA community to make sure that stays unified.

This morning, we'll discuss several significant research activities, including the failure mode characterization work being done by the Division of Engineering, an update on the digital systems statistical testing that we've done in the PRA area, and joint work on software reliability modeling we're doing with the Korea Atomic Energy Research Institute. In addition, we're very fortunate to have Roy Torok from the Electric Power Research Institute with us today to talk about their research activities in this area.

With that, I'll turn it over to Mauricio Gutierrez to begin the presentation.

MR. GUTIERREZ: Good morning. Thank you for your time today. I'll just jump in right into the presentation here on NRC's failure mode-related research.

For the agenda here, I'll just provide a quick summary of the digital failure mode-related research efforts that we have. I'll also provide a summary of feedback that the ACRS I&Committee Subcommittee provided and NRC's response to that feedback at our meetings. And after I review that, I'll just provide a summary of staff follow-up actions. Some of that will include just a review of the differences of how our each respective divisions look at the problem, the PRA perspective and the deterministic assessment perspective. And then we'll conclude with a look at the failure modes that we have identified.

So as mentioned before, ACRS has a longstanding concern on the digital I&Committee systems. Digital I&Committee system failure modes are not well understood. The concern here is that there are misbehaviors or things that digital I&Committee

systems can do that are not performance -- I'm sorry, excuse me. There are misbehaviors that can occur that occur when there's non-performance of required functions.

ACRS brought these concerns to the Commission's attention in 2008, and that resulted in an SRM, which directed the staff to do two things: to report the progress made with respect to identifying and analyzing digital I&Committee failure modes and to discuss the feasibility of applying failure mode analysis to quantification of risks associated with digital I&Committee.

On this slide here --

CHAIRMAN STETKAR: Mauricio, if I could, from the previous subcommittees and I think our letter way back then, our concern was, with failure modes our concern was especially with people trying to model failure without really understanding the failure modes.

MR. GUTIERREZ: Right, yes. That's a good clarification. I went back and looked at the original or, I guess, many of the original transcripts, and it goes along the lines of what you were saying. There was a lot of, there were a lot of statements indicating that there was a concern that it wasn't just the failure modes. Failure modes was, I guess, a secondary issue. The issue was understanding how digital I&Committee systems operate and how they potentially fail. And that's the issue that we've been working on, the broader higher-level issue.

CHAIRMAN STETKAR: I think failure modes are not a secondary issue. Failure modes are an important issue for framing the PRA models. I go back to the analogy that we've always used. Until we identify clear failure modes for a valve, failure to open, failure to close, spurious opening, spurious close, people were floundering trying to develop models for valves. They would have, somebody would say, well, leakage from a seal is a failure mode, so I should model that. Loose bolts is a failure mode, so I should model that. Until you develop that taxonomy of failure modes, people don't have the construct to create the models. They don't understand what it is that should be in their logic model, nor do they understand how they should compile information and, if it's available, experiential data to support those particular failure modes.

So failure modes isn't an ancillary function. It's the primary function for making the transition from a drawing of a system or a description of software to a discrete model for that system or the software. And I think that's the sense of our letters.

MR. GUTIERREZ: Okay. Perhaps I chose a poor word there in describing what was done. But, yes, I mean, to go back, that was a concern is how do digital systems operate, how did they fail? And one approach to looking at that was to try to identify the failure modes that can occur in digital I&Committee systems. Is that fair? Yes. Thank you.

MR. SKILLMAN: Mauricio, I would like to add perhaps a different perspective or reinforced perspective. As you identify at the bottom of slide three, report of the progress made with respect to identifying and analyzing digital I&Committee failure modes, would you contrast the difference between the failure of the software versus the failure of the digital hardware? Those are different issues, and it seems that those two are combined in this discussion when, in reality, the failure modes of each may contribute to the total system failure, but they are not the same.

MR. GUTIERREZ: You're right. I mean, so, yes, there are different things that can go wrong in hardware systems and there are certain things that can go wrong in software systems. In RIL1002 and perhaps in some of our other work, we've made a distinction as to what is a digital system failure mode, and we're using words here like software failure modes. We've chosen to use a different terminology for what can go wrong with software.

I think our senior technical advisor, Sushil Birla, has a comment here.

MR. BIRLA: Thank you. Thank you for that question. I'm Sushil Birla, senior technical advisor at the NRC in the Office of Nuclear Regulatory Research Division of Engineering. The work that we performed focused at the system level, the system function level, rather than at a component level, whether it's a hardware component or a software component, and, at the function level, how to abstract the behavior in a manner that we can relate to bad effects, like adverse effects on safety.

Your observation is accurate, and that could be the thrust of some of the later slides that when you have a system that is not the traditional hardware component-based system, there are new kinds of misbehavior that are arising for which we do not have an adequate, good enough understanding.

So the traditional hardware component-based systems, we used to think that if a hardware component fails, primarily due to wear and tear, the function that the system is supposed to be performing will not be performed to its specification. And there is, unfortunately, the carryover that, when we have systems that have something more than hardware, complex logic, whether it's in the form of software or firmware or whatever, that same kind of characteristic, the wear and tear oriented and then the hardware failure, that carryover does not occur. And we are victims of what we have grown up with, what we are used to, whatever our thinking is, and that has interfered with the proper understanding of misbehaviors when you have complex logic in the system. And he'll get to it, and if you are still unsatisfied I can come back and add more.

MR. SKILLMAN: Thank you, thank you.

MR. GUTIERREZ: Okay. So move on to the next slide here, and this slide basically just presents research that has included the use of failure modes or has identified failure modes within NRC. For the DRA portion, Ming Li we'll be speaking about this work a little later in his presentation.

For DE's work, here are the products that we have been working on: RIL1001, which dealt with software-related uncertainties; NUREG IA-0254 dealt with understanding faults attributable to complex logic; RIL1002 that dealt with the identification of digital I&Committee failure modes; RIL1003 is a current work-in-progress and it deals with the feasibility of applying failure mode analysis to quantification of risks associated with digital I&Committee systems. RIL1001, which was recently completed, concerns a broad view of hazard analysis to address misbehaviors attributable to engineering deficiencies in digital I&Committee systems.

So in 2013, the ACRS I&Committee Subcommittee was briefed on RIL1002 and provided some feedback. They appreciated the synthesized set of digital system failure modes that were identified. In the most recent version of RIL1002, the final version, this is set out, and some members requested harmonization of the failure modes that were identified with work that has been done by DE, Division of Engineering, by the DRA, and by EPRI.

So the staff response to that feedback was that we have been meeting and working more closely. DE staff and DRA staff have been meeting regularly monthly since that time, and DE has also been meeting with EPRI to discuss harmonization of the failure modes that have been identified.

MR. BLEY: I just want to interrupt with a note for the record. You've said a couple of times the subcommittee told you to do things and you have action items from the subcommittee and we requested. In fact, the ACRS only speaks through our letters, so members gave you individual comments, but we can't request or give direction, actually, except in our letters.

MR. GUTIERREZ: Yes, that's good feedback and a good point for clarification. In all the work that we do, we regularly discuss and obtain multiple viewpoints of the work that we do. We have our work reviewed, and, in our discussions, we take all the technical feedback and then we go back and look at what was provided, and we try to make the best technical decision of which the ACRS members that provided their comments. That's how we took that.

So one of the things that we did to begin our discussions was to try to take a look at the viewpoints from which each of our respective perspectives comes from. For deterministic licensing, the area that DE is mostly focused on, we looked at our objectives, and our objective is safety assurance: making sure that a system is safe, that it's able to perform its functions. It involves asking questions, like what can go wrong and what are the consequences? Perhaps Ming can speak a little bit to this if I don't speak clearly enough on this subject, but, for probabilistic risk assessment, they're looking to support quantification of system reliability. They're looking to estimate risk by computing real numbers. They ask questions like what can go wrong, how likely is it to go wrong, what are the consequences, and which systems and components contribute most to risk? We find that we have a lot more in common than differences when we look at our different perspectives.

And this slide here, slide number eight, it just has the failure modes that have been identified and that we have been using. Failure mode set L on the right is a set of nine failure modes. The middle set was done by a WG Risk Survey, which was, I guess, partly sponsored by NRC. DRA had input to these failure modes. And the last set of, I guess, of failure modes that we have here, they were identified by EPRI. EPRI called them guidewords. And it should be important to note that EPRI has identified several different sets of guidewords or keywords that they can use for different hazard analysis methods and tools that can be used for considering digital system failure modes.

And what we've found, as we've been discussing what DE has identified, what DRA has identified, and what EPRI has identified, is that, although we may be using different ways of describing or characterizing what we're talking about, that there is a considerable amount of overlap in terms of what we have identified. So there is no, as far as we can tell, no technical disconnect in terms of what we were discussing in terms of what can go wrong with digital systems.

CHAIRMAN STETKAR: Mic.

MR. BROWN: Sorry about that. Thank you very much. If you look at, I just clicked on output intermittent. I'm just asking a question here. That's not consistent, in my mind, with no signal actuation when demanded. You have intermittent function, intermittent output, and then you've got something definitely doesn't happen. So on a equivalency basis, I just, you've made the comment that they're roughly similar in terms of the concepts you came up with. That one had a little bit of a disconnect for me. I understand intermittent, but intermittent means a lot more than, hey, I've demanded something and something doesn't happen. That's a different, that's a whole different thought process. It seemed to me that would be, from past experience, whether it's software or hardware, intermittent operation even in software -- I mean, a set of software commands or a sample time or whatever it's going to run through and it to not work, but when it comes to the next time it works just fine because of some initialization that was done or some particular signal was there. Tracking that relative to even in analog systems, intermittent stuff drove us crazy. Sometimes it worked, sometimes it didn't. We never could, you can't pin it down.

So it's a little hard for me to grab how you have typed that piece. I'm just making this from the observation that, when I look at these, I see concepts or thoughts or functions, but I'm still trying to grapple, as I made the comment in the subcommittee meeting, with is there another topdown approach that the PRA can take relative to these systems, as opposed to a piece part, build it up from the bottom, in terms of failure modes or how they operate or their risk assessment in terms of their operation, the risk associated. I still haven't come to grips with how you do that, but I know I've made that comment several times. And I'm still struggling with how we get there. This is a very difficult task, no matter how you slice it.

So, anyway, that's just an observation on thought processes.

MR. SCHULTZ: Mauricio, let me ask this differently. You seem to present this to suggest that there's commonality among the columns, going left to right, right to left. Hearing the comment earlier that was made by Kevin that we're dealing with certainly communication and language and definition here, it seems to me that there's a lot of difference between the line items across the page. And I would have thought that you would be trying to come to a better agreement or common, commonality in terms of the terminology so that all of the document, the survey, EPRI's guidewords could all merge in some sense so everyone knows what is being said and it can be used analytically sometime in the future.

MR. GUTIERREZ: Yes. So --

MR. TOROK: May I? This is Ray Torok from EPRI. I'd just like to add a little clarification. In regard to the EPRI guidewords, those are from one of six hazard analysis methods that are documented in the report we put together. This particular one is functional failure modes that affects analysis.

And in some of the other hazard analysis methods use guidewords. Not all of them do. And I guess the point is that, with different sets of guidewords, you can still cover the waterfront in terms of potential failures and misbehavior.

So if I look at these and try to compare them, for example for the operative intermittent one versus intermittent function, what I'm asking myself is about the effect on the downstream equipment because by itself, it doesn't do anything directly, right? It controls some component that's part of a system, and you want the system to work.

And so what I ask myself is under what circumstances could the system not actuate, let's say, or could the component not do what it's supposed to do? And if there's intermittent function from the control system or if there's output intermittent from it or if there's no actuation signal when demanded, all of those can pick up that kind of failure. So the point is can we put together a set of guidewords that will cover the waterfront that you really care about? And that's why our conclusion was the guidewords don't always have to be the same because different sets of them can lead you to the thing you care about, and that's what we've found.

I can go into a lot more detail on that but . . .

MR. POWERS: It's still kind of a mystery to me why you didn't do exactly what Steve said because you end up with things like degraded function. There's a term that refers in another set to a whole variety of different things.

MR. TOROK: That's right.

MR. POWERS: And it seems to me, if you're using that as a framework for modeling, you're going to be very confused.

MR. TOROK: Yes. Well, for us, where this came into play was in the assumption that -- and for PRA, you care about what the system is doing and you care about what the components within the system are doing to make the system work. The I&Committee is at a lower level than that. The I&Committee can affect these components. And if you talk about degraded function, yes, you're right, the function can be degraded in lots of different ways by lots of different types of misbehaviors or failure modes at the level of the I&Committee, which we would probably call failure mechanisms, not failure modes. But it's the same idea. And the understanding of those is important in helping you figure out if the system, or the I&Committee in this case, has design measures that act to prevent or avoid certain failure modes by defeating the mechanisms that cause them, that sort of thing.

So if I talk about degraded function, the waterways that I&Committee can push you down that path, depending on the failure mechanism you care about. Did the processor lock up, is there an incorrect control algorithm built into the thing, that sort of thing. But in the end, what you care about is whether or not the component that's controlled can misbehave, and there are ways that the I&Committee can help that happen.

I don't know if I answered the question or not.

MR. POWERS: Well, I mean, what I'm detecting is that you're directing your work for a very short-term kind of goal, do I need to fix it or not, and we're looking at a more comprehensive thing I think. We want to understand in a more predictive fashion when these things are going to happen, and you're not giving us the framework to do that.

MR. TOROK: Are you thinking in terms of looking at failure data and using that to generate failure probability?

MR. POWERS: Sure.

MR. TOROK: Yes. It turns out, in our case, that's very difficult for the digital equipment, especially in high-integrity systems, because there's not a lot of failure data to look at and there probably won't ever be. Although we did do some of that. I shouldn't say we didn't do that. But in a lot of ways, for practical purposes, it appeared to be more useful to try to understand the failure mechanisms of the digital I&Committee and then look to see if the design was set up in such a way that it could defeat those. And that was a better way to get a handle on whether you're looking at a robust system or a not very good system.

So, yes, if you're talking about gathering the data to support it, like you would for a traditional piece of hardware, that's problematic for digital I&Committee. Oh, and somebody mentioned there are hardware failures and software failures, and that's right. But what we see in a lot of the high-integrity digital systems is they'll have redundant hardware with the same software in each channel. And what that does, effectively, is it eliminates hardware failures from a practical standpoint as significant contributors to the system failure or to the I&Committee failure, and then your focus is on the software and now you're into design measures that can help you, as opposed to failure data.

MR. COYNE: If I could build off of this -- this is Kevin Coyne from the staff. If I could build off one of Ray's point is this slide with the digital failure mode mapping is an imperfect exercise, at best. And one of the dimensions that's really missing here is a level of detail we're looking at the systems. And Mauricio actually has a backup slide that I'm not sure that he'll cover or not, but it's hard to find a good analogy but we did an analogy back in the November meeting of a failure of a system to deliver adequate flow, and it drills down on a valve. And depending on the level of detail, there's a cascading effect between the failure mechanism mode and effect. And, you know, as you move up and down those levels, failure modes change, and so to come up with a strictly consistent, uniform mapping of failure modes at all levels of detail is really beyond what we can do, so it really is dependent on the level of detail you're looking at the system.

And I think with the WG Risk Survey, one of the issues is that's looking at PRA function. So, again, as Ray had said, you know, it's the availability of core cooling is the ultimate function you're looking at, and so you're looking at the digital I&Committee system's effect on your ability to maintain adequate core cooling.

MR. TOROK: That's a really good point, Kevin, and I neglected to mention that the guidewords in our cases go with this method called functional FMEA, and they're intended to be useful at any level of abstraction, from the I&Committee up to the system in the plant, and they work that way. And that's one of the reasons that I think that maybe you could look at and was kind of vague in regard to I&Committee.

So I consider them sort of generic failure modes in the sense that they can be applied at any level of abstraction, which is the normal thing, by the way, for hazard analysis methods. They don't focus on I&Committee.

MR. BROWN: John, you were going to say something? I was going to say something but let you go first.

CHAIRMAN STETKAR: No, go on, Charlie.

MR. BROWN: You mentioned level of detail, and I guess that's one of my concerns and maybe I didn't express it very artfully the last time. But if you look at a whole chain of an instrumentation system, you've got a detector, you've got an analog-to-digital converter, you've got some processing you go through, you generate and go through an algorithm of a trip that's got other signals from other detectors coming into it, then you trip, then you go to an actuation device or you set up a conditional set of things for multiple, you know, two out of three or whatever it is. Where do you start with that?

I mean, the bottom line is the last part, the setting up the conditional condition, two out of three. I've got a trip. One of the three or four I need to do something. How far back in the food chain do you try to pick it up? Do I say, okay, this analog-to-digital converter failed, I now no longer have a valid piece of information out of that, and it's one of three signals that's used to develop or go into an algorithm that produces this signal. You work on that, or do you assess, hold it, there's dozens of little things that could go, do I get the trip or do I not? Which is the most important part? It's not intermittent. It's not necessarily duration too short. It's do I have it or not? Do I care about the other circumstances, and am I complicating the effort here to try to look at this stuff by going down to that level of detail? That's what I've been struggling with at looking at how you do this in this mode or with these systems.

MR. LI: This is Ming Li. By level of detail, we mean something a little bit different. Mr. Brown, you mentioned that the information flow changed at our level of details. Level of detail, like an RPS. So we can model the RPS in a PRA sequence, like take that to RPS, add one black box. So the black box RPS function which generates trip when the trip condition occurs. So one failure mode should be it did not trip when it should. Another failure mode, it trips when it should not. So we call this the system level.

And if we have data to support that failure mode, then everybody is happy. Then we just model the RPS at that level because we have data support. It's unfortunate we don't have data support that's a black box. Then we had to divide fuller to one level below, like the input module, output module, data processing, and the communication possibly. And then we started at whether we have data to support that. What's the failure mode for the input module? That might be incorrect value and incorrect timing, you know, something similar.

And for the PRA, normally, it's rare we go down to the very bottom level, like the transistor failed. Do we need to kill the transistor for PRA? It might sometime if we really don't have data. So we might come from the parts level. So you use the parts count method, start from each part individually, and then come up with failure data.

But whenever they have the data support that card, the communication card, if I know the failure rate for that communication card, I don't need to go down to the parts level. But if you have the failure rate for that card, the model, you know we've got the card at the black box in our, you know, models.

Software might be something different. I'm going to cover software a little more in my talk. But by level of detail, we mean the functional level, instead of the information flow from the input to the output where something happens.

MR. BROWN: I understand. I wasn't trying to say take it to that level. I'm just using it as an example. But I would argue that your ability to find a significant failure rate for what you call an input module or an output module, whatever it is, one level down from did it trip or did it not trip functionality, is there a great industry reporting system for all that?

CHAIRMAN STETKAR: Charlie, try not to force everything into data and numbers, okay? That was the problem 35 years ago when people --

MR. BROWN: I, I --

CHAIRMAN STETKAR: Charlie. Thirty-five years ago when people first started to do risk assessment, people were trying to collect data for loose screws. But until they reached the taxonomy of failure modes and didn't care about the minutia, it got easier to understand the experience base to dump into that intermediate level of detail. You didn't care about the data for loose screws. You didn't care about the data for resistor open circuits or --

MR. BROWN: I agree with you.

CHAIRMAN STETKAR: Okay.

MR. BROWN: I'm not arguing with you. I agree with that.

CHAIRMAN STETKAR: But then don't talk about where is the data available or where are the data available.

MR. BROWN: He said several times, he threw data in, he says if we had the data to do something. I was responding --

CHAIRMAN STETKAR: And that's --

MR. BROWN: So that's part of his response, okay? And that -- because I think, I agree that is not a very useful way of getting to where you want to go.

CHAIRMAN STETKAR: The point is that, once one identifies a set of, we'll call them failure modes then everyone understands conceptually, we'll call this L1 through L9 and we'll give it names. It's just L1 through L9 boxes, but everybody knows what an L3 is. Once we understand what the L3 is, we can then look at experience and find out what's our evidence for that thing. Sometimes we might not have any. Sometimes we might need to rely on expert opinion, okay? But that's important. I think we're saying the same thing. It's just I want to keep us pulled away from this notion of where are the data and we don't have any data and data, data, data.

MR. BROWN: That's what I was trying to get to in responding because they started talking about we get failure information on these pieces, whether it's here, or do we want to worry about the -- we don't. And the point is how far functionality do you look at it? And that's why I'm concerned that, when you look at these particular things in here, you're down in the bottom part. You're down in the midst of the thing and close to a higher level of that -- I'll stop right there and we'll get on with this.

MR. POWERS: It seems to me the other question that rises from your discussion, I think I understood, is that you spoke in terms of trip/not trip, but I see on this list of roadmapping things fall somewhere in between, maybe fluttering or intermittent function or things like that. Have we gotten to the point that we can, indeed, set up modeling that treats yes/no kinds of responses or do we have this intermediate it functions but it functions badly or poorly or functions for a while and then stops, things like that?

MR. LI: I believe your question -- again, this is Ming Li. I believe your question regarding, you know, in my examples I talk about the failure mode happened, not happened, trip, not trip, at the very high levels. And this chart, the main thing here, it's a mixture failure mode at different levels. And if we take a look at spurious actuations, I'm talking about the middle column of WG Survey. Say they're to activate the failure mode that I was talking about, which is not trip when it should, and the spurious actuation is another. So those two, the row number two and number three, is actually the system level failure mode I talked about.

MR. POWERS: I mean, you're hitting it -- the philosophical issue that I have here is that we've got this map that's just not very useful to us because you want to use just a higher level than this map was operating at, and I'm just not sure what I do with the map now. Do I just throw it away or ignore it or . . .

MR. GUTIERREZ: I mean, I think that the mapping has actually been very useful to us because when we have our discussions and we start talking about things that can go wrong with digital systems, we find out that we're covering much of the same ground, that we have common understanding of how the systems function and what can go wrong with them. That's the purpose of the mapping.

MR. TOROK: Well, and it comes in very handy, for example, if you're doing hazard analysis on a system and you end up asking yourself under what circumstances is it a bad thing if the system doesn't actuate when it's supposed to or if it does actuate when it's not supposed to. And if it is problematic, then the next question is what is built into the system to prevent that or to avoid that, that kind of thing. So it does help a lot in terms of figuring out if the system is robust. It gives certain failure mechanisms and failure modes. So it's very helpful there.

MR. POWERS: I suspect we're operating in a different mind set because I'm blatantly worrying about modeling these things, and I don't think that's your focus here because I look at this and I say, gee, I've got yes, no, and maybe, and I don't know how to, I mean, in a PRA context, maybe is a problem for us because PRA is not well set up for handling maybe.

MR. TOROK: I don't know that we use these at the PRA level. We're using them a level below that because the PRA is the controlled component, what that's doing, and this is a level below that, at least in our work.

MR. POWERS: Then the trouble I have is then just making it difficult for two levels to communicate with each other, which I think is what we kind of hoped we would get to the point that we would have smooth communication by understanding as failure mode issue.

MR. GUTIERREZ: Well, I mean, I think the communications is improved. I think some of the things that you're bringing up are legitimate things that we've discussed is how do you define the problem, how do you set the boundaries, and what we're using here called failure modes, what is useful for the perspective that each of us is applying to try to work on one piece of the puzzle.

MR. POWERS: I'm just not seeing how you do that right now. Maybe as you go through the presentation I'll understand how you're doing that. Right now, it seems to me that we're no better off than we were whenever Apostolakis came on to the ACRS because he's the one that pushed this failure mode.

MR. TOROK: I think it was 1950, wasn't it?

MR. POWERS: No, he came on after I did so . . .

CHAIRMAN STETKAR: Oh, you were 1950.

MR. POWERS: I think I was 47, wasn't I?

CHAIRMAN STETKAR: We had two and a half hours on this. We're on slide eight.

CHAIRMAN STETKAR: Green light.

MR. RICARDELLA: What do you mean by Byzantine behavior?

MR. GUTIERREZ: So Byzantine behavior, we define that in RIL1002 as such, in a distributed system, arbitrary behavior as response to a failure or fault. It's arbitrary behavior of an element that results in disruption of the intended system behavior. So it's arbitrary behavior.

MR. RYAN: It's everything else that's not above.

MR. BLEY: Weird stuff. That's really what they're talking about.

CHAIRMAN STETKAR: But see, Pete, in some sense, that's L9. In my taxonomy, that's L9. As long as everyone understands what an L9 is and if you see one of those you have evidence of an L9, whether you call it Byzantine behavior or whether you call it really weird stuff or whether you call it some other taxonomy that a particular I&Committee engineer might want to use. It doesn't make any difference. As long as everybody understands what an L9 is and what the effects of an L9 are if that thing occurs, that's the important part, in my opinion anyway, of this mapping process.

So, yes, Byzantine behavior may not be a very clearly-defined term. But if everybody from the engineering part who uses completely different terminology to the risk assessment people, who may want a different set of terms, if everybody understands what an L9 is and when it happens, yes, I had an L9 and how I evaluate the effects of an L9 in my PRA model, you've solved the problem.

MR. BLEY: But since it is weird stuff, if I might, what happens in practice, I think, is if they collect a large number of those, pretty soon you'll see categories within it and you generate some new categories here. But you don't expect to see a whole lot of these or at least patterns of them yet, but if you have that could be interesting.

MR. SKILLMAN: What's been going through my mind is kind of addressing Charlie's question, where do you start in the food chain, and what I'm really thinking is we've gone from Boolean in analog-type equipment or Boolean logic in analog equipment to digital. What gives me comfort, to answer Charlie's question, is where can you test with certainty? And my experience is you can test at the card level. And if you begin with a notion that you can identify your failure by knowing how your card failed, then that becomes the smallest element upon which you can be certain of function. I'm thinking of ESAS modules, of RPS modules, where prior to modifying the system or repairing the system, you actually do a module test. You then know that that card or that module is healthy, it's fit for duty. And at least my experience is, you find the failures in the software

are actually embedded in the firmware on those cards, and that's where you detect the failure, particularly if you've had a spurious trip or a spurious actuation. You pull that card and you find that you have an EPROM or some device that is not functioning the way you had believed it was going to behave.

So I guess I start with answering Charlie's question to myself. If I know that the individual components are functioning the way they're supposed to function, then at least I can see how this matrix answers a whole bunch of questions. But if I don't settle on some form of architecture that has devices connected to the architecture, then, quite candidly, I get lost. It's got to be brought back to a practical arrangement of devices that you can actually put your finger on and test, and if you can test it I think you can figure your way through this. If you can't test it, I think we're pumping against the tide.

MR. GUTIERREZ: But I think that there might be a little more to that than just testing something or looking at something once it's already been built. In all of our work here, both at DE and EPRI, we're looking at a broader view of things by looking at different hazard analysis techniques that can be used starting from requirements identification of what you're trying to design.

What we find with digital systems is that you can't wait until it's already built to try to consider what might go wrong. You have to start right at the beginning.

MR. TOROK: Well, and the other thing that comes into play --

MR. SKILLMAN: Excuse me. I agree with that, and what I said before doesn't suggest that I don't agree with that. It's got to be designed right in the first place.

MR. GUTIERREZ: Right. I understand. I'm just trying to say that there's this broader view in which that's included. That's a part of the picture, but there's that --

MR. SKILLMAN: I would just submit you can't get to the broader view until you've assembled the components that you know accomplish the functions that are required. And if you haven't done that, then this grander view basically dissolves.

MR. TOROK: You said something I think is very important. The way we look at it, the failure mode is the behavior from outside the thing, the box, whatever, the card. Typically, the number of failure modes is pretty limited if you look at it at that level. Now, there may be 47 things inside that box that can cause a failure mode, but the failure modes themselves, there aren't many of typically and that makes a thing far more manageable.

MR. BROWN: I'd like to make one more observations, and I'd request that John and Dennis not leap on me when I say this, okay? Because it's somewhat heretical. This is another thought process I've been going through for the last couple of years is how we address this.

Fundamentally, when you talk about your assessing it, does it trip or does it not trip, and what do you do whether you have data, whatever the circumstances are, but that's what you model in your PRA thought process. So I come back and say why isn't that enough? Why is modeling digital I&Committee different from what we do with other systems, what I call the mechanical blacksmith technology type systems? Because the digital I&Committee has an advantage that all these other systems, the hardware-based systems, valves, pumps, you know, all the things that can fail, operators, what have you, that they don't have. You can continuously test these systems, self diagnostics, in realtime, okay? And you can test it for all the inputs because you can have little test units, you know, like a test signal, like a resistor for an RTE, a precision resistor that allows you to calibrate, is this thing calibrated right now?

So you can test the entire chain of processing from beginning to end over some period of sample time while you're doing this realtime operation. You can't do that with the other ones. So is one of the thought processes that, since we can know with a fairly high degree -- I don't want to get into the percentages here -- of certainty that that channel is working because, if it doesn't pass its test, a light goes on and somebody is told when that happens.

So another way to look at this is how far do we want to go? Why isn't your approach on the output enough? Why do I have to worry about the failure modes down in the rest of the system when they contribute to that if I'm able to test each and every division from beginning to end for each input? That's what they're doing. That's the stuff, the self diagnostics. We started doing that in 1979 and '80 with the stuff we did in the Naval Nuclear Program.

The only ratchet on that is what if you don't complete your processing? And that's where the watchdog timers come in, you know, the lockup comment you made a few minutes ago.

Just two thoughts on the lockup issue. If you have processing systems that, if you reset them, which is what we did with the watchdog timer -- we didn't trip anything -- but when you can start up and have your outputs within 250 milliseconds or so, it's a blink of an eye. You don't care. You just let it reset, and, as long as it's working, you're okay. If it's five minutes or ten minutes, like it is with the Common Q platform, that makes a big difference. You don't have functions for quite a while. But, still, you've got the diagnostics that let you know that's happening.

And I'm not trying to denigrate anything. Don't think that. I'm just trying to apply a different level of thought process as to how you address this. I wanted to get that on the record from a thought process standpoint. I hope I've been clear with my trying to articulate what I'm thinking.

MR. LI: This is Ming Li. I totally agree with your comment, and I just feel that trip and not trip, that one is a simple example that demonstrates the level of detail. I didn't mean to say that PRA can only wish they had that level. I totally agree with you. Although the online diagnostic for tolerance of those 16 measures should be included in the PRA analysis, and in my presentation I'm going to talk a little bit more detail on that.

MR. BROWN: All right. Well, thank you for letting me rambling on. Thanks, John and Dennis, for letting me ramble on.

MR. GUTIERREZ: Okay. For our final slide here, I'll present conclusions and our next steps. Based on our work, DE, DRA, and EPRI, we believe we have a shared understanding of the issues that lead to misbehavior, other than non-performance of required function in digital systems. DE and DRA agree that Failure Mode Set L could be useful for each of our respective divisions in our work.

NRC and EPRI will continue to share technical information from digital system failure mode-related research. We are continually working on vocabulary harmonization. It's a topic that's on the I&Committee research plan 2015 to 2019 candidate pool. And we are continuing our work on RIL1003, which will report on the feasibility of applying failure mode analysis to quantification of risk associated with digital I&Committee system.

MR. BROWN: Should they continue, John?

CHAIRMAN STETKAR: Yes. This is the ACRS. Always interpret five seconds of silence as proceed as rapidly as possible.

MR. GUTIERREZ: So now I'll hand it over to Ming Li.

MR. LI: Good morning, Mr. Chairman and the Committee. My name is Ming Li. Next, I'm going to brief the Committee the standards of the NRC research on digital I&Committee PRA.

NRC started this research program trying to address the regulatory needs associated with a shift of the nuclear power plants' instrumentation and control systems from analog to digital. Since the Commission encouraged using PRA technology in regulatory measures as much as possible, this shift to the digital I&Committee system should be included in the PRA.

Since there are no agreement on the method that could be used in PRAs, the National Research Council recommended that NRC should develop a method to address failures from the digital component, including the software. The case to include the digital I&Committee system into PRA is to develop a reliability model to quantify and then to model and to quantify the digital I&Committee systems.

Since the digital I&Committee system consists of the hardware, the software, and a lot of dependent interactions among them, so, ideally, such reliability modeling for digital I&Committee system should also include reliability, hardware reliability models and the software reliability models and a model that can account for all the dependent interactions.

We already touched the concept of the level of the details a little bit. I want to highlight here again that the PRA focused on the functional levels, so here's an example that it's very rare to see a PRA started from the transistor failures or start from software statement errors, error in the statement levels. It rather focused on the functional level, as I mentioned, trip/no trip or even lower, like the input module, the output errors and the output models, the actuation errors or the processing modules so the processing failures.

So as for the hardware reliability model, I will claim that it's well developed and well accepted in the industry, especially in the telecommunications and aerospace industry. Normally, they use the two methods they call the parts count or parts stress, and they use a lot of handbook data to start if there are no field data available. If fortunate and there are field data available, then people use the field data because the handbook data sometimes is way too much conservative. Their example from NASA that a reliability prediction is like a two-year lifetime, but after 20 years the satellite is still operational in space.

So if there -- yes, go ahead.

MR. BROWN: I'll wait until you're done.

MR. LI: So if there are field data available, operating experience data available, so people tend to use that data instead of the handbook data. But if start from scratch, their new design, there are no field data availalbe, then start from the handbook data.

MR. BROWN: I would just make one observation there. We went after the handbook data years ago. There was an Air Force manual or some other manual that had voluminous quantities and how you would consider it and how often, you know, the failure rate for various types of parts. And the fundamental point was the more parts you had in it, the more likely you were to have failures. I mean, I'm generalizing somewhat, but that was generally the approach. The more parts you have, the higher the probability of some failure to not perform that final function. And quite frankly, when I went from analog to digital equipment, I probably quadrupled the number of parts in our modules in the cards and every place else, and our failure rate for cards went down.

So I guess came up with the conclusion the more parts I had, if they were the right kind of parts, and, fundamentally, it was driven by the fact that it was digital, as opposed to an analog, and the drift and other types of functionality that caused them, whether it be temperature, vibration, or what have you, had less of an effect on the modes of those, you know, the failures than it did in the analog systems. I'm not trying to say that as an absolute statement, but that was it.

I had my boss at one time, when I wanted to increase the operational functionality of the submarines, I wanted to install two more of a particular type of instrument that are having two and tripping on one out of two, I wanted to go to four and trip on two out of four. He threw me out of his office.

When I got a new boss, I proposed the same thing, put it in, and the problems we had with those systems went down and it was not allowing the ship to operate. I put in more parts, a lot more parts, doubled the parts, but, yet, the operational performance of the submarines and the carriers improved markedly. We no longer had midnight phone calls because you had noise preventing your source range or intermediate range, you couldn't start up because the rules you said you couldn't start up if you didn't have a full complement of such and such.

So the parts count part, I really get stuck on this parts count and those types of rules, in terms of defining what the failure probabilities are. I just don't think those rules of thumb are as applicable to the digital systems. The digital systems are more tolerant of variations, as you look at how the analog to digital and then how it's triggered. The variations, once you're digital, are very, very small. So, anyway, that's --

MR. LI: Yes, I agree.

MR. BROWN: That's my experience. I'm not speaking --

MR. LI: Yes, I totally agree with you, but we need to consider this from a different perspective. First of all, the digital parts are more reliable than analog part if you take a look at the handbook. So if the same amount of the part, so digital design are normally more reliable than analog design.

Second of all, you mentioned a redundancy, and the data are there to implement redundancies. If you implement redundancy in the system, so you dramatically drop your failure probabilities, from that perspective --

MR. BROWN: Functional failure probabilities.

MR. LI: Functional failure probabilities, yes, yes. And if you have the same design, the same functionality, there are no redundancies. One, you have 100 parts, another one you have a million. That's a more complicated part more likely to fail. That's what I mean by parts count.

MR. BROWN: Maybe. Okay. Go ahead. I'm sorry.

MR. LI: All right. Thanks. On the contrary, software reliability are more complicated.

MR. BLEY: I'm sorry. Charlie is looking at me. You just discovered something that the Germans figured out in about 1940. But it's true, it's true. System reliability is different than piece part reliability. And the way you put the piece parts together make a big difference on how --

MR. BROWN: And the nature of --

MR. BLEY: Counting doesn't do it.

MR. LI: All right. Let's get to the software reliability. Software reliability modeling is more complicated than hardware reliability modelings. So although there are over a hundred software reliability models in the literature, so none of them is acceptable to current NRC and PRA requirements.

And there are still a lot of arguments in these disciplines. For example, one big argument is that software does not fail, so software failures is not a valid concept. And in this sense, we define software failures in terms of a functional deviation, sorry, deviation from expected behaviors. So software does behave differently from the end user expected them to do. So from that perspective, software does fail.

And another big argument is that what do you mean by software reliability? Software failure mechanism is a deterministic process. Software either fails or it functions. It's not a random process what we mean by software reliability.

So it's true that a software failure mechanism is deterministic. If one can repeat the software execution environment, normally we call it operational profile. Then you can repeat the same errors. But think about that, that operational profile. That operational profile is statistic in nature. So think about the combination of the statistical input and the deterministic failure mechanisms. So the overall failure behavior manifests as a statistic process.

MR. BROWN: When you're done.

MR. LI: So by that, so software reliability is still probability. It's still probabilistic process, so software reliability is a legitimate concept.

MR. BROWN: Okay. Let me provide just another observation comment here. The more complex the software, in terms of how it's configured or how it's set up, can translate into the type of what I call more unknown-unknown. The more interrupts you have in a processing chain in anything, if you run an interrupt-driven system, you significantly increase the probability of having collisions or confusion arise in the computational process from beginning to end. That's why you want a short sample time. You want everything to be executed in one pass, everything every time. The main operating loop just regurgitates itself.

MR. LI: And you block all interrupts.

MR. BROWN: But if you have no interrupts -- you can never get rid of all interrupts. There are certain types on the beginning in terms of putting stuff into memory buffers and things like that. You have those, but those don't interfere with the main processing path, okay?

So the reality is if I look back and I get rid of interrupts, I won't say there's very few but there's a more limited set of things that can prevent that deterministic main operating loop from not going from start to finish. Much fewer items that can do that. And now you're down to where a particular set of logic shifts doesn't trip when it's on the leading edge or the trailing edge of whatever the clock signal is. So you don't get the signal and all of a sudden it doesn't know what to do.

So you're more hardware-oriented in many circumstances if you get that. The complexity, in my experience, was a failure to the software. Whenever we had started introducing interrupts, that's where we started having problems and it was difficult to test them out. So, you know, it was just an observation.

MR. LI: Yes, I totally agree.

MR. SKILLMAN: I'd like to ask a question here, please. You've got a definition at the bottom of the page of what software failure is. It's defined triggering of a defect of these software, which results and contributes to the host system failing to accomplish its intended function.

And in our homework package, in the BNL document, the NUREG draft, software failure, at least for the study, is identified as the triggering of a fault of software introduced during its development life cycle. And what I would ask you to do is to explain whether or not this software failure at the bottom of your slide is a failure that comes from an incipient failure from the software development or whether this failure is a random event because the software forgot what it was doing.

MR. LI: You are talking about, actually, two things. One, the failure mechanism. So the software failed because of a defect in the software. Defect could be the errors the developer made during the development process or even from the end user from the very beginning, the user requirements.

So the defects, those types of defects, including the end user requirement defect, as I call it, and the errors made by the developer and introduced what we call defects during development process, those defects exist in the software. So during the software executions, some conditions triggers those defects. Then the software behavior manifests as a failure behavior, which means that the software does not perform the expected function.

So you're talking about the same thing but from a different angle. One, the failure mechanism is deterministic. Every time -- deterministic means that every time the input conditions trigger that defect, software fail. So there's a zero or one condition. But the randomness from the operation, the condition, the condition itself is random. So that's two aspects. I hope I answered your question.

MR. SKILLMAN: No, I understand the distinction that you have made. What I'm thinking about, though, is how do you ensure that the as-designed package is error free?

CHAIRMAN STETKAR: First of all, it's not. It can't be.

MR. SKILLMAN: Okay. So starting there then, how do we resolve this riddle?

MR. BROWN: I'll tell you what they've done. They test and test and test, putting in input and data and data and data, and they run it and they keep correcting the problems until it asymptotically comes down to a constant low-level amount and they say it's good and we have -- whatever defects are remaining, that's what you issue and that's what you've got in your smartphone.

MR. SKILLMAN: Again, let me just respond. So you're down to testing even the smallest piece until you know that that piece is functioning the way you want it to function?

MR. BROWN: Within some --

MR. SKILLMAN: Good enough.

MR. BROWN: Good enough.

MR. SKILLMAN: Good enough. Okay. Well, that's where I was an hour ago. I'm good.

CHAIRMAN STETKAR: Good enough. But there still can be conditions, even though it's functioning good enough, that challenge it to perform in ways that the designers didn't anticipate. And that's the crux. That's the search in the risk assessment is to understand how it's supposed to work.

MR. TOROK: Yes, you're exactly right. I would argue, I would agree that software is not going to be defect free. You shouldn't expect that. But the good news is you don't really need that. What you need is software that doesn't do bad stuff, and that's different. And that's where you get into things like what Charlie was talking about with this simple loop architecture.

CHAIRMAN STETKAR: In a risk assessment, it doesn't do bad stuff at a frequency at which it's challenged to do bad stuff to get you into trouble. You don't design against meteorite strikes, okay? We accept that. We accept the risk of meteorite strikes, even though our plants are not hardened against meteorites. The software doesn't need to be perfect. It has to be good enough to withstand the types of challenges that it's going to be introduced to. If those challenges occur frequently enough, such that it misbehaves in ways that perhaps the designers didn't anticipate, that's part of the process of doing the risk assessment. So, yes, it has errors in it.

MR. TOROK: And there are many things you can do in software design to hedge your bets on that. A good example is, if you're talking about the operating system in a digital gadget and the way it's used to control a real system, you want to make sure that the operating system is blind to plant transients. And what that means is that every time step their operating system does what it does, regardless of what's going on in the plant. And why that's important is that means, on every condition coming from the plant, it can't trigger a defect in the operating system. The operating system is never going to get to its defect because it's doing the same thing every time, regardless of what's going on in the plant. That's an important design feature.

MR. SKILLMAN: Thank you.

MR. TOROK: Right.

MR. BROWN: But the testing to get there can be difficult. I mean, if you take one instrument, a temperature, pressure, whatever it is, and if you had the resolution down to ones or maybe 0.1, 0.2, 0.3 resolution, now there's a set of ones and zeros in a field that represents every one of those states. Try testing that millions of states even with a highspeed computer and feeding that into the system and making sure every field produces the proper response. It's very time-consuming and costly. And that's why when it's good enough and you're putting multiple channels in and that kind of covers the waterfront. You're kind of betting the ranch that one discrepant set of ones and zeros is not going to hit you and disrupt you in all four of them at the same time because no instruments ever read the same all the time. They just never do. You're betting on hope.

So, anyway, do you want to go on?

MR. LI: All right. This digital I&Committee PRA research, the NRC digital I&Committee research plans. And the objective of this research is to identify and develop methods and the tools and, ultimately, the regulatory guidance to include the digital system into current NPP PRAs.

And we already developed a number of deliverable here. In 2009, NUREG CR report on the application of traditional PRA methods to digital feedwater control systems and also the BNL internal technical reports based on the expert panels on the software reliability studies. This was published in 2009, also.

And another BNL internal letter report reveals the surveys on the so-called quantitative software reliability method. This is a summary. And a recent NUREG CR report, 7044, summarized the results on the selection of quantitative software reliability methods and picked up two of them, which BBN, Bayesian Belief Network, and the statistical testing method for further study.

Two NUREG CR reports published in 2016 and 2017. One is the Bayesian Belief Network study and another one, statistical testing studies. And, ultimately, we expect regulatory guidance out from this research.

CHAIRMAN STETKAR: That's the current schedule for those, Ming? '16 and '17?

MR. LI: Yes. '16 is for STM, or statistical testing method, and the '17 is for Bayesian Belief Network report.

CHAIRMAN STETKAR: Okay. Thank you.

MR. LI: This chart depicts this digital I&Committee PRA research programs. This was previous research, and the staff identified some open issues and they proposed the ongoing research on software reliability and proposed future research on digital I&Committee dependencies and common cause failures and also to include some 60 design features, such as fault tolerance, online surveillance functionalities. And out from the current ongoing research and future research, a revised PRA framework to include digital I&Committee component are expected. And after that, a pilot study will be conducted before it reaches regulatory guidance.

And this research, of course, is not a standalone. So we collaborate --

CHAIRMAN STETKAR: Ming?

MR. LI: Yes?

CHAIRMAN STETKAR: Before we get into the piece parts here, you said that the dates for the NUREGs are --

MR. LI: It's here.

CHAIRMAN STETKAR: -- 2016 and 2017.

MR. LI: Yes, it's here, ongoing.

CHAIRMAN STETKAR: Right. When might one expect the final endpoint of this process, that regulatory guidance? I'm just trying to figure out whether I need to worry about it before I retire. No, trust me, as chairman, I don't need to worry about it. I'm thinking, you know -- well, honestly, in some sense, we did have this discussion during the subcommittee meeting in terms of both, functionally, how the piece parts fit together, which I know you're going to get into. But the endpoint being that regulatory guidance, the focal point of this whole effort, it's been going on now for, you know, seven, eight, nine years or more. When might we expect some sort of useful practical output from it? And that is an honest, you know, all facetiousness aside. Are we looking at 2018, 2019, 2025?

MR. SCHULTZ: Does it show up in the five-year research that we described earlier?

MR. COYNE: It's a good question, but I'll say we've trained Ming well because he did give a good answer that it is too soon to tell. And we have been doing this for a while, but it is a very complex research area. But I'll say we're very pleased and optimistic with this statistical testing work. That project actually has gone quite well, and we moved that up in advance of the BBN work, which we actually had the priorities of those research projects flipped. And then when we saw how well the statistical testing work was coming together, we decided to put a higher priority on that.

CHAIRMAN STETKAR: Yes, I think that's the first that we heard. Back in November, I'm not sure where they were in the --

MR. COYNE: Right. So you've seen the draft report on that, and Ming is going to talk about some of the redo of the testing that we did to further improve the approach we used. So that work is gelling together. Ming said '16 to publish it. You know, the report is going to be ready this year. It just takes a while to get through the publication process.

CHAIRMAN STETKAR: Okay.

MR. COYNE: The BBN work, which he'll also brief you on, is going quite well. It's been a very fruitful collaboration with KAERI and KAIST, who has a lot of experience in doing this kind of software reliability work. We'd like to make that a joint report with our international colleagues, and that might take a little more time to get through the publication process.

So, honestly, the FY 16 for the publication is probably accurate, but we expect to get that report pulled together within the next 12 months to a pretty good state. And then --

MR. BLEY: Are we talking that that might be an CSNI report, as well as NRC, or something else?

MR. COYNE: It would be, it would be similar to what we've done with some of the fire work that it's a joint NRC/EPRI, except it would be -- we'll have to decide if it's a NUREG IA or some other designator. But we want, we're moving forward with getting that report finalized.

Then the big question we've always had is is this practical and useful? Do we get good insights from the work? Is it practical to do? Is the information available? And, honestly, that's been a big challenge for us. The level of information we need on these systems and dealing with the proprietary nature of what's in the system and the software development cycle and that type of information that we actually need to implement the method has been very challenging. We were very fortunate to have Idaho National Lab come forward and volunteer the advanced test reactor loop operating control system. Honestly, we were at kind of a dead end until that came through, so that's been very fruitful for us to have that available to us.

When Ming mentions that pilot study, that's going to be a big challenge for us to figure out how we're going to do that pilot study on a real realistic system. So we do have a target. We have the pieces really starting to come together. I can actually begin to see the light at the end of the tunnel on this. It's just I'm not sure, we have to come to the conclusion whether it's practical and useful with these methods and then how we're going to put the rest of the pieces together for things like a pilot study, which I really think would need to be done to have good confidence that whatever regulatory guidance we propose is appropriate.

CHAIRMAN STETKAR: I think, you know, we've learned a lot about the need to do realistic pilot studies in any proposed methodology. I'll mention NUREG CR 6850 and the fire analyses as one example. The experience has been, I think and I would hope going forward, is that if, indeed, the outcome of this process seems to be a practical methodology that is endorsed both by the staff and, if not endorsed, accepted by the industry, there may very well then be a licensee who steps up to use their plant as a pilot, which is then obvious the need for the staff to obtain directly the proprietary information in a real system at a real plant. And, of course, there aren't going to be any volunteers for that, unless there's some evidence that, indeed, the methods are practical.

So getting to that center part there, the revised PRA framework, is certainly a necessary goal. And I was mostly trying to challenge what the timing on that is. Okay, thank you. Sorry to interrupt. I know you want to talk about the piece parts but . . .

MR. LI: Let me quickly finish this chart. As I mentioned, this work got a lot of collaboration under MOUs with EPRI and with NASA and the international collaboration and the bilateral with South Korea and also with NRC. And we got a lot of support from the Division of Engineering on the failure mode, on the operating experience analysis data collection, and also on the digital system inventory and the classification studies.

I want to quickly summarize our research in the past. For the hardware on the system-level reliability modeling, Ohio State University worked together with ASCA and the University of Virginia, applied some dynamic reliability modeling method, such as the Marco Chen methods, to digital feedwater control systems and they published a number of NUREG reports in the 2006 to 2009 time frame. And the BNL also applies to some traditional reliability modeling methods, such as FMEA, they call it revised FMEA method, to the same systems and they published their results in a NUREG report in 2008 and another one in 2009.

And if we go back further in the history, Ohio State University developed the so-called metrics-based studies for software reliability modeling. So, basically, this started, like, 40 software metrics and expert panel ranked those 40 metrics with respect to their capabilities of estimating software reliabilities and then developed 12 software reliability methods from those 40 metrics to verify the ranking. And there are some results from that, and they published the results in the GR report and two NUREG CR reports.

And the ongoing study conducted by the BNL, the national lab, and the NUREG CR 7044 that's already published summarized the expert panel results and the philosophy, the foundation of the software reliability work and also identified two candidate methods which I mentioned, the Bayesian Belief Network and statistical testing, and applied that with a collaboration with Idaho National Labs to apply those two methods to estimate software reliability so that ATR, advanced testing reactors loop operating control systems. I'm going to talk a little more in detail later.

This research also got a lot of support from the international partners, including the South Korea, the KAERI and the KAIST colleagues. They provided a lot of valuable support on the STM method, which they practiced in the past. And also they're actively involved in the Bayesian Belief Network research. They provide the algorithm and they provide the models and the execution of that to support BNL's study on this.

And, furthermore, the PECD also worked on digital I&Committee PRA areas. So there are two reports published: one on the failure mode taxonomy published last year and there's another recommendation on digital I&Committee PRA published in the year 2009. And there's an effort called a COMPSIS, computer-based system important to safety project, spanned from 2005 and 2011. There's not much output from it because only the U.S. contributed to the data, so it's a pity.

Next, I'm going to talk about the ongoing research on software reliability, which is the focus of today's presentations. The first one I'm going to talk about is the statistical testing method. We already talked about software testing here a lot, but this statistical testing method is different from the functional software testing. In short, this statistical testing method tried to estimate the failure probability of the software instead of trying to prove the correctness of the software.

So in order to do that, I mentioned that software failures probability could be zero or one, depending on the input. So if you select a failure of an input, you can prove the software, you know, never failed. So as I mentioned, software reliability is a function of the defects and a function of operational profile.

So in order to test software in the PRA context, it's important that, I call it the testing conditions, and, fortunately, the PRA can provide the information, the software and the test, the conditions, and we call that, again we call that operational profiles. And, also, the PRA insight can help to determine how many test cases is good enough. Think about --

MR. BLEY: Can I interrupt you at that point just a second? You use the PRA to define these conditions. However, there are lots and lots of cut sets evaluated by the PRA, so you're using some kind of a screen to find them. My concern would be that the kind of failures we might see here could elevate otherwise very unlikely cut sets up to be more likely through some kind of common effects. How did you try to look for that kind of problem and make sure you've got the cut sets that might be most important?

MR. LI: Okay. First of all, what the BNL did was to rank the cut sets, according to their likelihood.

MR. BLEY: So based on some assumption of failure rates?

MR. LI: Yes.

MR. BLEY: Okay.

MR. LI: And they picked up about 10,000 cut sets.

MR. BLEY: Okay.

MR. LI: And then they used those 10,000 cut sets, defined 10,000, RELAP5 starting conditions. Then they execute the random simulations because the simulation generates all the plant conditions. Those are the inputs to the software and their tests. I hope this answered your question.

MR. BLEY: Well, a little. Doing it that way, depending on how they modeled or you modeled common cause among these things, through the common cause you might have elevated higher-level cut sets so that we make sure we see them. And if you don't do that, you're seeing primarily the higher order, the fewer element cut sets. And if you do it that way, then at least one ought to look and see if, when you go through this testing, you see some of the highest order among the set that you actually use showing up in important results, which might lead you to have to dig further. Did you take either of those two approaches?

MR. LI: Well, I'm not sure I'm the right one to answer your question. Definitely, I can pass this question to BNL. As far as I know, well, of course, the quality of this statistical testing work depends on the quality of the PRA. So what BNL did, they have the PRA from Idaho, they have the PRA from Idaho, so their cut sets are based on the Idaho PRAs. So I believe Idaho PRA, they addressed the common cause. They basically went to address all the common cause.

MR. BLEY: I'd be real interested in being able to see some depth on that at some point to help increase confidence.

MR. LI: Thank you. I just talked about the testing process. So, basically, BNL used PRA models from Idaho and generated the cut set, the 10,000 cut set, and then it ran the RELAP simulations for those 10,000 conditions, then produced the test cases to the LOC system and then passed those test cases. So you can imagine, you know, for each condition, there might be 10,000 inputs, so 10,000, all those data points, pass all the information to Idaho. Then Idaho automatically have the actual LOC systems and then provide all the test results back to BNL.

It's very interesting that the results, if we take a look at the testing results, before the November ACRS subcommittee meetings, BNL identified a large number of, they called it anomalies. It's either early or delayed trip. Early means that the trip occurs earlier than it should be, and a delay in the trip, of course, it's a couple millisecond or, you know, a half second after it should be tripped. And we examined those results, and then we figured out that BNL introduced some artificial noise to that test data to mimic the actual operation, which means the noise from the sensors. Then that introduced an additional layer of uncertainties because, you know, for instance, the inputs to the software might be 4.01 and that might lead to early trip. So after we realized that, then BNL regenerated, removed all the artificial noise.

CHAIRMAN STETKAR: Ming, you characterize this as artificial noise because you're trying to have a perfect laboratory setting here. In the real world, there really is noise. So by removing what you characterize as artificial noise, have you removed this one step from the real world?

MR. LI: Well, this is software testing. I completely understand your point, but this is software testing. So we have to know exactly what the input value is in order to decide whether the output is right or not. So you have to have that clear. You need to remove that uncertainty. For instance, if the input is 4 and the input becomes 4.01, then the software trips. So you never know is this a software error or error caused by the input noise.

And, in reality, yes, you're right. So the sensor introduced noise. But then that becomes part of the plant. So within that threshold, the system need to trip. Even the plant condition, not there yet, but for the conservative consideration they trip that. But, in our case, we have to be able to tell exactly what the input is in order to decide whether this is a software error or --

CHAIRMAN STETKAR: What I'm trying to figure out here is are you trying to create a spherical chicken?

MR. LI: I'm sorry. I don't follow you, the last word.

CHAIRMAN STETKAR: It's an old joke. Look it up. You cannot predict how a chicken can fly unless you simplify it to the point where it's a perfectly spherical chicken. And that's, obviously, a useless piece of information.

What I'm trying to understand is you're saying, well, we had these artificial noise that Brookhaven introduced because they wanted to simulate the effect of differences that might be in the plant, and we didn't like that so we threw that away because we wanted to take a more purist approach to just the software. My question is what is the use of just having an artificial purist notion of the software under conditions that it probably never will really see in the real world. We'll always see some sort of noise.

MR. LI: Well, they are two different things. We are talking about the input. Now you're talking about a pure system. So by input, I mean -- well, let's talk about software testing.

So in order to test a software, you have to know for each input what the expected output is. If you don't have that information, you cannot tell whether your test is successful. So you have to be clear, there should be no uncertainty for input. If the input is four million, then it should be four million.

MR. BLEY: I agree with you, provided you keep careful note of this because, when we operate in the real world, the problems in software-driven systems might not be problems in the software. There might be problems in the input information that's outside of what we've tested and outside of what we expect. And that might be the main source of the risk. We don't know for sure yet. So step one in your testing makes sense to me, but don't forget the other --

CHAIRMAN STETKAR: In a sense, you're right. Step one in the testing is just to try to get that pure notion. But step two of the testing would then be to introduce noise and find out how sensitive --

MR. LI: A statistical testing. We tested the LOC system. Now you're testing, it's a broader system --

CHAIRMAN STETKAR: No, no, no. Test your LOC system but with the noise and those input signals.

MR. COYNE: Kevin Coyne from the staff. There was a statement you made that I want to correct. We're not throwing away the initial data. In fact, we thought that was a more realistic portrayal of how the system behaved. But when 10 percent of the test cases fell out of the range we expected, we realized we had to do more work to understand why that was the case. And when we did the initial round of testing, INL calibrated the LOC system as they normally would calibrate the actual operating LOC system using their normal procedures and normal calibration tolerances. BNL introduced some additional noise on top of the RELAP output to represent what they expected real instrumentation would experience, and then we had this issue with 10 percent of the cases. We felt it was due to the input errors that were being sent into the software, but it's hard to prove that. So the idea with the second round was we were going to calibrate everything as dead-on as we could get it, and INL actually could do a fairly good job at really getting the calibration of the analog-to-digital setup and the processing setup very well and removed the additional noise. And so now we're getting a much cleaner set of test cases with the second test.

So I think both sets of tests give you valuable information to how the system is performing. If you're focused solely on the software, a cleaner set is more representative of software, and the messy set is probably more representative of how the system would actually behave. So I think they both tell us something that's valuable, and it was a learning experience for us going through this process.

MR. BLEY: Okay. To me, that makes some sense. I'd also ask is the only function of the ATR LOCs to create a trip, or does it do other control functions?

MR. LI: Other --

MR. BLEY: Are you looking at those? Are they being affected? You're only looking at the one function?

MR. LI: We isolate the functions, yes.

MR. BROWN: Dennis, to the point, I

understand what you did trying to isolate the thing. But what we did, and just based on experience, we had the same circumstance. The fundamental problem of going from analog to digital, the digital was a nice crisp signal. But if you're a-to-D conversion had variability in it, then you had to design the system to account for that variability. So you didn't get the 10 percent unusual triggers.

So there's a way to use both sets of data or information in order to end up with a system that is reliable and functionally repeatable, which was the important, the key issue here.

MR. LI: I totally agree. But, unfortunately, in this case, our capability to study the system is limited because the proprietary system, we don't have document and we don't know how the system was designed, what's the part number, what's the, you know -- all the information we don't have. So even further LOCs is not safety system, per se.

MR. BROWN: No, another comment I was going to make is that there's a difference between the control systems, the feedback control system, and just a straight-through trip or don't trip type system.

MR. LI: Yes, I totally agree.

MR. BROWN: You just got to take that into account. You've got to do things in a control system that you wouldn't necessarily do in a straight-through safety system, in terms of accomplishing your final function.

MR. LI: Sure. Thanks. Well, another very useful feature we added for the second round of testing, we introduced what we call synchronizing timing signals during the first testing. So there are trips there, but we didn't know this trip was caused by which input signals. So now we have the timing signal. There's a pulse there. So from the input, then we know the output, the pulse continues and then we can count where the input signals, which input signal triggered that, caused that trip signal.

There were still 45 delayed trips and the 16 early trips. And the preliminary analysis on that, and Idaho agree with that, is that all the trips were caused the A-to-Digital I&C converter. It's still the revolution. Very small input errors caused early trips or delayed trips. It's like a 0.01 percent of the input range.

CHAIRMAN STETKAR: Ming, I'm assuming that, we discussed in November, mischaracterized it as an anomaly that you couldn't reproduce, one event where it actually never tripped. Delay was, like, infinite.

I'm assuming you haven't experienced that again?

MR. LI: No.

CHAIRMAN STETKAR: Okay.

MR. LI: That failure never repeated.

CHAIRMAN STETKAR: Never repeated.

MR. LI: Never repeated.

CHAIRMAN STETKAR: Okay.

MR. LI: Another ongoing research on software reliability, the Bayesian Belief Network. As I mentioned, that software failure defect there and the operational environment triggered those defects. So it would be useful to know how many defects in the software and then from the number of defects to the failure of probability by introducing the operational profiles. And this BBN approach, basically, established the causal relationship between what we call the software development or software product characteristics -- we call, each one is a node -- that causal relationship between those nodes to the number of defects in the software.

And this research heavily relied on the expert opinion, unfortunately, because the lack of data. So we don't have any adequate data, so we used three rounds of expert opinions. Our first round established the set of attributes and then the column network. Then the second round of expert opinion is used to quantify those causal relationships, what we call MPD tables. And the third round, we applied those networks to the ATR LOC systems, so we were utilizing the expert to provide input to each attribute because we are not developer of the system, so we are not very familiar with the systems.

And this chart is just a demo. This is not the actual network. This is just for demo purpose.

So the path forward, as I mentioned, we're going to publish the statistical testing method report next year.

MR. BLEY: Are you considering whether it might be a good idea to kind of put the two methods together, use statistical testing method to develop some estimates of parameters and then use the Bayesian Belief Network as the real model that you update with the results from the testing?

MR. LI: This is already under consideration. And, furthermore --

MR. BLEY: I kind of thought that's what you had said the last time, but I think it's really, it allows you to pick up things that maybe you didn't pick up in testing until we gathered much more experience.

MR. LI: That's a very good recommendation. Thanks. And, furthermore, normally, the BBN results served as prior information to Bayesian upgrades. So based on the BBN work, then we can estimate, a rough estimate, the failure probability. Then we can better do an STM, using STM, so it upgraded the STM results. So there are multiple ways that we can, you know, play on the numbers.

So we're going to publish the STM NUREG report in 2016 and the BBN report after that in 2017. And we're in the process of updating the digital I&Committee research plans to reflect the next stage of the digital I&Committee PRA work.

MR. BLEY: I lost track of what Kevin said. The BBN report, it's going to be an international report, or both of them?

MR. COYNE: It would be a NUREG publication, but we would cross-batch it, hopefully, with KAERI.

MR. BLEY: And that's the BBN?

MR. COYNE: That would be the BBN work.

MR. BLEY: Okay.

MR. LI: So the research plan is going to include the software failure data collection. We still need to continue collecting data on hardware failures, and we continue working on the software reliability modeling work. And we're going to start the digital I&Committee dependency modeling. And we also need to model the safety design features, such as the floor tolerance, online surveillance, so forth and so on. And, ultimately, we're going to develop the reg guide.

And this concludes my talk. Any questions?

CHAIRMAN STETKAR: Any further questions for the staff? If not, EPRI has prepared a presentation. Anything for the staff? Thank you very, very much. Ray, you're up.

MR. TOROK: Am I driving, or are you?

CHAIRMAN STETKAR: This is a low-budget operation. We can put you in the car and on the road, but you have to drive.

MR. TOROK: Okay.

MR. BLEY: Ray, before you even start, the work NRC just described to us, especially the testing and the BBN, you guys aren't directly cooperating, I don't think, but you're following?

MR. TOROK: Yes.

MR. BLEY: Any comments you have along the way would be helpful, and your paper is on the microfilm.

MR. TOROK: Sorry about that. Yes, well, we periodically meet with NRC research under a memorandum of understanding where we share information on what each of us is doing. So in those meetings, we hear about it and we comment on it and maybe we'll raise questions as to things that ought to be addressed in what they're doing, those kinds of things. And then they do the same for us. So in that sense, yes, we know about it, but we're not involved in the research --

MR. BLEY: Okay.

MR. TOROK: -- at all. Okay. So moving right along now, as you know, we presented material to the I&Committee and PRA subcommittees back in November, and this is, today is an overview, a brief overview of the same topics we covered there. This list shows those same topics. So there's something on failure modes; modeling digital in PRA, what we've done; and ways to deal with potential failures in terms of prevention and mitigation; and hazard analysis. We talked about a demonstration project we're doing with Palo Verde and, you know, where they were and information from that. So I'm going to just briefly hit each of those things.

Overall, the so what is that, you know, all this work we did started in a way with this notion that, with digital systems coming in, there's potential for new failure modes, including common-cause failure. That was raised as part of this SECY 93087. And in a way, this concern about new failure modes and so on for digital pushed a lot of things. So we've been working on that for several years now.

And the same things we've been talking about, failure modes and how do you protect against the failure modes and, you know, what can you do about that. Our understanding now is much better than it was when the SECY was written and since the industry standards have come a long way. There's been multiple iterations of some of them. And this notion of what do you do with digital in PRA, we've been playing that game for several years now trying to understand what kind of insights we can get, what the limitations are, those kinds of things. And then this notion of hazard analysis, or failure analysis some people call it, because that turns out to be very useful in terms of identifying potential vulnerabilities and understand what you can or cannot do about them.

So from our position, it may be now that the SECY 93087 has seen its day and it's time to think about applying the more recent knowledge and the work that's been done since then. It's been 20-something years. I mean, really, it started before 1993. And EPRI's role in this has been to develop methods and guidance and so on that can support the utilities. The utility engineers are our audience for the most part. And the idea is that if we can provide good technical guidance that's practical to use and so on, that's a good thing for them. Sometimes, it comes down to communicating the tech transfer issue, especially if it's something new. That can create problems by itself. So we do that, as opposed to discussing regulatory implications, let's say, and arguing about what's a good or defensible licensing position. That's somebody else's job.

But the main point is we know a lot more about this stuff now than we did, you know, 20 years ago. Any comment or --

Okay. So failure modes, just real brief because I think Mauricio already addressed the topic. But this issue of what's, you know, are the EPRI and NRC research treatments really compatible in a couple of areas. One is what are the words themselves? You know, do we understand each other? And is the coverage comparable? And I put the phrase in there "level of interest." Some of you may remember our level of interest diagram from the last time we talked, but the idea is that, if you look at the plant, there are various levels of interest you can consider from the I&Committee and the software embedded in the I&Committee at the bottom all the way up to plant systems and the overall plant safety at the top. And you want to understand where you are in that hierarchy and what you care about, what you don't care about. That becomes important in terms of understanding what you can do and so on and how to deal with potential failure modes and so on.

Overall, it's important, I think, that we're communicating when we talk about failure modes, failure mechanisms and effects, and so on. And in the MOU discussions with NRC research where we get into that in some detail, our conclusion was we understand each other pretty well and we're pretty much on the same page throughout, you know, even when we're using different words. So that's okay.

Now, for us, the words are important and understanding the modes, mechanisms, and effects are important in all of this stuff, in hazard analysis for sure, in how you're modeling things in PRA because there are, as I said, multiple levels going on here.

We already mentioned these periodic meetings. Those are under the memorandum of understanding.

I wasn't going to go into anymore detail than that on this issue because I think it's already been presented and discussed.

CHAIRMAN STETKAR: But, again, presented and discussed to the subcommittee, so most of the rest of the folks haven't heard about this.

MR. TOROK: Well, the main issue was are we on the same page in terms of understanding, and I think Mauricio addressed that earlier, so I wasn't going to go anywhere with that.

Now, this is the next topic on that list, modeling digital in PRA. And this is something that we started working on in 2004, so it was quite a while ago. And there are a number of what I call hot-button issues tied to modeling digital in PRA. This notion of diversity and defense in depth, what can PRA help us with there?

And the reason that's driving this was because some guidance on the street was looking at the need for diverse backups for the I&Committee to deal with certain events, and I guess the leading one was a large-break LOCA where you're worried about low-pressure injection and you've got multiple trains of low-pressure injection with the same software in each train and suppose there's a bug in the software that defeats all the trains. Wow, what am I going to do now? And you end up in a situation where you're talking about a diverse backup for the initiation of low-pressure injection. And some pressure rises, that's all well and fine. But what does the PRA tell us about that? Is that a good idea or not? And I'm not talking about a detailed understanding of failure probabilities. I'm talking about risk insights. And so you want to be in a regime where the risk insights are not sensitive to specific assumptions you've made in your analysis.

And so in this case, if I talk about large-break LOCA and diverse backups, I'm talking about a combination of a large-break LOCA, which is a relatively rare event, with a common-cause failure in the digital control system, which is a relatively rare event, and the PRA would say, wow, that's a really rare event. And, you know, so you end up in this discussion of whether it's beneficial to do that. So we got into that discussion.

The notion of estimating failure probabilities, we've been talking about that. We looked at a number of ways to do that based on design measures built into the software and the digital system or attributes of the architecture that can help add some protection based on some data from French plants in terms of their experience with microprocessors and a lot of safety systems for a lot of years. We did some of that. This notion of modeling level of detail, we looked there again.

And this is where you get into the thing we talked about earlier today: failure mechanisms versus modes versus effects. Where are you in the software? What is it you really care about? And this notion that the software by itself doesn't do anything directly. It controls some component which is part of the system, and you care about the system functionality. And, typically, with the PRA, you're talking about what's the system doing and what are the key components in the system doing, not necessarily what the I&Committee is doing. Although I shouldn't be so glib about it. The I&Committee can certainly become a factor there. Anyway, so we have spent some time looking at that and the effects of the level of detail.

The latest EPRI publication on this is that -- the titles here, "Modeling Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk

Assessments," and that was published in 2012. This figure on the right is a figure out of that report, and I don't want to encourage everybody to read all the fine print and we're not going to go through all those steps. The point is that it proposes a systematic nine-step process to model digital instrumentation and control in PRA, but what's more important is it pushes for a team effort between the I&Committee guys and the PRA guys. And so certain tasks, the I&Committee takes a lead. Others, it's PRA, and some may have to work together to do it. And this came out of a lot of discussions in our projects where it was really clear that, typically, the I&Committee guys in the plants and the PRA guys don't communicate very well. They're talking different languages. They don't necessarily want to be bothered with each other, that sort of thing. However, our position was that the PRA guys really had a lot to offer in terms of helping the I&Committee guys understand the risk significance of what they were up to and where they can get into trouble. And we wanted to make sure they were taking advantage of that.

You know, the I&Committee guy will say something like, wow, my I&Committee here is really important because this is a safety system. And the

PRA guy might look at that and say, well, yes, okay, but it's nowhere near as important as the feedwater system, right, because the PRA guy is seeing the whole plant and the I&Committee guy is focused on his I&Committee. So we were trying to get past that, so that's why there's this note here about the I&Committee in the context of the integrated plant design. The PRA guy can help them understand that, and I think that's important.

The next one, though, defensive measures for I&Committee, that's an I&Committee guy kind of thing. The I&Committee guy can help the PRA guy understand -- we're okay?

CHAIRMAN STETKAR: Just ignore it.

MR. TOROK: Okay.

CHAIRMAN STETKAR: If you can. It happens. It's our sophisticated system.

MR. TOROK: Okay.

CHAIRMAN STETKAR: But it's predictable Byzantine behavior. Go on, Ray.

MR. TOROK: Okay, okay. Wow, I forgot where I was. Defensive measures. Okay, yes. So the I&Committee guy can help the PRA guy understand what's going on in the software that affects the failure probability. Initially, when we started talking to

PRA guys, you know, they'd say, hey, just give us the data, we know what to do with the data. And I&Committee guy would say, oh, you don't understand, this software is not like that, it doesn't wear out. We have to look at it in a different way.

So we get into that whole thing. And somebody mentioned this earlier, this notion that software doesn't wear out and the failures, if we can call them failures -- a loaded word there -- it fails deterministically, but it fails in unanticipated conditions. When software is operating in anticipated tested conditions, it's pretty darn bulletproof. When it gets into trouble is when the going gets weird. And just about --

MR. POWERS: Apparently, any time it flies near Pluto.

MR. TOROK: All kinds of things. And there are a lot of stories about this, right? There's an air traffic control system that was used successfully in Denver for many years exported to the UK. It turned out it didn't work at all there because it didn't understand the difference between east and west longitudes, which doesn't matter in Denver, right? But it makes a big difference in London, right, because the Prime Meridian is right there. But, again, the software designer knew he was building a system for Denver. He didn't care about east and west longitude.

Anyway, so that's just an example of anticipating conditions where you get stuck --

MR. BROWN: Before you push your finger down, you said it behaves deterministically. It doesn't behave deterministically unless you design it to behave deterministically. Let's say if you wanted to pull my chain a little bit, you certainly did.

MR. TOROK: Okay.

MR. BROWN: If I did not react, I would ruin the entire overview of the entire meeting.

MR. TOROK: I think I know what you mean, and what I was referring to was the notion that, whenever software sees the same set of conditions, it will react the same way. And when you get into this deterministic discussion is when you're talking about --

MR. BROWN: That's not the same. Bad word.

MR. TOROK: That's a different, that's a different application.

MR. BROWN: That's the wrong word.

MR. TOROK: I see what you mean. Next time, I guess I need to straighten that out so that you can't comment.

MR. BROWN: No, it's not a matter of me commenting. It's a matter of people getting the wrong perception of what reality is.

MR. TOROK: I understand. Yes, and that's an interesting comment because there are different uses of the word deterministic as it's applied to software. Different people mean it different ways. And you're right, I created an unnecessary --

MR. BROWN: But you can go on now, please.

MR. TOROK: Thank you. Okay. So, again, in our world, it's not about the numbers and the failure probability and those kinds of things. It's more about the insights you can get from this.

And so, as I said, where you want to be is in a situation where I can vary the failure probability, the same failure probability to digital I&Committee by two or three orders of magnitude, and the risk insights remain the same. And then I've learned something about what's important maybe and what's not.

An example of that might be, just for comparison purposes, the one I was talking about earlier, large-break LOCA plus a common-cause failure in the I&Committee. Pretty darn low probability and, in fact, it doesn't really matter what you assume about the failure probability of the I&Committee. It's not going to be a large contributor to core damage frequency, okay?

However, if you do things like introduce the possibility of a common-cause failure that can affect multiple mitigating systems for an event or can affect both the initiator and the mitigating system, now you have a big impact on core damage frequency and you need to watch out for that and you need to be aware of that. Those are good insights, and you can find those without using numbers, so that's a good thing.

MR. SKILLMAN: Ray, let me ask you this. I understand the words that you just used, but I will tell you from experience if the I&Committee system misbehaves, while one might predict that the core damage frequency is low, what that I&Committee failure does is drives the operators into situations that they might not have been in before and the permutations and combinations of what those operators can do becomes an issue, and they may not do what they should because they've been thrown a curve ball by the behavior of this otherwise very reliable I&Committee system. And so one might say, based on the PRA, there's very little core risk, core damage risk. If the operators are put in a situation where they are perhaps beyond their training, there is a different outcome for that event.

MR. TOROK: So in other words, you're saying that if it creates an unanticipated condition for the operators, that's a potential, that could be a real problem.

MR. SKILLMAN: That's what I'm saying.

MR. TOROK: Yes, okay. And I agree. In fact, one of the things that keeps coming up -- our PRA expert is Dave Blanchard. Many of you know him, I think. And he's been trying to teach me this stuff for several years now. But one of the things that he keeps harping in is that in a lot of events the operator really is the best backup for the systems.

So if you do something in updating I&C systems, that somehow creates an event and disables the indications that the operator needs, now you've got a real problem. So it's important to make sure you don't do things like that. In our technical work here, we're trying to make sure that we alert plant engineers to that kind of thing.

Another thing that we've seen here that's kind of interesting is you can look at, in the PRA you can look at what kinds of reliability, what it has to be for the I&Committee to end up being a small contributor to risk compared to the hardware that's in the systems. And in some of our work, what it turns out is that lots of times the I&Committee reliability targets are pretty modest compared to what you should be able to get from digital equipment.

It's also very useful or can be very useful to look at the proposed I&Committee mods early in the design process before they're installed because PRA can identify potential vulnerabilities that you could get into based on the conceptual design and can help avoid those kinds of things early on. So we've seen cases like that.

It's also, another insight here is this notion that you can, if you did your job on the I&Committee, basically the PRA is going to be insensitive to what it's doing. And, typically, that means the I&Committee, the digital I&Committee should be at least as reliable as that of a comparable analog system. And, usually, the digital I&Committee is better than that for reasons like what Charlie was talking about earlier. And in many cases, what happens, especially in non-safety systems where one of the goals is the digital upgrade is to reduce the incidence of failures coming from that system.

So what the engineers do is they look at all the failures that system has had and intentionally design the digital system so it can't have those failure modes. They design those failure modes out, and that has been very successful with things like feedwater systems and turbine control systems. So that's a good thing.

CHAIRMAN STETKAR: Ray, I think some of the feedback that we've been trying to give the staff and, to some extent, the industry is that you constantly present this in the sense of not doing what it's supposed to do. The problem is that we've seen is that when it does things that we don't expect it to do, those misbehaviors. We used that phrase. And that's the real challenge. It's not -- and everybody compares it to the old analog systems as if they were perfect. The analog systems, our experience is, until people started to look at fire analysis for example and think carefully about what combinations of spurious signals could set these systems off on trajectories that nobody even thought about in risk assessment. The designers hadn't thought about it because they weren't forced to think about those combinations of failure modes, and the risk assessment people traditionally hadn't thought about them because they were only looking at not doing what it was supposed to do.

And one of the things we've learned from doing comprehensive fire analysis is, indeed, the analog systems misbehave also. It's just people hadn't thought about it before. And part of the message for going forward with digital systems is don't fall in that same trap. We've learned the message, the lesson that looking at only not doing what it's supposed to do may not very well be the source of the problem. It's doing things that it ought not to do.

MR. TOROK: Yes, yes, you're --

CHAIRMAN STETKAR: So I just, you know, I want to make that statement on the record because I think that's the real challenge.

MR. TOROK: I agree. And a common complaint about digital is an engineer, let's say, had to specify requirements for a new digital system that's going to replace an analog system, so he gets out the requirements for the old analog system, dusts them off, and gives them to his supplier who says got you covered, no sweat. What he gets is a system that does everything the analog system does and it does a lot of other things that maybe you didn't want, right?

So I agree. That's --

CHAIRMAN STETKAR: And most of the time, it doesn't do those things, so you don't discover it until you get to a situation when it's not a good day.

MR. TOROK: That's right. And one of the things that we push for in terms of encouraging people to understand their system before they put it in the plant is look into that stuff. That's right.

Okay. Where am I? This is the new, a new topic here. Well, we've talked in this presentation the same thing we talked about last time, techniques for failure prevention and mitigation. And this is an ongoing project now, and it's about our understanding and managing, let's say, potential digital failure modes and misbehaviors and so on, including common-cause failure.

Now, I think you've heard about a project that I guess that NEI is pushing this. It has to do with the 50/59 rule and document in any IO 101. Does that ring a bell for anybody?

CHAIRMAN STETKAR: No.

MR. TOROK: Okay. Well, that's good. Maybe that simplifies things for me. The point is that there is some guidance out there. NEI is working on updating it. This work is intended to be technical basis input for that, and so there is a relationship there. And I know Christina has been asking me about it so --

CHAIRMAN STETKAR: Given the answer is no, what is NEI's schedule for that, do you know?

MR. TOROK: What is NEI's schedule?

CHAIRMAN STETKAR: Yes.

MR. TOROK: I think they expect to have some draft guidance out late this year.

CHAIRMAN STETKAR: Late this year.

MR. TOROK: But don't hold me to that because I don't really know.

CHAIRMAN STETKAR: That's good enough. Thanks.

MR. TOROK: We're having periodic meetings with them to explain where we're headed and they explain to us where they're headed and so on. Anyway, so the point of this thing now is to produce guidance for addressing, as I said, the failure modes and misbehaviors and so on, which, of course, plays into licensing space at some point because you want to convince yourself that you do have adequate protection against those things.

We're using earlier EPRI reports, lessons learned, where we've addressed bits and pieces of this thing. We wanted to or we are addressing both safety and non-safety applications in traditional licensing space. They worry more about the safety side. And our guideline is intended to be out late this year; and, hopefully, we'll hold to that.

The approach here is what I consider a little more holistic than some traditional approaches that are used in regulatory space. And what I mean by that is one way to look at potential failures in CCS is to assume they happen and be sure you can tolerant them. And that's all well and fine in one sense. The problem from the EPRI standpoint is if you just do that, you're not maybe paying enough attention to the good engineering that goes into the plants to make the failures unlikely or to defeat them because, from an engineering perspective, you're better off if it never happens. So you want to make sure you're taking the right steps to do what you can to make sure it doesn't happen. And that's what this notion of preventive measures is really about. What can you do with your system to make sure, not to make sure but to reduce the likelihood of failures, misbehaviors, CCS, and so on.

The coping analysis is a demonstration

that, should the failure occur, you have adequate mitigaiton. And, of course, if either you decide that your failure likelihood is too high or the coping analysis says you get results you don't like, you can go back and you should go back and redesign your system to reduce those things. Or another way of looking at it is to increase the overall protection against the failure.

In the end, it becomes somewhat qualitative. You look at the preventive measures you have. You look and see what the results are if the bad stuff happens and ask yourself have I got adequate protection? There's the notion of adequate protection in an engineering sense, and there's the notion of adequate protection in a licensing sense. They're not necessarily the same.

What you do want to do in our world is document what you've done in an assurance case where you're effectively making claims about why you think the system is okay and what evidence you have to back that up. That's what that's a reference to.

MR. BROWN: Before you leave that, you say it's a guideline. But I'm trying to figure out, you didn't say what type of information is going to be in this guideline. Is it just here's some good thoughts and lessons learned, or is it going to be translated into design guidelines or dos and don'ts, or is there a framework? I mean, if you're going to publish it this year, that should mean there's a framework of what point you're trying to get across.

MR. TOROK: That's right. And it's really a step-by-step process where you assess the potential susceptibilities. You look at also how risk significant they can be, and you look at what kind of defensive measures you have in place to deal with the potential susceptibilities and whether there's a need for more. And if there is, you go back and reassess your conceptual design and start over, you know, and reiterate.

So it is intended to be a step-by-step process where there are various --

MR. BROWN: But is there an overriding message you're going to be trying to send, like make it simple?

CHAIRMAN STETKAR: Let's get away from I&Committee design and guidelines that might go into NEI guidance and keep focused on PRA because we've got about seven minutes left and PRA is the subject of the briefing.

MR. TOROK: We can talk more about it. The concepts that go into this are considered here. The notion that you care about protection against the failures in the CCF, and that means some combination of prevention and mitigation. We want both.

I think we talked about this earlier, this notion that software failure needs a defect in the software, a fault, a bug, whatever you want to call it, and some trigger, which is typically unanticipated conditions that can activate the defect. And the reason that's important is because, in developing a system, you've got a chance to affect both of those quite a bit. In your good software development processes and so on, you can reduce the likelihood of the defect. You can also institute design measures that are there to avoid triggers. And we've talked about some of those things already today, you know, cyclic architecture, data validation, those kinds of things.

This notion that you can generate protection at various levels. One is to put in features in the software, like diagnostics and so on. Another is to do it at a higher level. If I'm talking about a fuel-handling crane for example and I'm worried about it running out of bounds, I can do things in the software to check the position against where I want the thing to stay, but I can also put hard mechanical stops on the fuel crane so it can't overrun no matter what the software is telling it to do. Maybe I want both of those things. So you end up considering things like that.

Common-cause failure has a lot of different flavors. In 93087, in the olden days, it was about identical trains of safety equipment that all have the same software in them and you can defeat the whole system with a bug. But there's more to it than that, and that's what this cartoon is trying to show you. Here there are, on the upper right there, you use the same digital platform to update multiple non-safety systems. Each one is programmed a different way because it has a different application going on. They all communicate over a bus, and each of them is controlling multiple components. And that introduces all kinds of interesting possibilities in terms of common-cause failure. Suppose I do something to the network that affects all of the systems at one time. I can talk about spurious actuations coming from multiple systems at the same time. The point is there's a lot more to it than simply identical redundant trains in safety systems, and we're trying to make sure we cover those things, as well.

Ultimately, it ends up an integrated approach. What you would do for something that's highly safety significant might not be the same as for something that isn't. And what you really want is to make sure you've got adequate protection. There, again, you're getting subjective, you're applying engineering judgment, and so on.

Moving right along, as I said, the idea is to generate assurance of adequate protection, and there are a lot of things you look at in doing that. There's what you've done with the hardware, the software development practice, and so on, the design measures. And in my mind, the design measures are much more important than the process. Good process doesn't guarantee good design, so you want to make sure the design is okay. How good is your mitigation or your coping capability? How good is your test coverage? What's the operating history of the device saying? What are your risk insights telling you? So there, again, we see a role for the PRA guys in helping flavor this thing.

Simplicity. Somebody brought that up and, sure, that's a factor. Simple is better. And that's another interesting one, though, because there are a lot of different measures of simplicity or complexity for digital. Again, it comes down to an engineering judgment and figuring out what matters in your application. So we can't get away from that notion of engineering judgment.

Oh, the last topic here, this goes back to this hazard analysis. There was a guideline we produced a couple of years ago now. The title is there. We looked at six methods, things like FMEA failure modes and effects. That's design FMEA, functional FMEA, fault tree, and so on.

In this demonstration, we wanted to work with the utility to apply this methodology to something real and looked for a couple of things. One is does it work, is it useful, is it helpful? And the other is how difficult is it to teach some of these new methods and get guidance to apply them? So from the EPRI standpoint, that's what we cared about.

And the idea here was that the plant actually does the hazard analysis. We coach them and try to make sure they understand what's in the guideline, those kinds of things. So that's what happened.

At Palo Verde, who stepped up to do this, they were looking at replacing their generator exciters on three units. It's non-safety, but they really want to keep that plant running. They are putting in new exciter systems, one for each unit, and it's in a separate building. And, of course, Palo Verde is in a place that gets really hot in the summer. The air conditioning is pretty darn important. And at the time we talked with them, they were saying that if the HVAC goes down, they've got less than ten minutes before they have to trip the plant, although I heard more recently that they might reduce that number to something like two minutes.

Anyway, so they put in redundant HVAC units, and they wanted to use hazard analysis to look at that system to identify potential vulnerabilities and convince themselves that it was going to be robust enough for what they were doing. Their main focus wanted to be on this method called Systems Theoretic Process Analysis, or STPA, which is sort of a novel method developed by a team of researchers at MIT --

MR. BLEY: We had a presentation by them.

MR. TOROK: You did?

MR. BLEY: Yes, by one of her graduate students.

MR. TOROK: Okay. So you guys know all about that.

MR. BLEY: We had a presentation.

MR. TOROK: Okay. The really interesting thing about STPA, from our standpoint, is it's well suited to looking for not just failures of systems and components but also for what you call misbehaviors where every component works as designed but the overall plant does something wrong. And it's somewhat unique in that respect, compared to FMEA, which is a hard focus on failures.

Anyway, so that was what they wanted to look at. We also, sort of on the side, did a high-level PRA analysis on this system and gave them some additional insights that turned out to be pretty interesting, like do you really need three trains, you know, three redundant HVACs and why? And that's the kind of thing where risk insights from the PRA can be very helpful.

Okay. So this was their feedback or the results. The word "substantial gain with minimal cost" are in quotes because they're their words, not mine. They thought that it was really going to increase the odds of a successful project because they did discover some unanticipated failure modes, some vulnerabilities, that they were able to fix fairly well, able to address, let's say, fairly easily, even though they were at a pretty advanced stage of the design at that point.

They also generated insights from the STPA that helped them look at a lot of other areas. For example, they identified behaviors under unanticipated conditions that could be really important to them. So they added those things to the testing matrix for the factory acceptance test and, you know, pre-installation testing and so on to make sure that the system really did behave the way the manufacturer was telling them it would, those kinds of things.

They also noted areas where they had to refine their procedures or training and so on. So they saw all that as advantageous. They were surprised that doing this helped them understand the system itself as much as it did, and the reason was it forced them to ask questions where they didn't know the answers. They had to go back to the supplier and find out what was going on, and it was important that they did understand what was going on.

Let's see. They liked the fact that doing this was really quick and identified vulnerabilities much faster and much easier than they could with FMEA, which had been their traditional approach. They also liked the fact that they ended up with a report that helped them explain to their management why it was important to do some of these things. The report called attention to certain vulnerabilities where they knew they ahd to address them before the system went into operation, and they were able to make their case.

As a result of all of this, the guys who were involved in it are pushing to make it part of their standard procedure for mods and working to generate the right kind of management buy-in to make that happen.

Anyway, we're on schedule, right?

CHAIRMAN STETKAR: Close. I'm impressed. Ray, thanks a lot. Any further questions, comments for Ray, for EPRI? If not, first of all, I'd like to thank both the staff and EPRI. You covered a lot of ground this morning.

A couple of other administrative things that I need to do here. Is there any one in the room who would like to ask any questions, make any comments? If not, we'll get the bridgeline open, if there's anyone out there who'd like to make any comments.

Again, I know a lot of this stuff was pretty esoteric to a lot of the members, but both digital I&C and understanding of its performance in a risk perspective are important topics and they remain important topics, both from a regulatory side of the fence and the industry side of the fence where these systems are being installed.

I'm told that the bridgeline is open. If someone is out there --

MR. LEWIS: Marvin Lewis, member of the public.

CHAIRMAN STETKAR: Thank you, Marvin. I appreciate it. And, again, just for the record, identify yourself because I was talking over you and make your comments, please.

MR. LEWIS: No, no, no, you have the right to talk. I interrupted.

CHAIRMAN STETKAR: No, that's -- go on.

MR. LEWIS: My name is Marvin, M-A-R-V-I-N, Lewis, L-E-W-I-S. And I'm very pleased today because from what I am hearing you're finally looking at the situation where a red light is being hidden behind a maintenance tag, like as in Three Mile Island number 2 back in '79 and maybe a romantic triangle is going on winding up in a core meltdown, like at Chalk River, that there are things that go beyond I&Committee and analog. And I'm glad to hear you're finally bringing it into the record, and I'm very, very pleased to hear it because I've been listening since '79. Thank you.

CHAIRMAN STETKAR: Thank you, Marvin. Is there any other member of the public on the bridgeline who'd like to make any comments? If not, again, I'd like to thank the presenters. They covered an awful lot of material this morning. And with that, we will recess and we'll go off the transcript until this afternoon. Let's return at 11:20, and we'll start the topic of our research report.

(Whereupon, the above-referred to matter went off the record at 11:05 a.m. and went back on the record at 1:01 p.m.)

AFTERNOON SESSION

1:01 p.m.

CHAIRMAN STETKAR: We are back in session. And the first topic for this afternoon is the Nine Mile Point Unit 2 MELLLA PLUS application. And Joy Rempe will lead us through that. Joy.

4. NMP2 MELLLA PLUS APPLICATION

MEMBER REMPE: Thank you, Mr. Chairman. On June 22nd, our Power Uprate Subcommittee reviewed the license amendment requests and the associated NRC draft safety evaluation to allow operation of Nine Mile Point Unit 2 and the expanded Maximum Extended Load Line Limit Analysis plus or MELLLA PLUS domain. At the end of our meeting, our Subcommittee recommended that LAR be presented to the full committee.

This LAR for operation in the MELLLA PLUS domain is the third to be reviewed by the ACRS. The first was for the Monticello Nuclear Generating Plant and the second was for Grand Gulf Nuclear Station Unit 1. And as you'll hear today, several features of the Nine Mile Point Unit 2 which differ from Monticello and Grand Gulf are of particular importance with respect to MELLLA PLUS operation.

Today we're going to hear presentations from the NRC staff, their consultant and representatives from licensee, Exelon Generation Company. Part of the presentations will be closed in order to discuss information that's proprietary to the licensee and its contractors. And I believe we'll be starting today by hearing from Travis Tate of NRR Management.

MR. TATE: Yes.

MS. REMPE: Thanks.

MR. TATE: Thank you. Good afternoon, everyone. I'm Travis Tate. I'm currently the Acting Deputy Director in the Division of Operator Reactor Licensing in NRR. And as was just previously communicated, the staff did meet with the Subcommittee on June 22nd and is pleased to have the opportunity to discuss with the full Committee today our review of the MELLLA PLUS license amendment for Nine Mile Point Unit 2.

I also wanted to highlight in addition to the previous two that have gone before Nine Mile that we currently have a MELLLA PLUS application in house for Peach Bottom. Peach Bottom is currently under staff review and we will schedule in the near-term ACRS full Sub and full Committee reviews.

Those are basically my opening remarks. And I want to turn it over to Mike Dudek.

MR. DUDEK: Thanks, Travis. Good afternoon, everyone. Thank you for your time today in discussing this important issue. As Travis stated, my name is Michael Dudek. And I'm the Acting Chief of 11 Projects Branch in NRR.

For efficiency today, in varying my opening remarks, instead of spelling out Nine Mile Point Unit 2 every time, I'm going to say Nine Mile Point. And I'll be using licensee and Exelon interchangeably just for efficiency.

I'm going to use the next five minutes to discuss the specifics behind. As Ms. Rempe said, the maximum extended load line limited analysis or MELLLA

PLUS license amendment review that Exelon has submitted to the NRC for review. However, I would like to take the first couple of minutes and thank my NRR as well as in some instances my agency technical counterparts as well as my lead PM Bhalchandra Vaidya for the thorough review of the licensee's application and their excellent work in putting this SE together. I thought which I've read numerous times that it was comprehensive in addressing these complex technical issues as well as being easy to read for the layman such as myself.

With that being said, we are here today to discuss the specifics behind Exelon's license amendment request dated November 1, 2013 that proposed a revision to Nine Mile Point's technical specification to allow the operation of a currently licensed MELLLA domain to an expanded MELLLA PLUS domain established under the previously approved extended power uprate condition of 3,988 megawatts thermal rated core thermal power.

As a reference to those of you in the audience, an extended power uprate or EPU was approved for Nine Mile Point by License Amendment No. 140. And this was dated November 22nd. The extended power uprate increased power level to 3,988 megawatts thermal from 3,467 megawatts thermal or approximately a 15 percent increase. In case you're taking notes, that's by ML113300041.

Specifically in the application, Exelon describes MELLLA PLUS as when Nine Mile Point would operate in a domain where its operating power is maintained constant, but the recirculation core flow is allowed to operate within a wider window than under the MELLLA conditions, i.e., a flow window between 85 percent and 105 percent. The licensee in the application describes this operating window as providing flexibility that would reduce the need for frequent control rod motion.

The technical staff, thanks to Chris Jackson, performed a thorough review of Exelon's license amendment request application which as Travis and Ms. Rempe explained was the third such review request that we've conducted, the first two being Monticello and Grand Gulf and Peach Bottom which is currently under way. As a result of the staff's thorough review of Nine Mile Point, the staff's overall determination was that the licensee's proposed operation in the MELLLA PLUS demand provides additional operating flexibility while not compromising plant safety.

The staff initially presented as Travis stated these initial proposed findings to the ACRS Subcommittee during a meeting about two weeks ago. The ACRS provided some very good feedback on that meeting and presented the staff with a few takeaway issues which are open items to be closed and a couple of other items. From my perspective, the responses were provided to the Subcommittee expeditiously in which I hope through that initiative will help facilitate a useful dialogue between everyone in this room today.

CHAIRMAN STETKAR: Michael, just for the record, I have to interject this. The Subcommittee does not represent ACRS recommendations. The Subcommittee, anything you hear, individual comments from single members, we only communicate via Committee letters. I just always need to clarify that for the record.

MR. DUDEK: Understood. Apologies for that. At this point, that concludes my opening remarks. I'd like to turn the meeting over to my lead PM Balchandra Vaidya to give some additional information about the MELLLA PLUS license amendment for Nine Mile Point.

Thank you for your time and I look forward to addressing any questions that you have as we move forward.

MR. VAIDYA: Thank you, Mike. I'm Balchandra Vaidya, Project Manager in NRR for Nine Mile Point MELLLA amendment request. I will coerce among the points that we have heard in previous Travis' and Mike's presentation.

One thing is the licensee submitted a revised application on June 13 that reflected the completion of their implementation of changes to Standby Liquid Control System. They implemented the improvements to Standby Liquid Control System in the spring 2014 outage. Amendment for that was approved just before the outage.

During the review of staff, multiple rounds of requests for additional information were issued to Licensee on various topics such as reactor systems, instrumentation, controls, human factors, etc. Licensee submitted their responses in the time period between March 10, 2014 and February 18, 2015.

NRC staff also performed an audit at the Nine Mile Point 2 plant site on November 20, 2014.

Multiple technical specifications changes as well as existing license condition support MELLLA PLUS application. Existing license condition seven restricts feedwater Heater out of service by imposing a 20 degree Fahrenheit feedwater temperature band.

The proposed TS change for TS LCO 3.4.1 prohibits single loop operation in MELLLA PLUS domain. Some other technical specification changes are revision of safety limit in TS 2.1.1.2 by increasing the SLMCPR for two recirculation loops in operation from greater than 1.07 to greater than 1.09. Another change is revision of the acceptance criteria in TS Surveillance Requirement 3.1.7.7 by increasing the discharge pressure from greater than 1,327 psig to greater than 1,335 psig.

These are just a few of the changes. There were some other changes also in the original application which are just too numerous to list all of them here.

Other than these, if you don't have any other questions, then I can ask colleagues to start their presentation.

MEMBER REMPE: I think that would be great.

MR. VAIDYA: Okay. Thank you.

MEMBER REMPE: Just so you're aware I think from our Subcommittee meeting you know you'll have to turn your own slides, right.

(Off record comments)

MR. KHAN: Good afternoon. My name is Mohamed Khan. I'm the Senior Engineering Manager at Nine Mile Point Nuclear Station. I would like to thank the ACRS Committee and the staff for the opportunity to provide a brief overview of Exelon Nine Mile Point Nuclear Station Unit 2 Operating License Amendment Request to allow plant operation in a Maximum Extended Load Line Limit Analysis Plus domain or MELLLA PLUS. That was previously approved under the EPU conditions.

The station greatly appreciates the staff's completion of the safety evaluation final draft since our last Subcommittee meeting on June 22. This will allow the station to complete and finalize our plans to implement MELLLA PLUS during the week of September 13th.

My technical and operations team are here today along with representatives from Exelon Corporate Fuels, License and Regulatory Assurance, representatives from the Peach Bottom MELLLA PLUS team and technical assistance from GE. General Electric/Hitachi are here today to support us in our final overview to the Committee of the station's project scope, the modifications that we've previously implemented in the last Unit 2 spring 2014 outage, the remaining implementation and testing activities, completed training and procedure changes and on our overall station readiness to implement in September.

The agenda for today includes a brief station overview followed by the MELLLA PLUS project overview provided by Dale Goodney, the Project Manager, to my left. And to his left will be George Inch, our Senior Staff Engineer, who will present the MELLLA PLUS design analysis and followed by current License Shift Manager, Dan Cifonelli who will present operator actions, validation and training.

A brief station overview, Nine Mile Point Unit 2 is a BWR-5 with a Mark II containment designed pressure of 45 pounds per square inch. The operating license was issued in 1987 with an original licensed thermal power of 3,323 megawatts thermal.

MEMBER SKILLMAN: Mohamed, excuse me. What was your design pressure please?

MR. KHAN: Forty-five pounds per square inch containment.

MEMBER SKILLMAN: Thank you.

MR. KHAN: In 2006, we renewed our operating license to allow operation until April of 2046. But we will not enter that period of operation until 2026.

The station implemented EPU in July 2012 with a current license power of 3,988 megawatts thermal. Unit 2 is currently in its second period of operating under EPU conditions. We are in a 24-month operating cycle.

MEMBER BANERJEE: Are you operating at 100 percent?

MR. KHAN: Yes.

CHAIRMAN STETKAR: Green light.

MEMBER BANERJEE: I keep forgetting these new rules. So you're at 100 percent EPU.

MR. KHAN: Yes.

MEMBER BANERJEE: Are you able to get to 105 percent flow?

MR. KHAN: George.

MR. INCH: Yes. As part of EPU, we installed clean mixer, jet pump mixers. So we're able to get to the design rated flow of 105 through the increase of flow regime. That's towards the end of cycle. At a rated EPU conditions, we can get to 104 percent, the higher DPE conditions.

MEMBER BANERJEE: So you've operated in this range, 100.

MR. INCH: We operate typically between 100 and 101 percent to 104 percent. I think in

Subcommittee we had some choice.

MEMBER BANERJEE: Yes, I missed the Subcommittee. All right. Thanks.

MR. KHAN: As part of the opening remarks by the staff for the MELLLA PLUS benefits, it has rolled out an extended operating domain to allow us to fuel reactivity manipulations. As mentioned previously, during the July 2014 outage, we did implement the detect and repress solution, confirmatory density algorithm for thermal hydraulic stability solution. And this will provide a more reliable and stable solution to detect any core instability.

We did also implement during the 2014 spring refuel outage the enriched boron which provided us more margin for ATWS conditions. We did increase the boron enrichment from greater than 25 percent atom weight to 92 percent atom weight.

MEMBER REMPE: Mohamed, during our Subcommittee meeting, it was discussed that although this license amendment request is solely for GE14 fuel, that there is subsequent information coming to the staff and the staff is reviewing it regarding your switching to GNF2 fuel. Correct?

MR. KHAN: That is correct.

MEMBER REMPE: And the staff -- I didn't mention it earlier -- but that documentation has been submitted to the staff as I recall. Or it's in process.

MR. INCH: Well, you said something I don't think is quite right.

MEMBER REMPE: Maybe I'm confused. Correct me.

MR. INCH: The process that's being used to introduce GNF2 is the G Start process. And that process will allow evaluation of the GNF2 fuel under 50.59 provisions. And the 50.59 process will shake out whether or not any submittal of information is required. So there is currently -- The only thing that is required for the reload is the safety limit MCPR.

And I think we can clarify that process. I believe Bob Close from our Fuels Department could speak to the process being used. Could you put up that backup slide that summarizes that process?

(Off record comments)

Bob, you can speak to this.

MR. CLOSE: I'm just going to restate some of the points that Mr. Inch made. My name is Bob Close and I'm a senior engineer with our Nuclear Fuel group. We will be performing evaluations and reload licensing analysis in accordance with the G Start 2 requirements. And, of course, as part of those requirements, we'll also do those analyses necessary to meet limitations and conditions as well as the requirements of Develop PLUS LTR, DSS-CD LTR and the expanded operating domains LTR.

Our review to date has determined based on preliminary results that the safety limit MCPR change, an increase in that value, was expected with the transition to the GNF2 fuel bundle and consistent with what we've observed in the results for Peach Bottom and also Grand Gulf.

That will require a tech spec change. It will be greater than the value that was reviewed as part of this license application request. So there will be a submittal for that license amendment request. Our 50.59 review process will guide us in determining if there are any other changes requiring review by the NRC.

MEMBER REMPE: Thank you for clarifying that.

MEMBER BANERJEE: Can you just remind me please? GNF2, does it have CHF performance at low flow which is significantly different from G40?

MR. CLOSE: I would ask my vendor, GE/H to speak to that. But I'd also -- Is that potentially a response that should be done in closed session? Or can it be made in open session?

MEMBER BANERJEE: Yes, whatever you'd like. But I'd like to get some clarity on that.

MR. CLOSE: All right. So we'll jot that point down and we can respond to that question in the closed session. You guys understood the question?

(No verbal response)

Okay. We'll respond to that in closed session.

MEMBER BANERJEE: Okay. Thanks.

MR. JACKSON: Just to answer your question, that had not been submitted. That will be coming some time in the future, the safety limit for a tech spec change.

MEMBER REMPE: And the staff will follow whatever procedures are associated with the M PLUS generic LTR to deal with it.

MR. JACKSON: We will do a full 50.90, 50.92 license amendment request safety evaluation and document our findings.

MEMBER REMPE: It's interesting to hear about the CPR performance. But I think it's outside the scope of what we're talking to today. I just wanted to make sure that everybody on the Committee was aware of that.

MR. CLOSE: And just to clarify that submittal for the license amendment request safety limit MCPR change would be in approximately late August, very early September of this calendar year consistent with the NRC review period required to support loading GNF2 in spring of 2016.

MEMBER REMPE: Okay. Thank you.

MR. KHAN: This concludes the station overview at this time. I'm going to turn it over to our project manager, Dale Goodney.

MR. GOODNEY: Thank you, Mohamed. I'm Dale Goodney. I'm the MELLLA PLUS Project Manager at Nine Mile Point. And I'm going to provide a brief overview of the MELLLA PLUS benefits from what you've already discussed and also cover our MELLLA PLUS project implementation plan.

When Nine Mile 2 went to the extended power uprate in July of 2012, our available core flow window was reduced from 20 percent to six percent. And as was mentioned earlier, Operations maintains the core flow in a range from about 100 to 104 percent depending on where we are in the cycle.

With MELLLA PLUS we'll be able to expand that core flow window back to 20 percent which is where we were prior to the extended power uprate. That will result in fewer control rod manipulations. We're projecting that the number of deep down powers that are required near the end of the operating cycle for control rod sequence exchanges to be reduced by about one-half.

MEMBER BANERJEE: So you're showing on your graph around 85 percent of rated flow as the full power lowest flow.

MR. GOODNEY: The lowest flow at --

MEMBER BANERJEE: You're not going down to 85 percent.

MR. GOODNEY: We're not going down to 85 percent. That's correct.

MEMBER BANERJEE: Just to 85.

MR. GOODNEY: That's correct.

MEMBER BANERJEE: All right.

MR. GOODNEY: Now we'll also with the expanded operating region --

MEMBER BANERJEE: Why are you just going down to 85 rather than 80?

MR. GOODNEY: That's a good question. The 85 percent was the number that was selected very early on in the project during the feasibility assessment for the MELLLA PLUS for Nine Mile Point. Mutually agreed to between General Electric and Nine Mile Point is a reasonable value that would essentially give us back the operating margin we had pre-EPU. And that was the basis that all the analysis was performed on from the beginning.

MEMBER BANERJEE: Not just to steer a little further away from the stability boundaries which was probably the --

MR. GOODNEY: No, that wasn't really a factor at that point.

MR. INCH: Clearly, we wanted to analyze where --

MEMBER BANERJEE: For a little bit more margin.

MR. INCH: Essentially, yes.

MR. GOODNEY: Yes.

MEMBER BANERJEE: And if you don't need if you need to get to 80 it's fine.

MR. GOODNEY: That's right.

MR. INCH: Yeah.

MR. GOODNEY: Okay. And also with this expanded core flow window, it will enable Operations to maintain two percent margin to the MELLLA PLUS line compared to the one percent that they currently maintain to the MELLLA line. There are other benefits obviously for MELLLA PLUS, but the primary driver from a project standpoint was the improvement in reactivity management and the reduction in operator burn.

Also shown on the power to flow map is a point of reference or two key state points, the maximum power density which is point N and the maximum power to flow ratio of point M on the power to flow map. And those two values for Nine Mile Point fall in between the other two plants that have already been reviewed by ACRS for MELLLA PLUS.

The MELLLA PLUS project is comprised of several components that are shown on this slide. Those that are highlighted in green as was mentioned earlier have already been implemented. That was during the spring 2014 refueling outage including the enriched boron as well the DSS-CD. We have been operating with DSS-CD in service since May of 2012. I'm sorry. 2014 with the confirmation density algorithm trip bypass with jumpers pending a receipt of the MELLLA PLUS license amendment.

MEMBER BANERJEE: Was the plant previously an option three?

MR. GOODNEY: Yes. It was previously an

option three. Since 2000 we've been operating.

We expect to receive the license amendment in August. And based on that, we have scheduled the implementation for the remaining portions of the MELLLA PLUS project which will be implemented online in September of 2015.

We'll begin on September 8th with removal of the jumpers for enabling the DSS-CD as well as making the appropriate APRM/OPRM setting changes in accordance with the new tech specs. We'll also be implementing the MELLLA PLUS reload analysis including the MELLLA PLUS core operating limits report and updating the core monitoring computer with the new information for the MELLLA PLUS.

Once that's completed, we will implement the new tech spec and immediately after that begin MELLLA PLUS testing which is scheduled to start on September 12th. That will coincide with a planned downpower. It's scheduled for that same weekend for a control rod sequence exchange. We expect the test program to take approximately six days. And we will be completing all of the prescribed MELLLA testing prior to commencing normal operations in the MELLLA PLUS region.

Now there was a question raised at the

Subcommittee regarding the variability of the test results. In our next section the George will cover, we'd like to elaborate more on our response that we had discussed during the Subcommittee. Are there any questions from what we've covered so far?

(No verbal response)

All right. Given that, I'll now turn it over to George Inch to discuss the design analysis.

MR. INCH: Good afternoon. My name is George Inch. I'm the Senior Staff Engineer who is responsible for the MELLLA PLUS and extended power uprate design and analysis. I'd like to briefly cover a couple of key points with regards to the limitations and conditions.

We comply with all the applicable limitations and conditions. The 14 applicable from the methods, there are several that are not applicable mainly because the approach we've chosen with regard to the enriched boron. So some of the TRAC G analyses methods limitations are not applicable. And also we have a full core GE14. So some of the conditions associated with mixed cores don't apply.

For operability/flexibility limitations and conditions, I think Bhalchandra went through several of these. We have a tech spec for limiting single loop operation for both MELLLA and MELLLA PLUS. The original licensing for single loop at Unit 2 was up to the MELLA line and that has not changed with EPU. So it's now in tech specs. But it's always been part of the SAR.

We have an existing License Condition 7. We've had that since stretch uprate in mid '90s. It's a 20 degree design window about the rated feedwater temperature. And our assessment is that that limitation and condition satisfies the 12.5B. So we're not proposing a new one. That's sufficient to restrict feedwater heater out of service which is one of the restrictions in the MELLLA PLUS LTR.

And the COLR, there's another requirements for the power flow map to be part of the COLR. And those limitations will be part of that.

In Subcommittee, we discussed our power flow map and how that's integrated into our procedures. And it's under design control.

The key features of our license amendment request are that we've increased the enrichment to 92 atom percent. And what that does is it meets the limitation and condition 12.18b. So we essentially keep the integrated heat loads of the containment as really unchanged from the original licensing bases at

75 percent flow which is the limitation and condition.

And it has a significant improvement to margin to the HCTL curve which is the curve under which Operations would need to emergency depressurize that reducing the impact on the suppression pool temperature. Dan Cifonelli will talk a little bit about how that's improved operator responses.

It also has a side benefit where we're able to meet the 10 CFR 50.62 rules with one pump, the equivalency equation. We haven't changed the tech spec LCO or any of those aspects. So you still have both pumps start and initiate in the RRCS system.

We also have at Nine Mile 2 the redundant reactivity control system. It has an automatic injection start of the pump and an automatic feedwater flow runback that was part of the original ATWS design and licensing basis for Unit 2. And we currently under EPU in the ATWS credit those automatic functions. And these for MELLLA PLUS significantly improves the ATWS instability operator time requirements.

The redundant activity control system I'd like to talk about a couple of key features. The standby liquid control system pump start is on high reactor pressure when the APRMs are not downscaled.

So in any event where you lose the turbine, we have a 25 percent bypass capability. You'll get the high pressure signal.

If you're APRMs are not downscale, you'll make up the logic. For the pump start, it's 98 seconds. For analysis purposes, we use the 120 for the start. And for the feedwater runback, there is a delay of 25 seconds. The analysis uses 33.

The way the runback works is the redundant reactivity control system initiates a logic whereby the flow control valves on our feedwater pump, we have two motor-driven feedwater pumps under rated conditions. A third one's a spare. And it closes the flow control valve at max rate and opens them in flow valves simultaneously.

So within 21 seconds you're basically shutting the flow off to the reactor at which point the flow comes down quite rapidly.

CHAIRMAN STETKAR: You just have fixed speed motor-driven pumps. You don't have the variable.

MR. INCH: That's correct.

CHAIRMAN STETKAR: Thank you.

MR. INCH: For a dual recirc pump trip to trip the turbine, you don't have high pressure. And for that condition, the analysis for the ATWS with instability for the dual pump trip assumes two manual actions. One is that the operators manually scram within 20 seconds and the other is to initiate runback within 70 seconds.

I think one of the questions from the Subcommittee was where did the 270 come from. That was a design input before that we came up with at Nine Mile based on observing operators. We came up with what they were doing in place with a little bit of margin. And that's what we gave to GE for further analysis. We ended up not needing to change it based on the results of the analysis for the dual pump trip.

Dan will go through some of the details on the qualifications for that.

MEMBER BANERJEE: Do you see some results from this?

MR. INCH: Yes.

MR. CIFONELLI: Yes, I'll be covering those.

MEMBER SCHULTZ: Will that include any sensitivities evaluations?

MR. INCH: Yes, we have that.

MEMBER SCHULTZ: Thank you.

MR. INCH: We have that in the closed

session. Thank you.

One of the things that's impacted by MELLLA PLUS Nine Mile 2 is the prediction that the moisture carryover will go up. We have one state point which gets to about 0.236 weight percent at the 85 percent core flow point.

Our design analyses for radiological impact was always based on 0.35 weight percent. We didn't need to change that. I shouldn't say always. It was based on it when we extended power uprate. So we didn't need to revise that.

When we did the detailed evaluation of flow accelerated corrosion and what limiting components would be there, we determined that the outboard MSIV we needed to keep it below. The main steam leaving the reactor needed to be below 0.25 to keep the outboard MSIV below 0.5. That was the limiting component. The other limiting component is the main turbine at one percent.

The conditions that create the moisture carryover are really governed by the performance of the steam separators. And it's not necessarily the core flow effect. But it's really the combination of the rod patterns and the cycle exposure as the wear and the quality coming out of the given region of the core where you can get the quality not in that optimum band for the steam separator.

For Nine Mile at reduced core flow, we do see predictions of higher carryover that's not necessarily generically true. But that is true for us.

All of our evaluations of the moisture carryover have been done for 0.35 with the limitation of 0.25 going forward. That will be implemented in our implementation testing and then it will be embedded in our procedures.

Our experience with EPU core is really good. We've got the first cycle EPU data. We're below 0.2. The original predictions were about 0.08 for EPU. So we believe that and as part of our application explained in some detail why we expect that moisture carryover to actually not get above 0.1.

In Subcommittee, we had a question on our test program and what was the variability of some of the testing. We thought about our answer and we put together a variability of each test. You know there's two dynamic tests that are done where we adjust the pressure set point and the other one is water level changes.

Those are normal operator maneuvering

actions. So you're on a higher rod line. There's higher void content. So there is the transience that you see and the control system stability could be impacted.

This is a confirmation test. We've looked at it. It's a low sensitivity to exposure in the cycle of the rod patterns. So we don't see much variability there. Similar the neutron flux noise remains bounded by the -- We confirm it remains bounded by set point counts and we don't see much sensitivity there.

The stability monitor is also a noise check on the OPRM set points. The two tests that do have variability are the moisture carryover, the TIP power distribution and core performance. So these particular tests are baseline tests that we do. And then they're proceduralized that they're monitored continuously throughout the cycle.

So moisture carryovers checked at least every month. And core power is proceduralized such there are lot of times reactor engineering has to govern those. Hopefully, that answers the question.

MEMBER BANERJEE: I've often wondered why this moisture carryover is such an importance consideration.

MR. INCH: It's primarily dose ALARA considerations. The radionuclides that are in the liquid phase get carried over and it does cause or can cause higher dose in the main turbine and also potential for damaging the main turbine. You get moisture carryover too high. You get impingement on the blades.

MEMBER BANERJEE: But this is not that high, right?

MR. INCH: It's not that high. So what we've determined is that as long as you stay below 0.35 you'll be below the one percent. That's the important part. It's one of the things that we expect to change. We think we conservatively predicted it.

MEMBER SKILLMAN: George, when you say we expect a change, you expect a change from what to what?

MR. INCH: The predicted max value is 0.236 and that occurred in the prediction that it occurred at before 2,000 megawatt days per short ton. And it was for one rod pattern. We estimated it was going to last for only a few weeks at that higher level. And then it came back down.

And we think it will follow actually very much the chart we put up there and would be much lower than that value. But there's a potential that we could have a condition where you get higher moisture carryover.

MEMBER SKILLMAN: And if that were to occur, you would have temporary higher radiation levels and you would be considered at some level about your last stages of your low pressure turbine.

MR. INCH: As the moisture carryover -- Right now, we're going to keep our limiting condition for increased monitoring at 0.07. We're running at 0.02 right now. And we'll go into increased monitoring at 0.07.

There's an empirically -- It's both an analytical and empirical tool by which reactor engineering can predict the moisture carryover and also the core design as predicted to try and minimize the limiting rod patterns that are predicted to cause the carryover to develop higher.

MEMBER SKILLMAN: Thank you, George.

MEMBER CORRADINI: Since you brought it up, can we take a minute about the tool used? Can you tell us about that?

MR. INCH: The predictive tool?

MEMBER CORRADINI: Yes. I assume the measurement is dose-based.

MR. INCH: No. The way we measure the carryover is they measure the sodium-24 in the condenser. And then they also take samples in reactor. And based on that they can figure how much get carried over from the reactor. That's a chemistry procedure that we --

MEMBER CORRADINI: That's the measurement.

MR. INCH: Yes, that's the measurement.

MEMBER CORRADINI: Okay. Thank you.

MR. INCH: And then that's used to improve the analytical tool with empirical data to allow it to get better and better with time.

MEMBER CORRADINI: Thank you.

MR. INCH: I'll cover the sensitivity studies in closed session. Dan.

MR. CIFONELLI: Thanks, George. Good afternoon. I'm Dan Cifonelli, Active SRO and Shift Manager for Nine Mile Point Unit 2 and assigned to the MELLLA PLUS project team. And today I'm going to talk about the operator critical actions, the validation of them and the results from that validation process and the training we've performed in preparation for MELLLA PLUS.

The design requires two new critical operator actions as George already mentioned, 20 seconds to insert a manual scram using the mode switch. That provides a redundant RPS scram signal and also bypasses our low pressure MSIV isolation. The second is the 270 seconds for the dual recirc pump trip scenario. And it's combated by contingency five standard ATWS strategy for terminating and preventing injection to the vessel.

These actions were validated in September of 2014 using the Exelon process for validating time critical operator actions. That Exelon program is based on industry standards including ANSI and ANI 58.8 time response design criteria for nuclear safety-related operational activities.

These actions were validated using four normal operating crews. The purpose of the validation was to measure the actual time it takes for the operators to lower water level in the contingency 5 ATWS strategy. There was no new training given to the operators or no procedure changes required for this action to occur within this time frame. So the validation process was rigorous, used the validation team and four crews.

We also as part of the process or requirements evaluated the sensitivity to staffing. A couple of the observations were made with the operating crew at minimum staff. And what we found was the minimum staffing had no impact on either one of these actions and that's primarily because they're well trained. They're priority items in an ATWS.

All the controls are at the main control panel. The operator at the controls is continuously stationed at the controls area. And all the indications and controls are readily available to the operator at the front panels. And the actions are simple. Operator actions don't take many component manipulations for them to occur. So there is essentially no sensitivity to minimum staffing.

MEMBER SKILLMAN: Dan, would you comment as to whether or not your teams were preconditioned to know that they were going to see an ATWS-I event?

MR. CIFONELLI: Yes, the validation process includes the concept of them knowing what the criteria is. They are briefed on not doing anything any different than they normally do. The purpose of the exercise is to get a real valid result on what the time is. The crews are briefed on taking all the human performance actions, the procedures, as they normally do.

So the intent is to get real time. But they did know the criteria. That's part of the process. In our subsequent NRC audit, it was also confirmed that these times were valid. So the results are really on the next slide.

CHAIRMAN STETKAR: Dan, just for clarity though, you told them that you were going to test them on ATWS. You told them what the criteria was and then you tested it. Is that correct?

MR. CIFONELLI: That's correct.

CHAIRMAN STETKAR: Okay. And why are those times representative of 3:00 a.m. on a Monday morning when nothing has ever happened in the plant in the last year and a half?

MR. CIFONELLI: Because the times are -- Operators are trained. For a number of years they have been performing these actions since 1998.

CHAIRMAN STETKAR: So you've had several ATWS events at Nine Mile Point during 3:00 a.m. where these people have done this.

MR. CIFONELLI: We do out of the box examinations of operators for training.

CHAIRMAN STETKAR: I was an operator. I could find a steam generator tube rupture on a pressurized water reactor quicker than anybody else could in the simulator when I knew I was going to be tested on it. Not so much in the real plant.

So my question is you're characterizing these as representative times that I would expect 3:00 a.m. on a Monday morning after a run of -- pick any particular run you want -- 275 days where nothing has happened. They haven't even seen a glitch in feedwater flow. And I'm questioning whether or not this testing that you've put the operators through under conditions where they know what to expect is actually representative.

MR. INCH: It's not really testing though. What he's going through is a qualification for --

CHAIRMAN STETKAR: Is your light on by the way? I'm just making sure you're on.

MR. INCH: Correct me if I'm wrong, Dan, but it's not a test we're giving them. You're using an existing procedure for evaluating time critical actions.

MEMBER BLEY: It sounds more like a time in motion study the way Dan described it rather than a --

MR. CIFONELLI: That's correct. It is.

MR. INCH: That's what it is.

MR. CIFONELLI: We want real times, how long it takes.

CHAIRMAN STETKAR: But if I go to the grocery store and I know precisely where the can of peas is located, exactly where it is on the shelf, and I make sure all of the aisles are clear and then I test whether or not I can retrieve that can of peas within 47 seconds, that's one thing.

If I send a person to the grocery store under average conditions on a Saturday when everybody is shopping and say, "Go get me a can of peas," that's a much different condition.

MR. CIFONELLI: There's no doubt in my mind that at 3:00 a.m. the operators are well within the 270 second requirement. One of the observation criteria is that they're performing things that they normally would at 3:00 a.m., the use of diagnostic tools, three-way communications, time it takes to diagnose. And the margin that we're providing also is consistent with industry standards for examples of stress that you're talking about, Mr. Chairman, that would account for any variation under extreme circumstances.

MEMBER CORRADINI: But I guess I want to get back to the Subcommittee. But I think we went through this in the Subcommittee. What I remember was -- I'm not sure the human factors words with this, but this is some sense a rehearsal. But I thought NRC would go in with essentially an unknown and then do an audit check on this.

I think we want to check this with staff. But I think we went through this in the Subcommittee and asked the same sort of questions. But you guys have got to remind me. But this is what I remember because we were questioning essentially what this was versus a test.

MR. CIFONELLI: That's correct, Michael. And the audit results varied from 7.1 to 13.2 seconds for the scram and from 173 to 183 seconds for the 270 seconds. These are real numbers.

I watched the crews. I mean the guys are good. I'll tell you that. And this wasn't a race. We weren't trying to get them to achieve anything. We were trying to get a real number here.

MEMBER REMPE: The one thing that -- Maybe I was confused from the Subcommittee meeting, but the one thing I remember initiate manual scram within 20 seconds. That is something that is done for other reasons. And you just made it time critical for this particular application. So surely -- and maybe I'm inferring something incorrect -- you've had blind situations where the operators are having to do that in some of the others.

MR. CIFONELLI: Absolutely yes.

MEMBER REMPE: I would think that that has been tested before.

MR. CIFONELLI: Also keep in mind --

MEMBER SCHULTZ: Dan, the change of these features to a time critical operator action, does that change the training program at all?

MR. CIFONELLI: No.

MEMBER SCHULTZ: Or any aspect of it? It's just something that you're going to monitor appropriately going forward.

MR. CIFONELLI: That's correct. Keep in mind George's presentation. The basis of the number was an input based on what operators did at the time at the beginning of the project. It's not a number that we have changed on our program or changed our trainer or change our procedures to achieve. This is a real number. This is what it takes.

We will maintain it going forward. There's a process. It's been recategorized as a time critical action now because it's part of our design basis. So there's a maintenance program for those times. We'll revalidate every five years. Any changes to procedures or any changes to design, we'll have to consider these time critical actions.

MEMBER SCHULTZ: But it doesn't change the simulator program.

MR. CIFONELLI: No change in the simulator.

MEMBER SCHULTZ: The training program and so forth.

MR. CIFONELLI: Or the ATWS strategy. That's correct.

MEMBER SCHULTZ: Thank you.

MR. INCH: So the 270 second derivation was an observation of the normal training for ATWS events, dual pump trip. And they had no knowledge that we were timing them at that time. So when we came up with 270 we actually measured a value and then Engineering decided to add some margin on it.

When Dan came in with these numbers we're weren't surprised at all that they were able to do it faster. And I think the audit also included -- I think we talked about -- Diego as mentioned that there was a surprise event given to them.

MR. CIFONELLI: Just to states the results found, an average time of 8.5 seconds for shutting down the reactor and 193 seconds for terminating and preventing injection. These results demonstrate significant margin to the required times which account for uncertainties, stress, event recognition, action planning by the operators, team communications and verification practices.

MEMBER BLEY: In which way do you justify that last claim? Do you go back to simulator exercises? I'm kind of bothered as John is. I don't suppose when you put the guys in the simulator for normal training you say "You're going in and you're going to see a small LOCA. Now let's go over the small LOCA procedures and make sure you know how these work." And then go in and run the drill. They don't know what's going to happen.

Now you're saying we've got time and covers all of these contingencies. And you had a list of about eight or six. Please go through the basis for why it covers all of those contingencies.

MR. CIFONELLI: The basis for why it covers all of those contingencies is built into the margin that we find values at. Like you said, we will be doing surprise examinations as we do for all our time critical actions.

Going forward, those examinations will confirm that the operators will be able to perform those actions within those times on a surprise examination basis. We do those on a Monday morning. We call them out of the box examinations. And if an operator were not to be able to achieve these actions

--

MEMBER BLEY: I would believe that more -- I have a little trouble with the long list of things you gave me and said, "There's margin that covers all of these things" without showing me why it covers those things. What's your basis? How much time does it take for recognition? How much time does it take for getting out the procedures and going through them? It's just a blanket "Well, there's plenty of time for all of those things." Without a justification it leaves me wanting.

MR. CIFONELLI: The time it takes to get out the procedures and recognize the event are built into the range of 150 to 232 seconds. And the margin is what provides assurance of these other variables.

MEMBER CORRADINI: Can I clarify one thing because maybe I misunderstood? There are two times, one being the short time which occurs not just here but has to be -- I don't want to say practiced, but I can't come up with a better word -- practiced because of a number of other activities.

And the 270 is only if their automatic runback doesn't function. You don't need to do the manual runback. It's an automatic runback. This is a backup to the automatic runback.

MR. CIFONELLI: Well, that's not 100 percent correct. The 270 seconds is for the event where the high pressure doesn't trigger the automatic runback.

MEMBER CORRADINI: Okay.

MR. CIFONELLI: And that's specific to the dual recirc pump trip scenario which is not a high pressure event. So that's a derivation of 270 seconds which is particular to the automatic runback. It would not be triggered.

MEMBER CORRADINI: Thank you.

MR. CIFONELLI: But it was true that the 20 seconds is something we do very frequently.

MEMBER CORRADINI: Sure.

MR. CIFONELLI: That's the first thing the operator -- That's fundamental to initial operator training, how to shut down.

MEMBER BLEY: We weren't challenging that one.

MEMBER BANERJEE: So the runback, how reliable is that? Is it an automatic runback?

MR. INCH: The runback circuit within the reactivity control system has two divisions and has redundancy built in. And it's a digital system.

MEMBER BANERJEE: The 2RPT won't trigger

it.

MR. INCH: No. The high pressure in the reactor tends to be five pounds.

MEMBER BANERJEE: You'll have to --

MR. INCH: You have to have a high pressure to trigger it. You don't want to trip the turbine if you don't have to. So you can challenge containment. So you can get the reactor high pressure.

MEMBER BANERJEE: Okay. And if it doesn't trip with a turbine trip what happens then? Do you have some backup actions?

MR. INCH: Yes, we have some. We do have a presentation in the closed session to go through those details.

MEMBER BANERJEE: So we'll wait to the closed session.

MEMBER REMPE: During our Subcommittee meeting, we tried to anticipate some questions that other members might have. So that's why they're providing that in the closed session.

MEMBER CORRADINI: We knew you'd be here. So we're ready.

MR. CIFONELLI: So moving to the next slide we started our training early in the process, about a year ago, over a year ago in 2014. We introduced the operators to the MELLLA PLUS concept, the purpose of benefits of MELLLA PLUS. We introduced the DSS-CD solution, the changes to the OPRMs and the changes to the technical specifications. I'll give an overview of the automatic backup scram protection circuitry and the manual backup scram protection scheme.

In August 2014, we started our initial simulator training. We provided the power to flow map to the operators and solicited their feedback as it was in draft format at that time. Also in August we provided a demonstration of how good the 92 percent enriched boron is for shutting down the reactor. Demonstrated that the hot shutdown boron injection time was reduced from 16.4 minutes to 5.1 minutes.

The operators understand the importance of early injection of the standby liquid portion for boron to slow down the overall ATWS. And it basically trains itself in the sense that they're positively rewarded by slowing down the whole transient once you have boron injection going.

We also performed five different ATWS scenarios in August of 2014 that were started at the 85 percent flow, 100 percent power point.

In January of 2015, this year, we performed some additional classroom and simulator training. We spent time with our off-normal procedures using the new power to flow maps that have different lines in them for exits in scram regions and how the operators have to drive around the different regions of the plant for rapid power reduction maneuvers or for a sudden reduction in core flow.

In May of this year due to a recent industry event we want to take the opportunity to reinforce some fundamentals with regard to instability. We reinforced the fundamentals of early water level reduction to reduce subcooling and reduce the potential or consequences of the instabilities.

We also reinforced the importance of early rod insertion on an unexpected reduction in core flow, for instance, for a recirc pump trip. And we also reinforced the fundamentals of how to recognize and respond to instabilities in the reactor.

In July of this year, we gave the operators some additional reinforcement training. The initial training is complete and we provided some more similar scenarios in the MELLLA PLUS region. The training we have planned is focused around just in time training which will be for the testing program. The emphasis there is going to be on reactivity maneuvers and risk management and the testing procedures.

MELLLA PLUS will eliminate the burden of frequent control rod manipulations to control and maintain power which will reduce the potential for control rod manipulation errors and therefore reduce the related potential for consequences of fuel failures. This will be an improvement in operational safety. MELLLA PLUS will allow operations to maintain additional margin to rod lines and eliminate the current requirement to operate near limitations. This will also improve operational safety.

Based on the completed training of procedures and display readiness, our operator critical action results in a detailed implementation plan. Operations is ready to implement MELLLA PLUS.

MEMBER REMPE: So if there aren't any additional questions from ACRS members, this is going to be the end of the open session. I believe this is a good time to ask if there are any members of the audience and to open the phone lines if there's anyone out there that wants to provide a comment. This is a good time to have such comments.

While Zanya is getting the phone lines open up, is there anyone in the audience who wants to provide a comment?

(No verbal response)

We're just going to have to be patient here for awhile.

5. OPEN PUBLIC COMMENTS

MR. THOMPSON: Hi, this is George Thompson from GE/Hitachi.

MEMBER REMPE: Okay. So we know the closed line is open. And you believe the open line is open now, too.

CHAIRMAN STETKAR: We got the closed line. Thank you, George.

MEMBER REMPE: We got that, George.

MR. THOMPSON: Okay.

(Off microphone comments)

CHAIRMAN STETKAR: There we go.

MEMBER REMPE: Now the public line is open. If someone is out there, would you please just make a noise and speak up so we can verify it is indeed open?

(No verbal response)

If anyone out there has a comment, would you like to provide that comment at this time?

(No verbal response)

With that being said, we're going to close the public line and verify it is indeed closed and we'll start the closed session. I believe we'll still have GE/H or Exelon up.

CHAIRMAN STETKAR: Just procedurally, make sure that indeed everybody in the room is authorized to be here for the closed session.

MEMBER REMPE: And we're going to have to rely on --

CHAIRMAN STETKAR: Both staff and the licensee.

(Whereupon, the open session ended and the closed session begins.)

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

NRC
Failure Mode Related Research

Mauricio Gutierrez
RES/DE/ICEEB

Ming Li
RES/DRA/PRAB

July 08, 2015

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- Background
  - Summary of NRC Digital System Failure Mode Related Research Efforts
  - Summary of Advisory Committee for Reactor Safeguards (ACRS) I&C Subcommittee Feedback and NRC Response
- Summary of Staff Follow-up Actions
  - PRA and Deterministic Assessment Perspectives
  - Digital System Failure Mode Terminology and Common Concepts in Selected Definitions
  - Digital System Failure Modes Mapping
- Conclusions and Next Steps

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background

- ACRS has long standing concerns that based DI&C system failure modes are not well understood.
  - Misbehaviors other than non-performance of required function can occur.

- ACRS brought concerns to Commission attention in 2008.

- June 26, 2008 – Commission issued SRM-M080605B
  - Directed staff to
    - "report the progress made with respect to identifying and analyzing digital I&C failure modes …"
    - and "discuss the feasibility of applying failure mode analysis to quantification of risk associated with DI&C…

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Related NRC Research

- DRA – PRA Methods for Digital Systems
  - Brookhaven National Laboratory NUREG/CR reports
    - Traditional Probabilistic Risk Assessment Methods for Digital Systems (NUREG/CR 6962 and NUREG/CR 6997)
    - Quantitative Software Reliability Models for Digital Protection Systems (NUREG/CR 7044)
  - WGRisk
    - International effort to establish failure mode taxonomy for PRA related research.
  - Draft “Development of A Statistical Testing Approach for Quantifying Software Reliability and Its Application to an Example System” (NUREG/CR-xxxx, BNL-NUREG-yyyy-20zz)

- DE – Analytical Assessment of Digital I&C Systems
  - RIL-1001 [ML111240017, 2011] and NUREG/IA-0254 [ML11201A179, 2011]
    - Software Related Uncertainties
    - Understanding faults attributable to complex logic (e.g., software)
  - RIL-1002 [ML14197A201, 2014]
    - DI&C safety system failure modes – what is known so far
  - RIL-1003 (scheduled for 2015 completion)
    - Feasibility of applying failure mode analysis to quantification of risk associated with DI&C systems.
  - RIL-1101 [ML14237A359,2015]
    - Broader view of hazard analysis to address misbehaviors attributable to engineering deficiencies.

ACRS I&C SC Feedback

September 19, 2013 – ACRS I&C Subcommittee Feedback on Research Information Letter 1002. Subcommittee Members:

– Appreciated the synthesized set of system failure modes identified (Set L).

– Requested harmonization of failure modes used by DE, DRA, and EPRI.

Staff Response to I&C Subcommittee Feedback

- DE and DRA had technical discussions on harmonization.
- DE and EPRI also discussed harmonization.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

PRA and Deterministic Assessment Perspectives

	Technical Objectives	Involves asking:
Deterministic Licensing	Safety Assurance [RIL-1002].	1. What can go wrong? 2. What are the consequences? [NRC Website: Risk Assessment in Regulation]
Probabilistic Risk Assessment	Support quantification of system reliability. Estimate Risk by computing real numbers [NRC Public Website: How We Regulate]	1. What can go wrong? 2. How likely is it to go wrong? 3. What are the consequences? 4. Which systems and components contribute the most to risk? [Apostolakis Presentation]

Digital System Failure Mode Mapping

RIL-1002 Set L	WG Risk Survey	EPRI Guidewords
No output upon demand	Loss of function No actuation signal when demanded	No function Partial function
Output without demand	Spurious actuation	Over function Unintended function
Output value incorrect	Failure to actuate	No function Partial function Over function
Output at incorrect time	Failure to actuate in time	Unintended function
Output duration too short or too long.	Loss of communication	Partial function
Output intermittent	No actuation signal when demanded	Intermittent function
Output flutters	Spurious actuation	Degraded function
Interference	Adverse effects on other functions	Degraded function
Byzantine behavior	Other	Degraded function

United States Nuclear Regulatory Commission
Protecting People and the Environment

Conclusions/Next Steps

- DE, DRA, and EPRI have a shared understanding of the issues that lead to misbehavior other than the non-performance of a required function.
- DE and DRA staff agree that Failure Mode Set L could be useful for both DRA and DE.
- NRC and EPRI will continue sharing technical information from digital system failure mode related research.
- Vocabulary Harmonization topic is in the I&C Research Plan FY 2015-2019 candidate pool.
- RIL -1003 – will report on the feasibility of applying failure mode analysis to quantification of risk associated with DI&C systems.

Overview of Digital I&C PRA Research Activities

ACRS Full Committee Meeting
July 8th 2015

Ming Li
Probabilistic Risk Assessment Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
(301-415-2428, ming.li@nrc.gov)

Background – Regulatory Needs

- Nuclear Power Plant I&C systems shifting analog to digital
- Commission encouraged using PRA technology in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data – 1995 NRC PRA Policy Statement (60FR42622, August 16, 1995)
- National Research Council recommendation*
  - The USNRC should require that the relative influence of software failure on system reliability be included in PRAs for systems that include digital components
  - The USNRC should strive to develop methods for estimating the failure probabilities of digital systems, including Commercial Off The Shelf (COTS), for use in PRA

*National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues," National Academy Press, Washington, DC, 1997.

Staff Positions for DI&C PRA Research

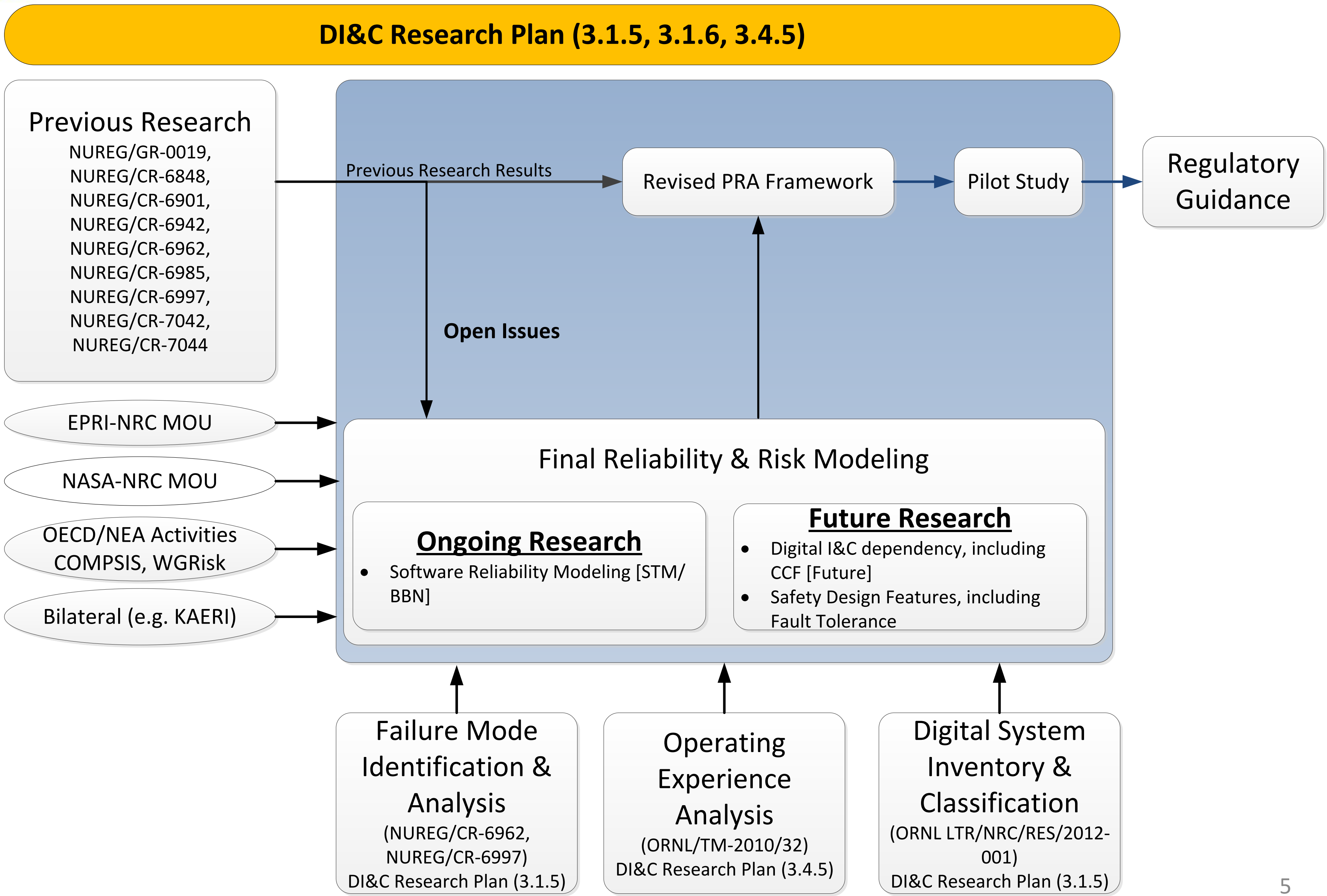
- DI&C PRA includes reliability modeling for hardware, software, and interactions among them
- Failure behaviors are examined (modeled and quantified) at functional levels of detail
- Hardware reliability modeling considers hardware random failures. Failure data sources include operation experience, and handbook data
- Software reliability modeling quantifies stochastic software failure behavior caused by logical errors in the design with deterministic failure mechanism
  - Software failure is defined as functional deviation from its expected behaviors

software failure is defined as the triggering of a defect of the software, which results in, or contributes to, the host (digital) system failing to accomplish its intended function or initiating an unwanted action. - NUREG/CR7044

NRC FY2009 – FY2014 Digital I&C PRA Research

- Objective: Identify and/or develop methods, analytical tools, and regulatory guidance for:
  - Including digital system models into nuclear power plant (NPP) PRAs
  - Incorporating digital systems into NRC's risk-informed licensing and oversight activities
- Deliverables
  1. NUREG/CR-6997: Applications of traditional PRA methods to a DFWCS (2009)
  2. BNL-90571-2009-IR: Philosophical Basis for Incorporating Software Failures into a Probabilistic Risk Assessment (2009)
  3. BNL-94047-2010: Review Of Quantitative Software Reliability Methods (2010)
  4. NUREG/CR7044: Selection of quantitative methods and how they will be applied to an example system (2013)
  5. Additional Reports:
     - NUREG/CRs on Application of selected QRSMs to candidate system (in progress)
     - Regulatory Guidance (future)

NRC Digital I&C PRA Overview



Previous Research on Hardware/System Reliability Modeling

- Ohio State University/ASCA/University of Virginia – Dynamic reliability modeling methods applied to a DFWCS (NUREG/CR-6901 [2006], NUREG/CR-6942 [2007], NUREG/CR-6985 [2009])
- BNL – Traditional reliability modeling methods applied to a DFWCS (NUREG/CR-6962 [2008], NUREG/CR-6997 [2009])

Previous Research on Software Reliability Modeling

- UMD-OSU Metrics Based Studies (NUREG/GR-0019, NUREG/CR-6848, NUREG/CR-7042)
  - Ranked metrics with respect to estimating software reliability
  - From metrics to # of residual defects in the software
  - Estimate failure probability using finite state machine simulation and operational profile
- BNL Studies (NUREG/CR-7044 and ongoing)
  - Expert panel on software reliability
  - Ranked software reliability models and chose two for further study
    - Bayesian Belief Network (BBN)
    - Statistical Testing Method (STM)

International Activities

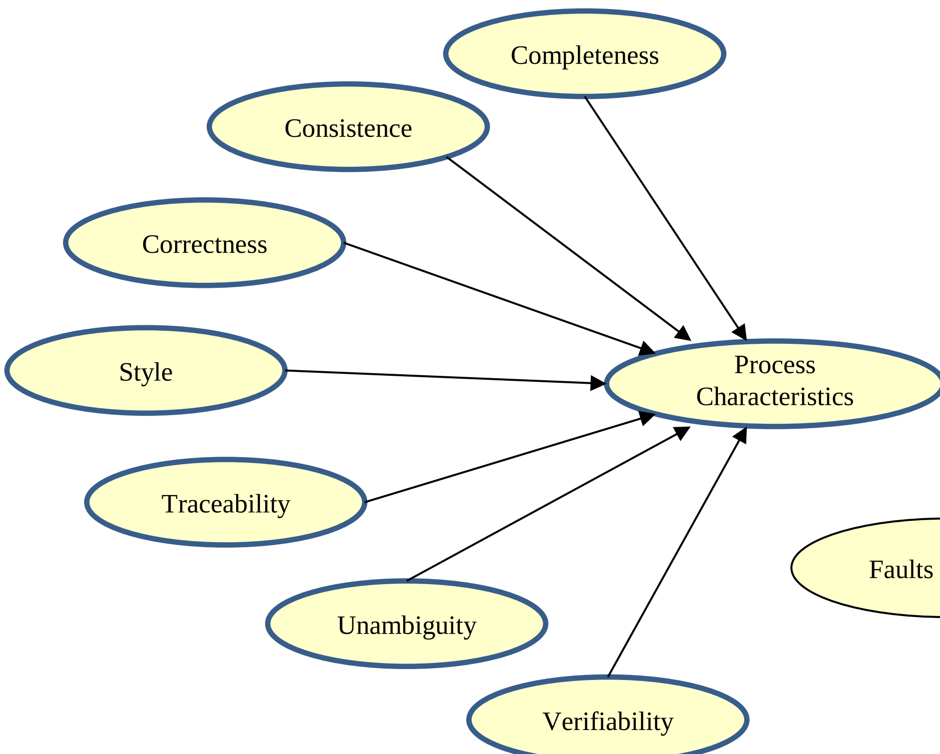
- Bilateral
  - South Korea (KAERI/KAIST)
  - A NUREG/CR report on BBN study is expected in 2016
- OECD
  - Digital I&C – NEA/CSNI
    - NEA/CSNI/R(2014)16: Failure mode taxonomy
    - NEA/CSNI/R(2009)18: Recommendations on digital I&C PRA
  - COMPuter-based System Important to Safety project (COMPSIS) (2005-2011)

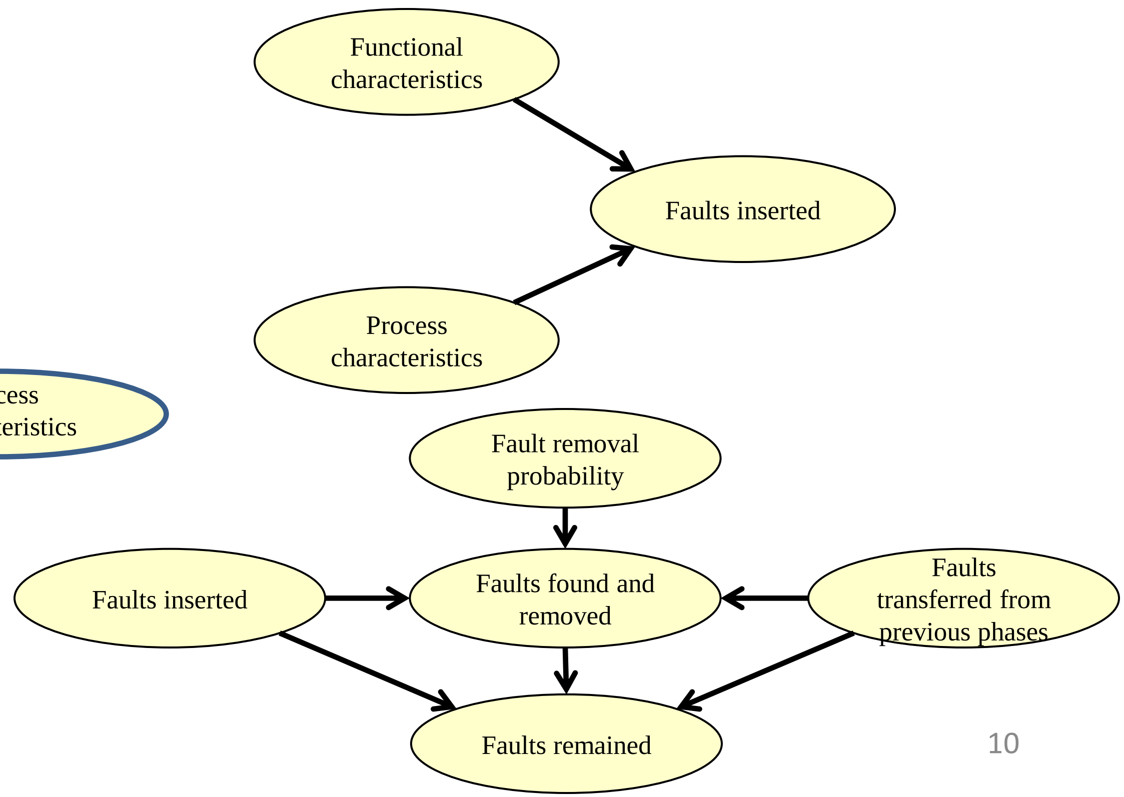
Ongoing Research on Software Reliability

- Statistical Testing Method (STM)
  - Test software in a PRA context
    - Uses PRA to define conditions the software should be tested (operational profile)
    - Number of test cases required can be determined using PRA sequence frequency
    - Generates test cases via the operational profile based thermal hydraulic simulation
    - Integrated hardware/software testing environment
  - Applied to INL ATR LOCS (loop operating control system)
    - 10,000 conditions were identified and tested
    - A large number of early(27)/delayed(964) trip anomalies were observed
    - Test cases were regenerated by removing artificial noise added to inputs, adding synchronizing timing signals, and recalibrating input/output modules
    - 10,000 new test cases were rerun, 45 delayed and 16 early trip anomalies still exist:
      - Small errors in processing input signals caused an early or delayed trip
      - Hardware (IO modules) resolution limitation caused these anomalies, not the software

Ongoing Research on Software Reliability

- BBN
  - Characterize software development and product attributes that can affect reliability
  - Establish a causal network that estimates the number of defects from software attributes, and then estimates software failure probability from the number of defects
  - Experts opinion elicitation is used to identify attributes, construct causal network, quantify the causal relationship and apply the model to the ATR LOCS system





Path Forward

- Publish STM results in a NUREG/CR report
- Complete BBN research and publish results in a NUREG/CR report
- Update digital I&C research plan to reflect next phase of work
  - Hardware failure data collection
  - Software reliability modeling
  - Digital I&C dependency modeling
  - Safety design features (fault tolerant, online surveillance, etc) modeling
  - Development of regulatory guidance for modeling DI&C systems in NPP PRAs

Digital Instrumentation & Control Projects

- Digital System Failure Modes
- Modeling Digital I&C in PRA
- Techniques for Failure Prevention and Mitigation
- Hazard Analysis Demonstration Project

Ray Torok
EPRI

Advisory Committee on Reactor Safeguards
July 8, 2015

Update on EPRI Digital I&C Projects
Key Points/Conclusions

- Problem statement: Potential digital failures, including common-cause failure, that result in loss of critical system functions (e.g. as expressed in SECY 93-087)
- Much progress in recent years:
  - Understanding of digital system failure modes and measures to prevent / mitigate them
  - Industry standards and guidance
  - Application of probabilistic risk assessment (PRA) to develop risk insights that help identify and address potential vulnerabilities
  - Advanced failure/hazard analysis techniques to identify and address potential vulnerabilities
- Time to apply updated knowledge and tools in plants
- Work ongoing by industry to update their guidance and plant procedures – EPRI supporting with technical guidance and tech transfer

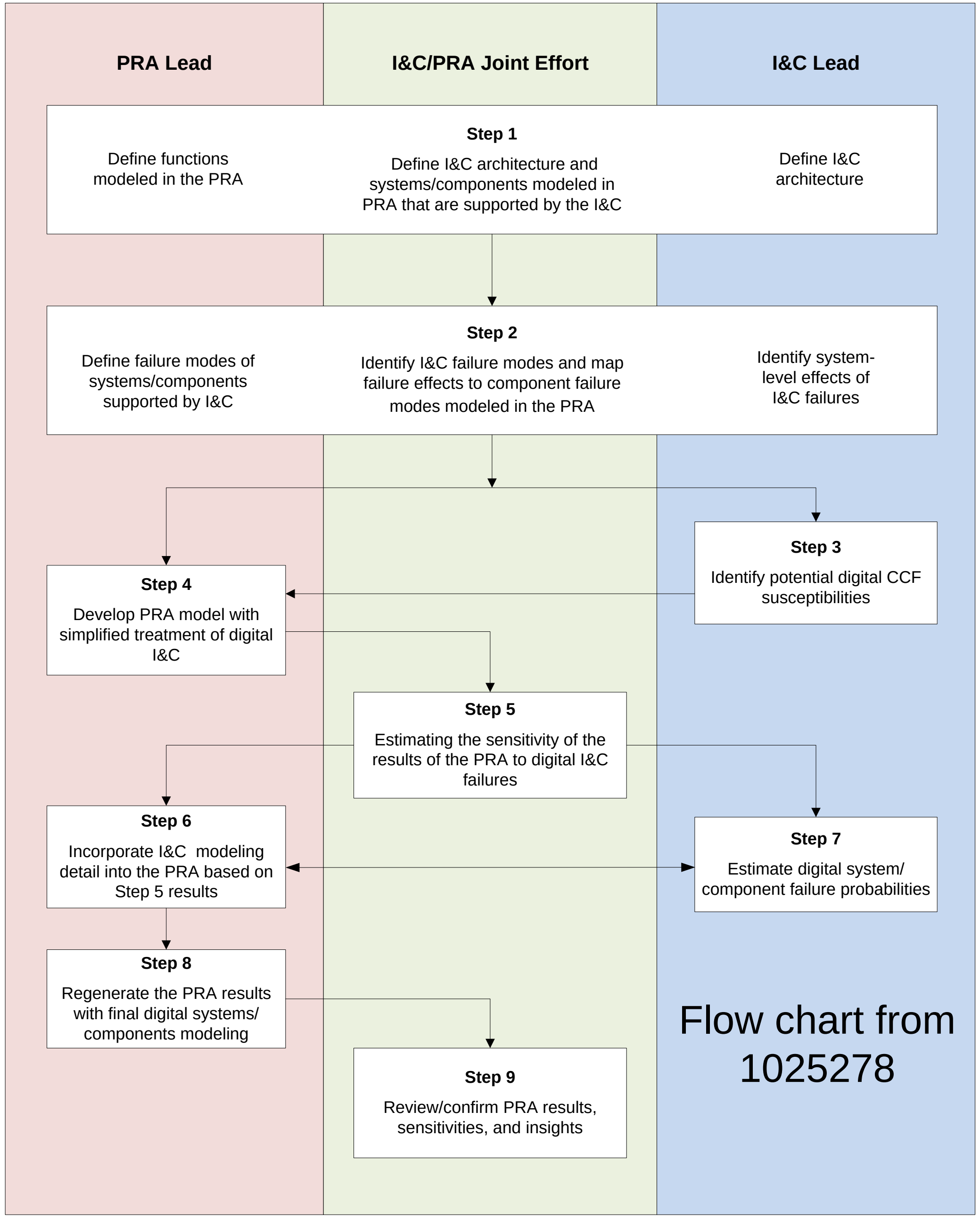
Our ability to ensure high dependability of critical digital systems has improved significantly since the SRM to SECY 93-087

1. Digital System Failure Modes

- Issue – Compatibility of EPRI and NRC Research treatments
  - Terms
  - Coverage / Level of interest
- Want consistent understanding of failure mechanisms, modes and effects for digital
- Important in PRA, hazard analysis, managing digital failure susceptibilities
- EPRI and NRC Research periodic meetings to share information
- For today's discussion - NRC Research addressed the details

2. Modeling Digital I&C in PRA

- EPRI projects started in 2004
  - Diversity and defense-in-depth
  - Estimating failure probabilities
  - Modeling level of detail
- Latest - *Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments.* 2012. (EPRI 1025278)
- Modeling is joint effort involving both I&C and PRA experts – considers:
  - I&C functions in context of the integrated plant design
  - Defensive measures in processes and designs that affect failure probability
  - Software is different – behaves **deterministically,** doesn't wear out, "fails" in unanticipated conditions



Flow chart from 1025278

EPRI ELECTRIC POWER RESEARCH INSTITUTE

2. Modeling Digital I&C in PRA
Insights

- Helpful to model digital systems in the PRA before they are installed:
  - Understand relative importance of I&C, full scope of the effects
  - Reliability target for I&C to be small contributor to risk
  - Influence the design
- The I&C can be designed such that the PRA is insensitive to its misbehaviors
  - To manage risk, the digital system reliability need only be similar to that of a comparable analog system
  - The defense-in-depth and diversity (D3) in the mechanical and electrical systems dictates the level of D3 that may be of value in the I&C

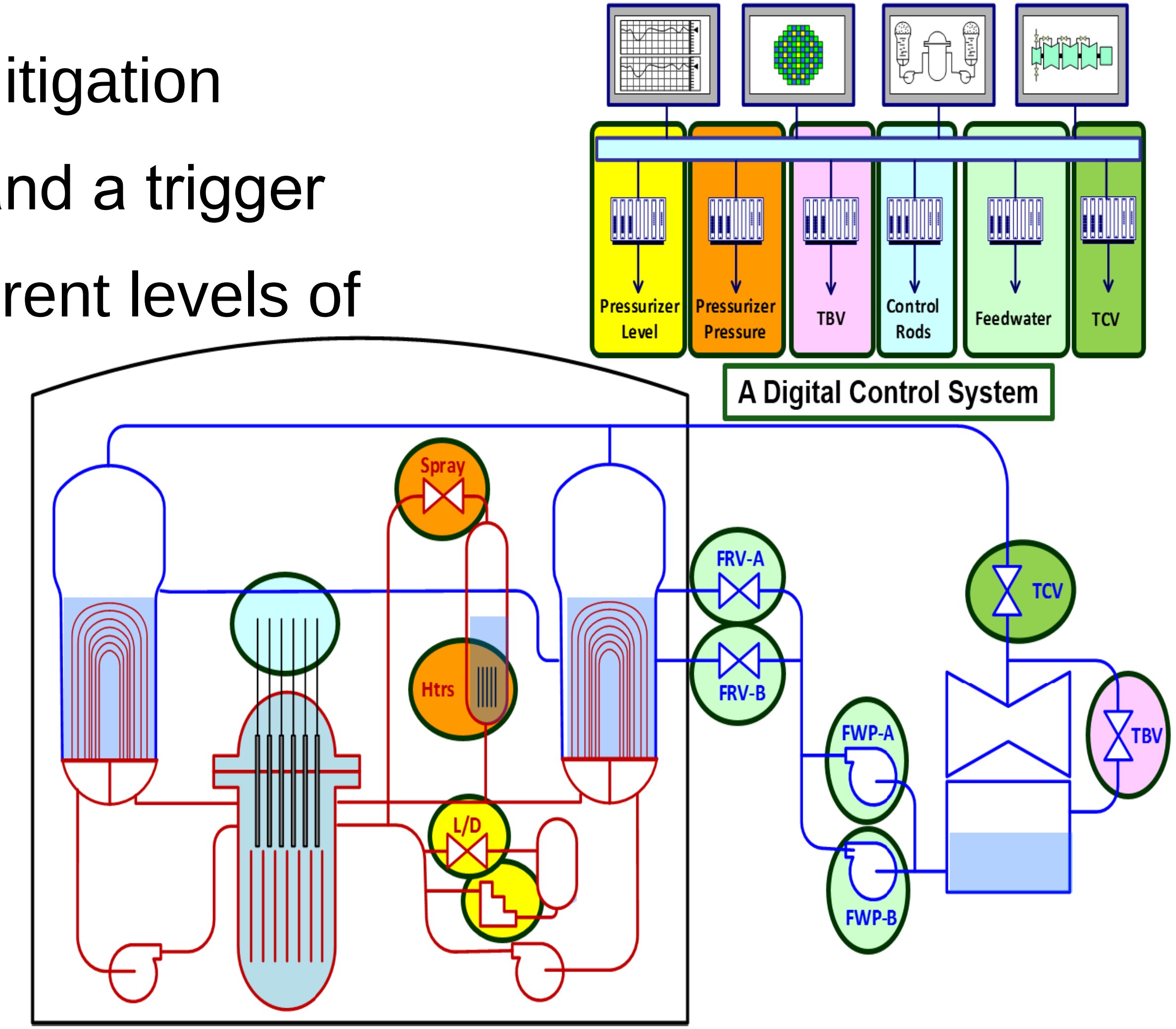
3. Techniques for Failure Prevention and Mitigation

- Ongoing project on assessing and managing digital failure/misbehavior susceptibilities, including common-cause failure (CCF)
  - Extend failure mode discussion to practical treatments and solutions
  - Apply results and lessons from earlier EPRI projects, industry standards, and industry guidance
  - Address safety and non-safety applications
  - Publish guideline late 2015

- More holistic approach
  - Assess susceptibility to failure/misbehavior of I&C and controlled components
  - Credit preventive measures (including diversity)
  - Apply risk insights
  - Use coping analysis where appropriate
  - Apply engineering judgment to assess overall protection
  - Document results in assurance case

3. Techniques for Failure Prevention and Mitigation

- Concepts / principles
  - Protection consists of prevention and mitigation
  - Software "failure" needs both a defect and a trigger
  - Protection can be accomplished at different levels of interest in plant architecture
  - Common-cause failure (CCF) has several contexts and initiators
  - Graded approach based on safety and operational significance
- The goal: assurance of adequate protection against effects of failures



EPRI ELECTRIC POWER RESEARCH INSTITUTE

3. Techniques for Failure Prevention and Mitigation

Assurance of Adequate Protection

Many potential contributors to assurance, e.g.,

- Traditional hardware practices - quality assurance, qualification testing, etc.
- Software development practices – e.g., standards, coding practices, etc.
- Defensive design measures in software, hardware, architecture, procedures, operation, etc.
- Mitigation and coping capability
- Extensive test coverage
- Performance records
- Risk and safety analysis insights
- Simplicity of digital platform and application

Consider the evidence and apply engineering judgment to determine whether there is adequate protection

4. Hazard Analysis Demonstration

Project Objectives

- Trial application of EPRI guideline - *Hazard Analysis Methods for Digital Instrumentation and Control Systems* (EPRI 3002000509)
  - Looks at 6 methods – failure modes & effects, fault tree, etc.
- Capture lessons learned
  - Efficacy of methods
  - Learning / applying novel method

Approach

- Plant takes lead in performing hazard analysis
- EPRI team provides training, coaching and reviews

4. Hazard Analysis Demonstration
Palo Verde Exciter Replacement Project

- Replacing main generator exciters on three units (non-safety, but critical to generation):
  - Each exciter system (controller, rectifiers and peripherals) to be in its own new building, adjacent to turbine building, with dedicated HVAC
  - Building HVAC is critical to generation (i.e., less than 10 minutes before rectifiers overheat on loss of HVAC)
  - Each exciter system building is equipped with three redundant HVAC units, each sized for 100% heat load
- Hazard analysis methods applied to HVAC – primarily *Systems Theoretic Process Analysis* (STPA)

4. Hazard Analysis Demonstration Results
"Substantial Gain With Minimal cost"

- Increase project success
  - Discovered unanticipated failure modes
  - Improved Design, Testing, Procedures, Training, Configuration Control, etc.
- Additional benefits
  - Increase staff knowledge
    - System training
    - Hazard analysis training
    - Facilitate handover to site personnel
  - Quick turnaround allows changes prior to implementation
  - Hazard analysis report helpful in design modification package
- Future plans
  - Investigating application to other projects

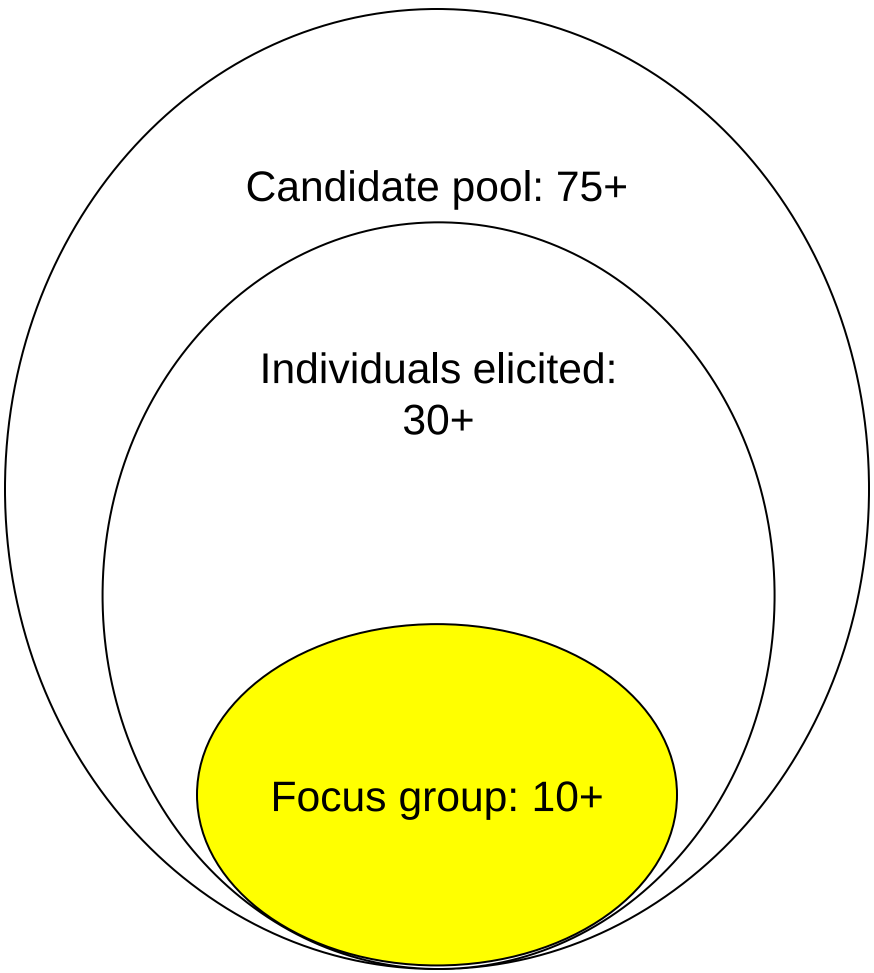
Together…Shaping the Future of Electricity

ELECTRIC POWER RESEARCH INSTITUTE

Backup Slides

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

DE Expert Elicitation



- Significant technical knowledge and experience contributing to project objectives
  - Safety-/mission-critical DI&C systems
  - Elements of the NPP application domain
- Broad and integrative rather than narrowly specialized perspectives
- Ability to identify influencing factors and their inter-relationships
- Ability to identify failure modes, their causes, and their interrelationships
- No conflict of interest
- Availability

Failure Mechanisms, Modes and Effects

- Failure mechanisms produce failure modes which in turn have failure effects on the system [NUREG-0492].

- As the level of analysis becomes more detailed:
  - Failure mechanisms become failure modes at the next level
  - Failure modes become failure effects at the next level

Level of Detail	Failure		
	Mechanism	Mode	Effect
Train	Valve Fails to Open	No Flow	
Component (Valve)	Stem Binding	Valve Fails to Open	No Flow
Subcomponent (Stem)	Corrosion of Stem	Stem Binding	Valve Fails to Open

Digital System Failure Mode Terminology

Term	WGRisk/DRA	DE
Fault	Defect or abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function (IEC 61508; "defect" added) [WGRisk].	The state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources (IEC 60050-191: IEC Vocabulary) [RIL-1002].
Failure	Termination of the ability of a product to perform a required function or its inability to perform within previously specified limits (ISO/IEC 25000:2005) [WGRisk]. Software Failure - The triggering of a defect of software, which results in, or contributes to, the host (digital) system failing to accomplish its intended function or initiating and unwanted event. [DRA Workshop]	The termination of the ability of an item to perform a required function. (IEEE Standards Dictionary, IEC 60050-191: IEC Vocabulary) [RIL-1002].
Failure Mode	The physical or functional manifestation of a failure (ISO/IEC/IEEE 24765:2010) [WGRisk].	The effect by which a failure is observed to occur (modified from definition 1 in IEEE Standards Dictionary) [RIL-1002]. The manner in which failure occurs. (modified from definition 4in IEEE Standards Dictionary) [RIL-1002].

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Common Concepts in Selected Terminology

Term	Common Concepts
Fault	Unintentional impairment of desired or correct functioning. Faults are often revealed when triggered by a condition that was not considered or not thought possible to occur. Faults are systemic.
Failure	The termination of the ability of an item to perform a required function.
Failure Mode	The manner in which failure occurs.

United States Nuclear Regulatory Commission
Protecting People and the Environment

RIL-1002 Cites DRA Research

- Set I and Set J in RIL-1002 were generated by DRA sponsored research projects.
- Set J: WGRisk Failure Mode Survey
  - Classify and organize digital I&C failure modes for the purposes of NPP PRAs or PSAs
  - No complete set of failure modes is developed
  - This taxonomy was demonstrated by an example study
    - Failure to actuate
    - Failure to actuate in time
    - Spurious actuation
    - Adverse effects on other functions
    - Loss of function
    - Loss of communication
    - No actuation signal when demanded

RIL-1002 Cites EPRI Research

- Set K was added to RIL-1002 per ACRS comments.
  - No function
  - Partial function
  - Over function
  - Degraded function
  - Intermittent function
  - Unintended function
- Set K was found in EPRI report: Hazards Analysis Methods for Digital Instrumentation and Control Systems.

MELLLA+ Design and Analyses

George Inch
Senior Staff Engineer, Exelon
Nine Mile Point Nuclear Station

Exelon Generation.

Limitations and Conditions

- NMP2 Complies with all applicable Limitations and Conditions
  - 14 applicable section 9 Methods SER (NEDC-33173P-A rev 4)
  - 47 applicable section 12 MELLLA+ SER (NEDC-33006P-A rev 3)
  - 4 section 5 DSS-CD SER (NEDC-33075P-A rev 7)

- Operating Flexibility Limitation and Condition Compliance
  - 12.5.a: Technical specifications amended to prohibit operation in Single Loop Operation (SLO) in the MELLLA and MELLLA+ region
  - 12.5.b: The existing NMP2 License Condition 7 restricts operation with FW heating to within 20 degrees of the design FW temperature which satisfies M+ LTR SER Limitation and Condition
  - 12.5.c: The NMP2 MELLLA+ COLR includes the NMP2 plant specific power-flow map specifying the license domain

Exelon Generation®

Key Features of the NMP2 MELLLA+ LAR

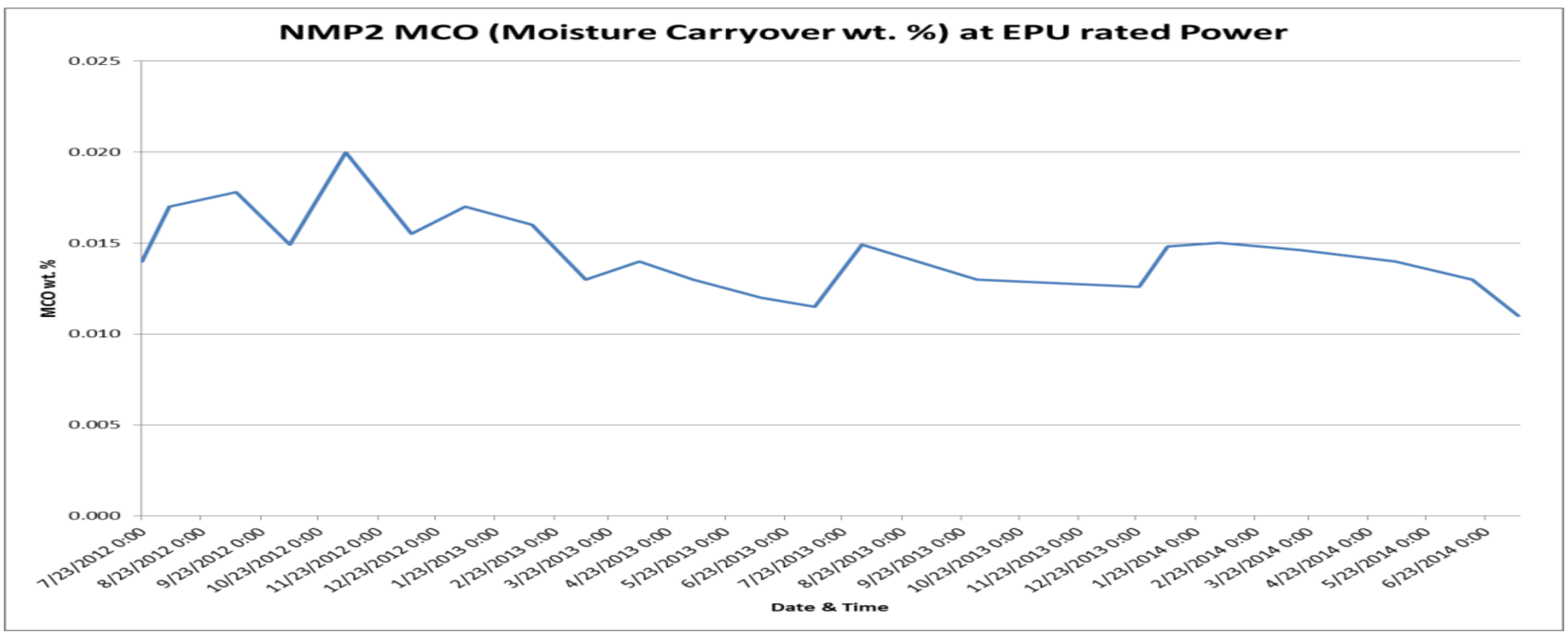
- Design and Analysis credits Boron-10 92 atom % to maintain margin to HCTL (Heat Capacity Temperature Limit) as per MELLLA+ LTR L&C 12.18b.
  - Improves Margin to HCTL compared to EPU conditions by reducing impact on suppression pool temperature
  - Increases Standby Liquid system pump redundancy
- Design and Analysis credit NMP2 Redundant Reactivity Control System (RRCS) design attributes for automatic injection of Standby Liquid control System (SLS) and automatic feedwater flow runback
  - Improves operator action response time requirements to mitigate ATWS for MELLLA+

NMP2 Redundant Reactivity Control System

- The NMP2 Redundant Reactivity Control System (RRCS) system includes two automatic features important for ATWS with Core Instability (ATWS-I) considerations:
  - Automatic SLS pump start on Hi reactor pressure, with APRMs not downscale
    - Nominal delay setting 98 seconds (RRCS has digital timers with minimal setpoint drift)
    - Analysis assumes 120 second initiation delay
  - Automatic feedwater runback on Hi reactor pressure, with APRMs not downscale
    - Nominal delay setting 25 seconds
    - Analysis assumes 33 second initiation delay
    - Runback from 100% to 0% in 21 seconds and automatically open FW pump minimum flow
- Operator actions required for Dual Recirculation pump trip where Hi reactor pressure is not reached:
  - Initiate manual scram within 20 seconds
  - Initiate manual FW runback within 270 seconds

NMP2 MELLLA+ Predicted MCO & EPU Operating Experience

- Maximum calculated MCO = 0.236 wt% for M+ conditions Point N (EPU rated / 85% core flow)
- Analyzed for MCO up to 0.35 wt%, Outboard MSIV is limiting component restricting MCO to below 0.25 wt%
- Actual EPU operating Main Steam Moisture Carryover (MCO) remained essentially unchanged from Pre-EPU power level measured MCO
- The EPU/MELLLA+ transition core has similar characteristics



Exelon Generation.

NMP2 MELLLA+ Testing

Tests	Basis	Variability
22- Pressure Regulator Setpoint Changes	Core responsiveness to pressure perturbation at the M+ rod line / higher void condition	Low - Sensitivity dominated by M+ rod line
23A- Water Level Setpoint changes	Core responsiveness to feedwater injection at the M+ rod line / higher void condition	Low - Sensitivity dominated by M+ rod line
99A- Neutron Flux Noise	Confirm APRM and LPRM noise remains bounded by setpoint calculation assumptions	Low - Sensitivity dominated by M+ rod line, possibility of increased bi-stable flow effects
99C- Stability Monitor Performance	Monitor OPRM data and confirm the plant noise level is within the expected range	Low - Sensitivity dominated by M+ rod line
1B-Steam Moisture	Test established MCO baseline at multiple points in M+ region	- This is a baseline test, results are sensitive to cycle exposure rod patterns - Core design monitored through cycle by procedure
99B -TIP Power Distribution 19 – Core Performance	Test results assessed against cycle specific predictions	- This is a baseline test, results are sensitive to cycle exposure rod patterns - Core design monitored through cycle by procedure

MELLLA+ Operator Actions, Validation and Training

Dan Cifonelli
NMP2 Shift Manager, Exelon
Nine Mile Point Nuclear Station

Exelon Generation.

Time Critical Operator Actions & Validation

Two ATWS-I Mitigating Strategy Operator Actions have been re-classified as Time Critical Operator Actions.

1. 20 seconds insert a Manual Scram using the Mode Switch
   - Provides additional Scram signal and bypasses the low pressure MSIV Isolation

2. 270 seconds to Terminate and Prevent injection in a dual Recirc Pump Trip
   - Step L-9 in N2-EOP-C5, Mitigates power oscillations to a PCT of 912°F

These actions times were validated in September 2014 per OP-AA-102-106, Operator Response Time Program.

1. A validation team including Engineers, Qualified Simulator and Operations Instructor, Shift Manager, and four active on-shift operating crews during a 5-week training cycle
2. The crews performed each action (Scram, Terminate and Prevent Injection into the Reactor Vessel (T/P)) while controlled by Qualified Instructor and Observed by Validation Team Members (time data captured by simulator computer and observers using watches)
3. Five scenarios were used for Scram data, one (Dual Recirc Pump Trip) used for T/P data gathering
4. Validation included minimum staffing review to test sensitivity of time to reduced staff. Reduced staffing had no measurable impact on times due to procedural priority, operator knowledge/proficiency, simplicity of tasks and action performance requires one operator.

Time Critical Operator Actions & Validation Results

Validation Results

1. Time Action 1: 5 to 16 seconds with an average of 8.5 seconds
   - Average Time is 43% of Required Time (20 seconds)

2. Time Action 2: 150 to 232 seconds with an average of 193 seconds
   - Average Time was 71.5% of Required Time (270 seconds)

3. Demonstrated times have significant margin to required times, which account for uncertainties, stress, event recognition, action planning, team communication and verification practices.

4 Required recognition instrumentation, controls manipulated and operator actions can be performed in front panels of the Control Room by a single operator.

5. Actions are controlled by formal procedures.

6. Validation reports were submitted to the NRC post Simulator Audit.

Actions are consistent with current Operator training, knowledge and proficiency. No procedure changes or training changes are needed to assure actions are met. The importance of timely reduction of reactor vessel water level to below the feedwater sparger to reduce subcooling and mitigate oscillations in an ATWS, has been and is reinforced during Licensed Operator training.

Operator Training and Readiness

- June 2014 Initial Classroom Training
- August 2014 Initial Simulator Training
- January 2015 Classroom/Simulator Reinforcement
- May 2015 Reviewed Industry Instability OE
- July 2015 Simulator Continuing Training
- Just In Time Training for Implementation

Conclusion: Operations is ready for MELLLA+ implementation

End of Open Session

Exelon Generation.

ACRS Full Committee Meeting

Nine Mile Point Nuclear Station, Unit 2

Maximum Extended Load Line Limit Analysis Plus (MELLLA+)

July 8, 2015

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Opening Remarks

Travis Tate

Acting Deputy Director
Division of Operation Reactor Licensing
Office of Nuclear Reactor Regulation

Opening Remarks

Michael Dudek

Acting Branch Chief
Division of Operation Reactor Licensing
Office of Nuclear Reactor Regulation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Introduction

Bhalchandra Vaidya

Project Manager

Division of Operation Reactor Licensing

Office of Nuclear Reactor Regulation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Review Timeline

- November 1, 2013 – MELLLA+ application submitted to NRC
- Acceptance Review completed with Supplemental Information from the Licensee on January 21, 2014. Additional Supplemental Information Received on February 25, 2014.
- Revised Application Dated June 13, 2014, to reflect the completion of Implementation of changes related to Standby Liquid Control System received.
- Multiple rounds of RAIs Issued to Licensee on the topics of Reactor Systems, Instrumentation & Controls, Human Factors, etc. Licensee responses received between March 10, 2014 to February 20, 2015.
- The NRC staff performed audit at NMP-2 on Nov 20, 2014

Licensing Actions Related to MELLLA+ Amendment

The licensee's existing license condition and the proposed technical specification changes support the MELLLA+ Application

- Proposed technical Specification change for TS LCO 3.4.1 prohibits single loop operation in MELLLA+ domain
- Existing license Condition 7 restricts Feedwater Heater out of Service by imposing a 20ºF FW temperature band

Licensing Actions Related to MELLLA+ Amendment

The licensee's existing license condition and the proposed numerous technical specification (TS) changes support the MELLLA+ application

- Proposed TS change for TS LCO 3.4.1 prohibits single loop operation in MELLLA+ domain
- Existing License Condition 7 restricts feedwater heater out of service by imposing a 20ºF FW temperature band
- Some of the TS changes are:
  - Revision of Safety Limit (SL) in TS 2.1.1.2 by increasing the SLMCPR for two recirculation loops in operation from ≥ 1.07 to ≥ 1.09.
  - Revision of the acceptance criterion in TS Surveillance Requirement (SR) 3.1.7.7 by increasing the discharge pressure from ≥ 1,327 pounds per square inch gauge (psig) to ≥ 1,335 psig.