UNITED STATES OF AMERICA

U.S. NUCLEAR REGULATORY COMMISSION

# BRIEFING ON DIGITAL INSTRUMENTATION AND CONTROLS

FEBRUARY 01, 2011

9:00 a.m.

TRANSCRIPT OF PROCEEDINGS

Public Meeting

Before the U.S. Nuclear Regulatory Commission:

Gregory B. Jaczko, Chairman

Kristine L. Svinicki, Commissioner

William D. Magwood, IV, Commissioner

William C. Ostendorff, Commissioner

APPEARANCES

Panel:

C. Keith Paulson
Senior Technical Manager, Mitsubishi Nuclear Systems

Tom Sliva
Vice President, New Plant Project Management and Construction, Areva

Tom Ray
Oconee Nuclear Station Engineering Manager, Duke Energy

Scott Patterson
I&C Manager, Pacific Gas and Electric (Diablo Canyon)

Gerard Holzmann
Director, Lab for Software Reliability, Jet Propulsion Laboratory, NASA

NRC Staff:

Bill Borchardt
Executive Director for Operations

Jack Grobe
Deputy Director for Engineering and Corporate Support, NRR and Chairman Digital Instrumentation and Controls Steering Committee

Thomas Bergman
Director, Division of Engineering, NRO

Stuart Richards
Deputy Director, Division of Engineering, RES

Pat Hiland
Director, Division of Engineering, NRR

Steve Arndt
Senior Technical Advisor for Digital I&C, Division of Engineering NRR

P R O C E E D I N G S

CHAIRMAN JACZKO: Well good morning everyone. The Commission meets today to receive a briefing on the digital instrumentation and control systems. In recent years, actually I think going back to about 2006, we began a process to really shore up our regulatory infrastructure to ultimately develop the necessary technical expertise, licensing processes and safety oversight approaches for digital instrumentation and control systems. These digital systems offer the potential to improve performance and safety but I think those benefits will only be realized if the systems are properly designed and ultimately successfully implemented. I want to commend the staff for their excellent work on digital I&C issues particularly in developing sound guidance to help licensees and applicants meet our safety requirements.

We have come a long way I think from the first meeting that the Commission had on this issue in 2006. We've developed a very robust infrastructure; have completed work I believe on almost all of the task working groups that were set up to deal with these issues. And so I think today presents a very different picture than from where we were five years ago. But this is certainly an area given the importance of these systems and the continuing obsolescence of existing analog systems, that's an area where it is important to continue to work and ensure that we have an appropriate process and a process that keeps up with the rapidly changing pace of systems in this area. So I look forward to the presentations today and offer my colleagues an opportunity to make any remarks.

OK, great, we will begin then with Keith Paulson who is the senior technical manager at Mitsubishi.

MR. PAULSON: Thank you very much for this opportunity. Mitsubishi appreciates the hard work that the Commission has put in on their design over the course of the several years that we've been working with them on this. And also for the fact that they've been very frank and open and although have not given us indications of what they would like to see in the design, they always comment effectively on our designs and have pointed us in better directions as we move forward. And I think we're making good progress as an overall statement with respect to our review, so thank you.

First slide I would like -- just a brief history review, I don't want to spend much time on this because I recognize that some of this is familiar to you already. But I did want to point the progression with respect to I&C activities. Mitsubishi started the process of being interested in submitting a design control document in 2006. We came to the staff early in 2006, I don't remember the exact date but it was around March or April in that timeframe, to identify our interest in using the USAPWR design which is a derivative of the APWR in Japan and using that as a basis for future U.S. plants. We had no customers of course at the time and that was an issue that we had to deal with.

In November of 2006, Mitsubishi gave its first I&C presentation to the NRC staff. And this was a series of what we call pre-application reviews where we were trying to introduce the design to the staff and show not only the consistency of the design with respect to designs that they were used to seeing in the U.S., but also to provide an opportunity to show some of the differences and some of the places were actually in Japan they moved ahead and I'm going to get more into that later on. Take that as just a note if you want to talk about it more later on, we can do that.

In March of 2007, we presented a series of topical reports on I&C, in fact throughout 2007 even before March we had provided some of our topical reports. We felt that the topical reports approach was very important for us because of the need to demonstrate first of all the sincerity of Mitsubishi, it's capability of building a nuclear power plant but also some of the advanced technologies that have been introduced in the Japanese design that maybe in Japan anyway a bit ahead of what has happening in the United States. The topical report was our avenue of doing that and hopefully getting some of these issues that are normally required to move forward in a design control process, design certification process, getting those out of the way as early as possible.

As you can see that first year although we submitted roughly 12 topical reports, a third of those were devoted to I&C in one way or another, three of them they're listed here and in the software program manuals, which we provided in December. And in that same December timeframe we also submitted our design control document for review and approval.

We received in February 2009, the first RAI's for the design control document on I&C and began wandering through the magic land of I&C approval with the NRC. Next slide, thank you.

The early review of the Mitsubishi systems in general of the DCD but specifically the I&C, was impacted, it started out slowly but was impacted for some obvious reasons. I'll have to say the staff was very honest when we came in and talked to them about moving forward with the design control document indicated that you guys were pretty well booked at that time with other reviews and we were coming in late without customers I am add. And that was almost two negatives that we had to overcome along the way. We recognized that and

did our best and continue to do our best to take account of that and recognize that in the process that's going on in the review. So Mitsubishi's position, was pretty low ranking at the time.

We also had because of the availability of the reviewers and one time, a couple time change in the review team, that also had some impact because there's a natural bringing up to speed so to speak of the new individuals. However, I'll have to admit that was aided and improved significantly by the NRC because they did have one reviewer, senior technical reviewer, that was part of the process the whole time and that does make a difference in terms of minimizing the impact of that relearning or learning process to get up to the same level of knowledge as the previous individuals.

So if I had to identify a status on this I would say, there has been substantial improvement from our point of view. We've had many, many good technical meetings over the course of the last six months. Not that they weren't before that, but we've been able to focus more on what the specific issues are with respect to the design that Mitsubishi is providing. And we've had a number of meetings over the course of the last couple of months that you may be aware of that have focused specifically in those areas and I'm going to next identify some of those areas that have been the primary focus areas for the Mitsubishi design.

Current issues impacting the pace of Mitsubishi's review are primarily two and these probably won't be too surprising to you, maybe the most surprising will be the first one, this is the process of developing a satisfactory software program and in our case software program manuals since we have one for our platform also. And having a basis for that we readily admitted that we

were behind in terms of understanding what that specifically required and it took us a couple of times to kind of get what was being looked for. The staff was also clear that they were looking for more than we had provided in the first couple of tries that we had. And finally after seeing templates that had been provided to other suppliers that had been approved, it helped us at least in the process of moving forward from that point in time. And, in fact, this month we have provided a third try at software program manuals, and have had a basic level of understanding on our part and an acceptance by the NRC part that at least in some of the samples that we have provided, we've reached the right level of information in the software program manuals. So there's has been a good process there where although it took a little bit of learning on our side and using some past history that had been developed by some of the other suppliers we think we've made progress there in where we want to be.

Next slide. The second issue is a fun one and that is the time required based on the design that Mitsubishi had presented in the design control document was complicated, it was complicated for a number of reasons. Probably the two that were most significant was we had what we called an engineering tool attached to the primary system which was continuously operating which gathered information about the reliability and availability of certain systems. And we thought that was valuable to have on a real time basis but it does complicate it because it's not a safety level system.

The second area was that our operational VDUs use a bi-directional approach rather than a mono-directional approach. So we had two issues that the staff believed were complicating the design and could cause significant delays in the overall review. From a status point of view, we've made

modifications in the design. Those modifications we think provide the basis for moving forward even though we have not completely eliminated the bi-directional aspects. We have prevented we believe in the design any possibility of the control of spurious signals from interrupting safety systems and that's what's being reviewed right now. Although we have no final indication from the NRC, they are reviewing it and have been at least positive with the progress that we're making in this area.

OK, I would like to move on now quickly to lessons learned. I think that there are a number that we can use and I also will try to take lessons learned and move forward with respect to some possible benefits that those lessons learned may have taught us and some ideas on things to be doing in the future. As you know the issue of digital I&C is not digital I&C systems for control and protection are not new; they've been around for many, many years and have been in the review process for many years to the point that the staff took an aggressive move with the interim staff guidance activities for interdivision data communications for defense-in-depth and diversity and the licensing process and putting those into a process that now provides good guidance with respect to moving forward on I&C designs. The lessons learned there we believe is from our point of view anyway, we believe that these ISGs were meant to fast track the I&C approval process. Probably hasn't happened yet, but that is certainly a good start and one of the things that we're hoping to look for are ways of taking advantage of what exists today as a broad knowledge with respect to I&C and how to move forward with respect to actually achieving the fast track.

Just a couple of other quick ones, a concern of ours because I think it has happened to us, but also possibly to some of the other suppliers and that is

because of schedule pressures with respect to customers and so forth, maybe we've made decisions that weren't the best to simplify our systems in order to move the regulatory process forward. I don't want to get into that too heavily but it's something to keep in our minds I think as we move forward with additional evaluations of how to make the review of I&Cs more complete and maybe faster with respect to moving forward with some of these issues like bi-directionality and of course from our point of view the definition of what is necessary from a software program manual point of view and the level of detail that is necessary in that document.

And the last lesson learned that I want to mention is that from the point of view of how the staff and Commissioners of course look at I&C as an important issue. And I was interested in your opening comments that you did focus on operating plants as well as new plants. I think that's an issue with respect to how staffing in the future from your point of view, and the importance of I think an issue that is going to be difficult for the industry to deal with as we deal with obsolesce. So let me move on from that, I wanted to mention just a couple of quick things about the Mitsubishi design that --

CHAIRMAN JACZKO: I'm going to ask you if you can wrap up, I think you're on your last slide so if you can try to wrap up so we can keep it moving.

MR. PAULSON: Mitsubishi has already implemented digital I&C; that's a benefit so there's a complete design available. The Japanese regulatory activities have been completed basically for the design. That doesn't mean that it's something that the NRC doesn't have to worry about but clearly it provides a basis because they use many of the same bases for evaluation although the

process is different but things like IEEE and so forth are fundamental in their design process. And availability of complete design information should help future activities.

Just two as I said, fast tracking on the last slide, this is some of the areas to address or possible areas that could be addressed that as to rekindle the ISG efforts using the information that we have complete design and so forth, using risk informed decision making as a basis for making decisions rather than a more deterministic approach, using the complete design information that exists in the industry now as looking for ways of getting beyond the DAC process and looking more at the ITAAC process for acceptable design whether it's by bi-directionality or uni-directionality. Prudently expand the staff to look at what's happening with respect or what could happen in the future with respect to activities both on the operation on the new plant side. To focus based on industry commitments focusing on independently not collaboratively and in this new plant area, and the last is a point I want to be considered and I hope that some of the other analyst pick up on this is to reconsider the operating plan upgrade requirements to focus on front loaded risks rather than what seems to be a risk that's loaded later in the process, which is not true of the Part 52 process.

CHAIRMAN JACZKO: Thank you.

MR. PAULSON: Thank you.

CHAIRMAN JACZKO: I'll now turn to Thomas Sliva, vice president, New Plant Project Management and Construction at Areva.

MR. SLIVA: Mr. Chairman, thank you, we're pleased to be here with you again. When I listened to Keith's comments on Mitsubishi's design

experience with new plants under Part 52 in the design certification process it very much parallels Areva's own when we started on the relatively long road to the acceptance of our digital design for new reactors. And we were really looking at the 2006 benchmark taking to heart, you know, the industry goal. Total industry goal with an emphasis on review that would be stable, predictable and would be done in a timely fashion; and I think in 2006 everyone agreed that was possible, everybody agreed that digital technology was a good thing and its application to the commercial nuclear industry would also be a good thing.

We started our design with digital technology, not just looking at it as a replacement for the analogue systems where we were going to digitize the existing analog configuration. We really wanted to take advantage of digital technology to enhance those systems and provide some functionality that the analog predecessor couldn't provide. Along that way we realized that there were several difficulties in communicating with the regulator on how digital technology fit into the paradigm of safety, how digital technology could be demonstrated to be proven to be as effective and reliable as analog technology.

And in April of 2006 after starting the process very much in the same fashion as Mitsubishi did in the submittal of topical reports in preparation for the submittal of the design certification in 2007, we started frequent interactions with the staff to try to explain the details of our digital design, how that digital design relates to the analog components that it was supposed to replace and how that visual technology was inherently safe and that the futures being introduced by that technology would improve the overall reliability, effectiveness of control and potentially the safety of the plant. Along a path very similar to Mitsubishi, we worked with the staff on trying to finalize the end goal.

What did we have to demonstrate with the detail of the design, where the design was coming from and how it functioned in order to give the staff the comfort to make a safety determination. And along the same time line as Mitsubishi we reached some conclusions on the complexity and how to simplify our design, basically a two step process that really concluded in the summer of 2010, where we felt we had reached equilibrium with the staff, where we simplify our design, where we did offer solutions or we felt we offered solutions to the staff on some of the issues they felt were extraordinarily complex in looking at digital technology. And I think we reached a basis of understanding of how to proceed forward with the review. When we go to the next slide, our slide 3, again – in new reactors I found we loved timelines, you know, it's running a marathon, not a sprint. Part of what we struggle with with the staff, and I think with the Chairman's comments, we have improved the guidance. But the guidance has been issued during the review process.

So, I think it forced both the reviewers and the designers to make some mid course corrections that perhaps challenged the timeliness of the review, perhaps put issues on the table that were not considered when the review process was started in its infancy in 2006.

And this timeline shows, basically, the issuing of the guidance, which I also agree with Keith and with the Chairman's assessment, that it's basically very good guidance; it helps clarify the positions on digital I&C, but if you look at the timeline, much of the guidance was issued during the review process. I think that with the change of personnel both on the staff and sometimes in our design organization impacted the timeliness of the review, added some confusion points, and I think they made more difficult to solve the

issue of complexity of digital system systems, and how they related to the analog systems that by virtually being analog, were relatively more simple.

We lost ground every time there was a change in guidance, lost ground every time there was a change in reviewer, lost ground every time we had a design change with one of our designers here. So, I think that also contributed to the length of time. What we have found is that to keep pace with that it really did require frequent interactions with the NRC staff, which the staff has responded to. And we went to monthly meetings and then weekly phone calls to review process and closure plans, and how both the staff reviewers and our designers were progressing on the closing of digital I&C issues.

Again the frequent interactions, I think, by and large, were good. I think they were caused by a shifting mosaic, we didn't start with a well defined endline; it started with a goal of what that endline would be, and in the process of clarifying what that endline should be, there were the mid course corrections necessitated along the lengthy review process.

Right now, we're at a path again, in strikingly similar fashion, to my colleague from Mitsubishi, where Areva's design is working towards we think final closure.

We have agreed with the staff that the final items that need to be demonstrated in design for the staff to make a safety determination. We have committed, in a letter, when we would submit the appropriate design material. I'm happy to say, at this point in time, even though there are slight corrections, in that closure plan, from Areva's standpoint, we are on schedule for delivering the promised technical information per commitment.

Some of the sticky problems, again, and I think this shows

consistency in where we are in digital technology, are very similar to Mitsubishi's in our design where we're really struggling with the resolution of criteria for the correction of the service unit.

We have proposed a solution to the staff that doesn't have constant two-way communication involved with this service unit device, we think that will be proven acceptable to the staff's requirements for this, but again it's a similar issue to what our colleagues had on two-way communications.

We are also struggling with the level of detail required under Part 52 to validate the design in the design certification process. How much detail does it require the reviewer to make a safety determination on the design, recognizing that perhaps the designs is not 100 percent complete at the time of its review.

So, we're working with the staff on adjusting this. Like our colleague, we are struggling with the level of detail that we are going to have to provide to close out the I&C issue and get a determination on the safety of our system for the new plants.

The issues I think, across the board are the same. The defense-in-depth issue is very key to our conclusion of the design, where we recognize analog backup in not required, however, demonstrating that the digital technology in and of itself in the configuration presented, does provide diversity in defense-in-depth, as a challenge on how to sort through and right now we're working on that as a part of our closure can.

Of course, we're making preparations to go with the staff, as requested, and present to the ACRS once we have finalized our closure plan on the digital design. I think, you know, the most perplexing thing that we come up

with when we look at closure, is the level of detail required to make sure that as a regulator you're comfortable with the technology being presented, and that it satisfies the safety criteria that are outlined in the different forms of guidance that we're working to. I think that's the biggest challenge in front of us and the staff as we push the Areva I&C design and design certification to closure.

In closing, I would like to say, digital technology, is, we think, somewhat magical. It does provide opportunities for functionality and reliability that we believe, were not available in analog predecessors. Digital technology, we feel, for the entire industry is important because of the obsolescence issues faced in older analog systems and the fact that the rest of the world is reliant upon digital technology. It's now the standard across the board in every industry in the modern world.

So, right now we are committed at Areva to working closely with the staff on the closure plans. We are committed to ensure that we close out the I&C issues in an effective manner. And what we want to do in that effort, as we close out our existing I&C issues, is to preserve the potential for digital technology, to improve the functionality, reliability, and potentially the safety of the plants, and still achieve a design that's understandable and meets safety requirements as put out in the various forms of guidance by the Nuclear Regulatory Commission.

So, I thank you for the opportunity to speak and look forward to working with you on the final closure of the I&C issues on new reactors and design certification.

CHAIRMAN JACZKO: Thank you. And I'll turn it to Tom Ray, who is the Engineering Manager at Oconee Nuclear Station.

MR. RAY: Thank you for allowing to me to speak today. I'm Tom

Ray, the engineering manager at Oconee Nuclear Station. I'll talk specifically about the implementation of our reactor protection system and engineered safeguards. I know it's of great interest in industry as far as Oconee's progress on that.

Current project status, this is the 13th digital project that we've performed at Oconee. The SCR was approved in January 2010, just over a year ago. Implementation for RPSES, as we called it for unit 1 in April, 2011 -- April 2, to be specific is when we actually start the implementation project. Unit 3 will be in April 2012, and Unit 2 will be in October, 2013.

We tried to put a year between each of the implementations to allow us to plow lessons learned back into the project, so we don't end up having to quickly make changes on those types of things. Since the SER was approved, we've completed all design packages. Site acceptance testing was completed on Oconee Unit 1. Unit 3 site acceptance testing will begin in June of this year, immediately following our outage. All installation procedures have been approved and post-modification procedures have been developed.

Looking specifically on Slide 3, on our testing activities, factory testing activities was performed prior to the issuance of an SER, due to the needs to incorporate the results of factory acceptance testing into the SER to demonstrate the design capabilities of the system. The site acceptance testing mirrored the scope of the factory acceptance test. We did use a slightly different method as in we provided inputs and tested it all the way through to the final output, to demonstrate the diverse methods of testing the system. The site acceptance testing simulated the inputs and then the outputs were actually monitored on a operator aid computer, an enunciated panel, indicating lights and

measured outputs signals so we did a full string test at the site acceptance testing.

The SAT procedures had to develop steps to specifically identify acceptance criteria that needed to be met in order to consider the system acceptable for use. The site acceptance criteria testing, actually tested the system, from all conditions from cold shutdown all the way up to 100 percent power-- we didn't just test it at a full power situation. And our site acceptance testing was observed by Region II inspectors.

On slide 4, looked specifically at our operations and maintenance activities, classroom training was developed for our operators and our maintenance technicians, for our I&C technicians we had to do three weeks of classroom training, an additional two weeks of qualification -- task qualification work was performed for those technicians to get them fully qualified on the new system. Our system engineers attended the maintenance training, classroom training, with the maintenance technicians, so they could sit side by side, hear the questions, see what types of issues that they looked like they were going to have going forward and be prepared for those who have issues once we put the system into service.

Training was specifically based on the type of work each group of would be performing on the system. Maintenance actually looked at troubleshooting activities: how the system operates, the types of troubleshooting activities you can do on the system, what types of outputs or diagnostic information the system provides. Same with the system engineers. Operator training focused more on operating of the system and types of failures that the systems could see.

All the operations and maintenance procedures have been originated and validated. They're currently in engineering for a qualification final review. For the operator training, we have -- at Oconee, we have recently installed a second simulator, so we have two simulators. One of the simulators was upgraded with the new RPSES system. It has capability of swapping back and forth between the old system and the new system. So, we are in the process of training all of our operators on the new system. And all of that training will be completed prior to the shutdown implementation.

MR. RAY: Slide 5. Specifically on the maintenance activities. For maintenance training, we procured a training simulator, it cost us about $1 million to do that but we saw a lot of advantage on that. The maintenance technicians provided a lot of feedback on that simulator. Simulator not only allows them to do training, but actually put their hands on the system, and so they can actually match it up with classroom training.

The training simulator is the full channel for the alpha channel, and then the other three channels are simulated so they have a full channel with all the components to be able to work with it. Not only does this allow us to do training upfront before the system is installed, after the system is installed and operating, should we have issues with the system, it'll give us a training simulator that can go do "just in time" training on priority and troubleshooting activities. When we develop troubleshooting plans for any issues that we have with the system, we'll be able to take those to our training simulator and actually run them through the training simulator to look at issues such as proximity of components, and what problems that can cause, how we'd actually take parts of the system in

and out of service, and the like, such that it's all done in a training environment prior to actually getting on the actual system.

We've currently trained about 20 I&C technicians and they will be fully qualified prior to implementation which starts in two months. All the training on the current system is on site and fully set up in a training environment. At the end of February, it will be packed up and then moved to the station in preparation for implementation in April.

On Slide 6, you see that in the SER there's about 40 inspector follow-up items that are outlined. The inspector will follow up on – broken down into six key areas -- we'll have follow-up activities associated with software plans, the maintenance software plans, and any training that we do for the software, and the installation and changes that are allowed on the software. We have a configuration management inspections to -- that will be going on. Key switch controls is an important one, how we control access to the system both hardware access and software access.

They will be in looking at our operations and maintenance procedures, how we've outlined them, how we do our testing, how we put the system in service and remove it from service, and the like. We have a number of activities that they will be observing associated with our cyber security, associated with system access control, how we use the test machine, the system unit interface, the cabinet alarms, how we actually implement actions associated with how we unlock and get into in any time you access the system will generate an alarm so that needs to make sure that's incorporated. Then we'll also have cyber security self-assessments in audit plans that they will be looking at. And

the last area we'll be looking at is coming in and observing our post-modification testing.

With the post-installation monitoring, we have developed directives to ensure the system engineering is involved early in the design process. We do that so that system engineers can identify those key functions and make sure that they have access to be able to monitor. All of our digital upgrades are considered safety modifications and as a result, by our directives, require post-installation monitoring plan. That monitoring plan will identify all the activities that the system engineer needs to monitor in the first year of operation – the first cycle of operation of that system, to ensure that the system is operating properly. And then after our first cycle of operations, the monitoring will drop to our standard system monitoring plans for our critical systems.

Slide 8. Looking at overall how we control our digital processes. Since 1997, we have had a digital upgrade directive that goes through how to actually control a digital upgrade. Software configuration management directives were implemented in 2005, as a result of -- from previous digital upgrades. The directives incorporate industry operating experience and things that came out of V&V activities or verification and validation activities. And the directives have been updated a number of times, incorporating industry lessons learned around digital upgrades. At this time, that completes my discussion on the implementation of our RPSES at Oconee. Thanks.

CHAIRMAN JACZKO: Now, I'll turn to Scott Patterson, who is the I&C manager at Pacific Gas and Electric.

MR. PATTERSON: Thank you today for the opportunity to speak before such a distinguished group about a project that's very important to PG&E

and the industry. My presentation will cover the background -- some background information on a process protection system replacement project, about where we've been, where we are in the licensing process, and the challenges that we're facing.

In 2003, Diablo Canyon established an I&C obsolescence management program to address aging I&C equipment. We selected a common hardware platform that we could use in many different areas in the I&C world, specifically for safety and critical control equipment applications. The common platform has many advantages, but it does create the question of diversity. So, one question that we had at that time was, “How much diversity is enough?”

We currently have a microprocessor based Westinghouse Eagle 21 process protection system that was licensed and installed in 1994. The system was installed prior to branch technical position 7-19 and NUREG-6303.

So, another question we had was could we just replace the system through the 50-59 process since it was a digital to digital upgrade. BTP 19 and 6303, however, did not provide us with enough guidance to understand the level of diversity that would be acceptable. It was evident that clarification was needed to determine an acceptable architecture with sufficient diversity, whether or not we went back for prior approval.

In 2006, PG&E had two meetings with the NRC staff to discuss our approach and conceptual design. Platform diversity was the main topic, but also the likelihood of a large break LOCA in conjunction with a common cause failure, seemed to be very small, so we questioned whether or not we really needed to add the complexity required to automatically respond to these type of events. At the time, the only way to get formal feedback was to formally submit a license

amendment request or a topical report. So, for PG&E, this approach was considered very risky and expensive. We needed a method of obtaining acceptance of a conceptual architecture and approach before committing the expenditure necessary to develop a license amendment that might be rejected. Slide 3.

Digital upgrades have been a hot topic in the industry and with the NRC. In 2007, as you know, the I&C Steering Committee established the task working groups to address areas of concern that would be beneficial -- where additional guidance would be beneficial. Task working group number two addressed the question of how much diversity is enough. And during those discussions it revealed the issues that concerned both the regulator and licensee. Participating in that task working group enabled PG&E to better understand diversity requirements and to develop an architecture that appeared acceptable to PG&E and the NRC staff. Our experience with the task working group confirmed our belief that a deterministic approach to evaluating diversity would involve less project risk than attempting a risk-informed approach.

The ISG-6 Phase 0 pre-submittal meetings were exactly what we were looking for. Back in 2006, it provided a venue for us to discuss the conceptual architecture, along with other areas that needed clarification, like cyber security and data communications. The meetings provided a forum for open discussion with the staff and allowed us to refine our approach. Formal feedback was provided for each meeting for several important concepts. They gave us confidence to move forward. This interaction with the staff was invaluable to our understanding of the licensing process, what was important

from a regulatory standpoint, and to reduce our project risk. We submitted our diversity defense-in-depth evaluation in April 2010, based on these meetings.

Our diversity defense-in-depth topical report is pending approval, and we are proceeding with application development. We've completed a conceptual design document, a functional and interface requirement specifications and those have been approved and issued to the vendors. Contracts have been let to vendors to proceed with ISG-6 Phase 1 documentation needed for our LAR submittal. We are using ISG-6 to guide us in determining the information needed to be provided with our submittal. And now that Revision 1 is approved, we can refine our documentation.

Our next Phase 0 meeting is this Thursday in San Luis Obispo, California close to our Diablo Canyon, and we'll be discussing several items including how to structure and format our licensing amendment report.

So what is next? We expect to have everything completed and ready for our submittal this summer. We have two vendors involved in our project, with topical reports that are currently being reviewed. These vendor topical reports approvals are essential for our project to be successful. In 2012, we'll be establishing our ISG-6 Phase 2 documentation, and submitting those with an expected approval of our license amendment in 2013 to support an installation in 2014. Slide 6.

Nuclear power is very special and requires more thought to make sure that all areas of concern are resolved. So it is expected to take longer than a non-nuclear project. However, if this process is unpredictable and risky, the utilities will delay replacement beyond maintainable life of installed equipment. So it's very important to provide a process that is easy to follow, provides the

right level of detail of review, and does not accessibly burden either the NRC staff or the licensee.

So here are some of the challenges that we're currently facing. Staying on schedule is the first one. It's always hard to stay on schedule when you're depending on resources that are not under your direct control. ISG-6 took much longer to get approved than it was forecasted originally because of the detailed discussions that went on. Vendor topical reports and our diversity defense-in-depth topical report are taking longer than originally was expected. There's also been some internal budget challenges that have delayed key projects that -- we had one project that had to be installed prior to our process protection system replacement -- that project got delayed so that also delayed our process protection system project.

The ISG-6 process has not been refined; it's just basically come out in Revision 1, so I expect as us being a pilot plant we will require more interface with the staff and more information needed than will be necessary in the future after the process is refined. The required level of detail is, as Areva had mentioned, is still kind of a question for both the NRC and the licensee. For this process to be more predictable a better understanding of what information is required and what level of detail is needed. ISG-6 has attempted to help with this, so as a pilot plant, that level of detail will be tested.

Budget is another concern. Utilities have many competing projects and emergent issues that change the cash flow and affect schedule. This has been an issue in the past as I said previously, and is currently being challenged by several emergent issues that come up for the plant. Demand for money for other critical projects may affect our current schedule. Another area of challenge

is continuity and availability of resources, and I did hear that in a previous speaker. The longer the project goes, the harder it is to keep the same researchers involved. Changing resources requires that they be trained, brought up to speed and integrated in the process, and along with these new people come with new ideas, new questions, and that could slow the process down.

Digital upgrades are complex and require a specialized skill set. Finding enough of the right people to assemble a team and keeping them is not an easy task. Competing projects also affect resource availability not only for PG&E, but vendors have the same issue. New plant designs require many of the same resources, and the opportunities outside of the United States are causing a resource drain throughout the industry.

To conclude, PG&E tends to communicate lessons learned from this ISG pilot plant process. And also to provide the most value in making improvements to the ISG-6, interactive discussions must continue between PG&E and the staff. That's been probably the most valuable asset we have had through these task working groups. The discussions during these meetings are extremely valuable in achieving the guidance that we currently have. These critical discussions must continue to get the greatest benefit.

The ultimate goal for PG&E is to replace our process protection system with a new, more reliable system. In addition, the goal is also to provide feedback to ISG-6 process, to help improve guidance that will reduce project risk, and provide a more predictable and stable licensing environment. And it will improve nuclear safety. That's all I have.

CHAIRMAN JACZKO: Okay. We will now turn to Gerard Holzmann who's at the Laboratory for Reliable Software at the Jet Propulsion

Laboratory in the California Institute of Technology.

MR. HOLZMANN: Thank you. Maybe, by way of introduction, I should say that my approach to the issues that are being discussed here is a little different from that of the previous speakers. I'm a computer scientist, a software engineer. That means I'm one of those people who actually enjoys reading code, and writing code, and analyzing code. I've done so for the last couple of decades, first in the telecommunications industry at Bell Labs and now at JPL. And if you study the issues in software development, the number of trends has very quickly become evident, especially in the last few decades.

One is that there is an exponential increase in the size of software applications pretty much across the industry, no matter which applications you look at, whether they are desktop applications or mission-critical applications or safety critical applications, the size and the complexity of the software is increasing very rapidly. That's a very interesting trend for me as a computer scientist to see and to study the implications of that. The other thing you can see -- of course, I'm interested in finding ways to develop software that is safe and reliable. Of course, there are many, many good ways to apply those techniques, but that means also looking at ways of finding the defects in software. And what you can see is it seems to be a rule of thumb that most people accept that there is a relation, seems to be a linear relation, between the size and complexity of code and the number of latent defects.

Now, a latent defect is a technical term that's a term for the number of defects that escape all the testing and checking at reviewing phases that are normally applied. More rigorous in critical applications than in non-critical applications. So typical -- latent defects and residual defects are those that you

don't catch, so they show up when the system goes in operation. At JPL, of course we look at deep space missions, the residual defects are the ones that show up in flight, and that's where we don't want to have them show up. We want them to show up in testing, in the test beds.

Now, there is a relation between the size of software and the number of residual defects that we find -- which you can see documented in the databases that we develop for the missions that we fly. Doesn't mean that we can't fly missions or that all the missions fail, as you know, most missions do actually succeed. The ones that fail are of the most interest to me, to study why they fail, especially when they fail because of software, and we have a number of those types of issues.

Not all missions are developed to the same standards of rigor. Human-based missions like the shuttle missions, of course, have the highest standards of rigor and they do see residual defects, and they follow the same trends that we see in the other applications. I would like to bring up my Slide number 2 summarizing those issues. One thing that concerns me is that software test methods that are routinely applied in industry pretty much date from the '60s and have not kept pace as much as they should have with the increasing size and complexity of software. We're trying very hard to change that, and there are new developments that are very encouraging, but they've not yet been universally embraced in critical software development. So we're trying very hard to change that.

One assumption that we make at JPL when we design missions is that all software has defects just like any other system components will have defects. There's no perfection in hardware, there's no perfection in software.

Hardware components have breaking points, they wear out, they have tolerances, and the better you understand these tolerances and the types of ways in which components have failed, the more reliable you can make systems operate. Slide 3.

So software we understand to be a component of a system, and we have learned in many other disciplines to make reliable systems from unreliable components. We do that in the telecommunications industry, and send data reliably over imperfect channels, noisy channels, channels with loss or distortion. We've learned how to do that; we can build reliable hardware systems by using redundancy in defense-in-depth strategies, and we can learn to do that in the software. But, in software these principals are applied very differently because the types of failures that you see in software are fundamentally different from the types of failures you see in hardware.

So, software failures, of course we studied that. We've collected, we've built databases of software failures in NASA missions dating back several decades. You see a number of common patterns emerge, and of course it's important that you can recognize these patterns because that's your leverage for preventing those types of failures going forward. So, many of the failures that we have seen in the past we can prevent with the proper risk avoidance techniques. And that spans the entire software development lifecycle, starting with requirements capture, into high-level design, low-level design, coding, testing, and mission operations. There are lots of things you can do to prevent defects from becoming catastrophic failures in operation.

So, one type of defect, on Slide 5, is unintended coupling. So, this issue has been studied by others. One well-known book that studies that issue is

by Charles Perrow. He is a sociologist, but he studied the types of failures that can happen in complex systems, for instance the Three Mile Island near-meltdown. He studied how these failures come about, and one of his conclusions was that if you have a complex system, typically many of the components are designed to be independent. By design they are meant to be independent, and when failures occur there can be hidden dependencies that show up and if you have combinations of failures it is almost impossible to reason ahead of time through the consequences that can occur when a specific combination of failure happens and introduces certain kinds of coupling.

We see that in our space missions as well. If you look at the most dramatic types of failures that we've seen where we lose missions, generally it is because of unintended coupling between system components that were never meant to be influencing each other. So that's an important thing because if you now use proper design techniques and proper analysis techniques you can look for those types of coupling and make them less likely.

Next viewgraphs talks about another common cause of failure in complex systems, which is risk conditions, and that's caused by the use of concurrency, multi-threaded systems, even sequential stand-alone systems that are meant to be deterministic, the environment always provides an element of non-determinacy, a concurrent asynchronous agent that can introduce events into a system that can cause failure. It is very, very difficult to detect those types of failure with standard software testing techniques.

Next viewgraph is my last one, and that is basically summarizing the lessons learned from these observations, knowing that complex, the more complex they are, the larger they are, the more vulnerable they are to residual

and latent defects. If we want to claim safety of a system, for instance for a spacecraft that we want human beings to fly on the spacecraft, we have to provide a really strong case that we believe that we have confidence in the safety of the system and that means that we must provide strong evidence. A strong claim requires strong evidence.

And I've outlined some elements of those types of evidence-based safety claims that should be present and that one could look for. The types of things that we're using at JPL and at NASA are based on the use of standards, rigorous standards, and surprisingly many coding standards that are used for critical software development are not based on risk-avoidance. They are more stylistic and general in nature. At JPL we have developed coding standards that are risk-based that try to exclude the types of failures that we have seen in practice by preventing those types of coding patterns from being used in software in the software that we develop. And we look for those types of -- we look for compliance with these coding standards with tools, like we do mechanical compliance checking, and that requires familiarity with state-of-the-art tools.

The use of static source code analysis technology, it's fairly general now. It hasn't really reached all of the mission-critical and safety-critical industries, really to my surprise, because it's a well-known technology. State-of-the-art static source code analysis tools have been on the market for about a decade now. They are extremely effective in catching residual defects, things that don't tend to show up in software tests in test beds. And so evidence that they have been used in critical software development is really important. And any use of formal design and code verification methods, which is my own expertise in developing these types of tools, that allow you to do design

verification very early in the design cycle.

That concludes what I had to say.

CHAIRMAN JACZKO: Thank you. We will now turn to Commissioner Magwood for the start of questions.

COMMISSIONER MAGWOOD: Thank you Chairman. As I listened to representatives from Areva and Mitsubishi talking about the process they've gone through -- and reaching back to 2006 is I think when you first got started in this process -- I can sort of hear the agony in your voice as you talk about the steps you've taken to try to get to this point. That sounds like a long time, but I remember having conversations about digital I&C systems in fact somewhat with NRC staff back in the late 90s, and a lot of these issues were coming up in those conversations, even back then. And obviously we didn't solve them back in the late 90s, otherwise we wouldn't be talking about them now. But it's clear that this is something that represents such a major shift in how we approach control systems in nuclear plants, that this agency has sort of taken a very careful and conservative approach to that change, and I think that's appropriate given the technologies we're dealing with. I think in the aerospace industry -- not so much with space flight but more with aerospace generally -- there seems to be a little bit more of an aggressive approach to incorporating technology. I think it was even perhaps in the early 80s that we started hearing about electric jets. I think the F-16 was the first one they called the electric jet, and that was kind of a big breakthrough and everyone was really excited about that in aerospace. But even though there were a few Luddites that seemed to think that maybe we're moving too fast and you never know what could happen with the software, in the aerospace area they kind of punched through that and now it's pretty standard to

have very advanced digital control systems in aircraft.

Now, another place where there is a lot of digital technology being used is overseas, and a question I have for both of you two is, when you look at what's been implemented in Japan and in France and in other countries, did you find that the process of engaging with NRC was substantively different in how our reviewers looked at these digital technologies versus how reviewers in Japan and France have in the past looked at them and perhaps are looking at them today? Keith, maybe you'd like to start.

MR. PAULSON: That's a good question. The issue in Japan was focused more on a recognition of paths for acceptability. Let's just take as an example what went on in this area of bi-directionality. It seemed that there was an acceptance of certain approaches to dealing with bi-directionality that we're still discussing with the staff. I can't tell you whether or not they reviewed it as thoroughly as the staff believes they have to, but I think that there is a basis there for getting feedback with respect to what they looked at and why they concluded that what went on was consistent with an acceptable approach moving forward. That would be a suggestion that I -- if you look at my last overhead, that I think -- there is a suggestion there of some interaction as to how some of these more difficult issues were solved or addressed or what the stopping point was with respect to their acceptance of a specific design.

MR. SLIVA: I agree it's an interesting question to address. Our experience, because we were approaching I&C design in actually four different Western countries, France, England, Finland -- which we now consider in the West -- and the United States. The interesting thing about the regulators is everybody has a slightly different pet peeve, so to speak. So, trying to achieve

consistency among the four sovereign entities that are looking at the same basic design has been a struggle. The common thread, though, is that the level of detail required, which again varies. The process in France is much more akin to the Part 50 process that we went through with the Gen-2 plants. The level of proof therefore established to go forward with the design is less detailed than we're asked to provide to the U.S. NRC. Finland is somewhere in between. It's kind of our modified Part 50 process with some proofs for Part 52 thrown in, where there are some aspects that have to be proven in extraordinary detail to justify going forward with design. There are other aspects of working with the Finnish regulator that allow more of a Part 50 evolutionary process prove-as-you-go type of mentality, and England just has almost a completely different approach, though the concerns in the United Kingdom are closer to the concerns raised by the NRC staff than the other two Western regulatory bodies. So, we found it varies from country to country, and the greatest difference is the level of detail on the design that we've been asked to provide in the different sovereign jurisdictions, to satisfy the particular safety-authority regulator. We really have not found complete equilibrium among the regulators, and the acceptability of some aspects of the design in the United States is some items that are being questioned, for example, in the United Kingdom.

Commissioner, I wish I could give you a better answer, because it would make my life a lot easier, because I do have oversight of some aspects of the European projects as well.

COMMISSIONER MAGWOOD: I appreciate that. And Mr. Chairman, I know my time is up, but I'd like to ask one follow-up. Again, for both of you, if you can make just very brief responses -- both of you have mentioned

that or alluded that there is technology that you leaving behind in going through the process of having your systems reviewed by NRC. Are the changes that you're making to simplify your systems, are they the sorts of changes that, as we go forward in the future, and as you have more time over the course of say a decade or so to look to technology and meet the concerns of the reviewers, are these things that can be reintegrated back into the system after the fact, and that you can regain some of the functionality that -- if they are ultimately approved -- that you would like to see?

MR. PAULSON: Once again you are spot on I think in one of the issues that we're dealing with. But I think the answer to that is yes, I think it can be, and in fact some of the changes that we've made for example like the engineering tool, the attachment of the engineering tool continuously as opposed to periodically is one that we can reevaluate along the way. I would hope also that there is a reevaluation of some of the design modifications we're making to justify certain aspects of the design that could ultimately be simplified based on a probability approach or a more detailed analysis. The staff has never said that our approach is not acceptable. What they've said is it will take a lot of detail to review the design, and what I'm hoping as we go through that process is we'll enlighten ourselves on ways to improve and simplify the design even more.

MR. SLIVA: I agree with Keith's remarks, and we've had exactly the same experience with the staff. The staff has not rejected any aspects of the design. They have remarked to us that to go forward with the design -- we made some modifications aimed at simplification that would require a significant amount of time, and the proofs we would have to submit with the design would probably be fairly difficult for us to do in a timely fashion. I do think, though, that

we are looking at ways to continue to develop our designs so that those features can be reintroduced with the proper level of proof as some of the regulations and comfort is developed with digital design in the future.

COMMISSIONER MAGWOOD: Excellent. And I thank all of you for your testimony today. It's been very helpful. Thank you Chairman.

CHAIRMAN JACZKO: Commissioner Ostendorff.

COMMISSIONER OSTENDORFF: Thanks Mr. Chairman, and I add my thanks to Commissioner Magwood. This has been very informative. I have three questions I'm going to try to get out here. I want to do this very quickly, and pick up where Commissioner Magwood was headed in the concern that comes across in the slides in your presentations about perhaps some sub-optimization of safety features as a result of the regulatory process. I want to ask Mr. Paulson and Mr. Sliva, is there one example -- if there is one -- from your experience at Mitsubishi and Areva, where as a result of regulatory process you feel like you have sub-optimized a specific safety feature that was part of your I&C design?

MR. PAULSON: I mentioned the engineering tool. The evaluation of the engineering tool is something that I think is worth doing, especially having continuous evaluation of the availability of systems because of its continuous attachment. We have detached that specific system as part of the acceptance and simplification process. As I've said, I don't think anyone on the staff has said that's either bad or good. It's just when it was attached it became a more difficult process to review. So, I would say yes I think that there is the potential for continuous evaluation of the performance of systems with the engineering tool attached as something that may be worth looking at in the future.

COMMISSIONER OSTENDORFF: Without that engineering tool, is the function now performed through some other mechanism?

MR. PAULSON: It's not performed continuously. It is still there, and we will -- part of the discussion with the staff is how often that we can go back in and recalibrate or reevaluate the systems.

COMMISSIONER OSTENDORFF: Thank you. Mr. Sliva?

MR. SLIVA: I don't think we would say that we've sub-optimized safety. Taking advantage of digital technology, we had technology that I think proposed a quantum leap from the systems that people are familiar with in even the most advanced Gen-2 plants. In that huge leap that we proposed in our design, we perhaps as designers just assumed -- just as the Jet Propulsion Lab does -- that people would enjoy reading code. Well, maybe everybody doesn't like the concepts of advanced digital I&C technology. It takes a little bit of time to understand how that could be proven to be both reliable and effective, because -- you know, "Gee, this analog phone worked just fine. I could talk to my mother every Sunday, just like I could on my digital phone today. I may not maybe know where she is on my analog phone, but I could still speak with her." So, we think that it's incumbent upon us to demonstrate functionality of digital technology and how that it could enhance the overall reliability and safety of the plant. I would not say that the simplifications that we've made have compromised the safety of the plant in any way, shape, or form. Certainly the staff has not pushed us in that direction. In similar experience to MHI, Areva has now modified its approach where we accomplish the same functions perhaps not on a continuous basis, perhaps not the way an I&C engineer would love to see it performed, but certainly we perform the same functions in other fashions. So I certainly don't

think in any way the safety of the plant was degraded or anything. We just need to demonstrate, I think, that the technology could enhance the portfolio of reliability of the plant. And we're working on those proofs.

COMMISSIONER OSTENDORFF: Thank you. Mr. Patterson, in your slides you talk about ISG-6 and concern about the level of detail required. Are there other specific improvements or enhancements to the ISGs -- recognizing that they have been an evolutionary set of documents -- any other ISG improvements that you think ought to be made by the staff?

MR. PATTERSON: Well one area that we're looking at is the sequencing of documents that's required. Right now ISG-6 specifies a Phase 1 set of documents, a Phase 2, and then some Phase 3 for audit at the end. So hopefully in the process of going through this we can look at the high-level documents that you develop first and get a sequence of those. The NRC can't review all of them at once, so what sequence of those documents is the best way to do that? And then that would actually streamline the process for the project and maybe shorten the project.

COMMISSIONER OSTENDORFF: Okay. Mr. Ray, do you have anything to add from your experience at Oconee?

MR. RAY: No I don't have anything specific to add to that.

COMMISSIONER OSTENDORFF: Mr. Chairman, I have got one more question. Dr. Holzmann, I wanted to ask you a question here. From what you understand -- and I realize you're in the space community and so forth, not necessarily following the nuclear community -- but from what you've heard today and from what other experience you may have had prior to coming here today, do you have any suggestions to the NRC staff on how to look at the software

code issues that you have been working on with JPL?

CHAIRMAN JACZKO: Yes, well, I think I'm here mostly to articulate caution, against underestimating the implications of using complex hardware for critical applications, but there are techniques that can be followed, so the emphasis in my presentation was on evidence based safety cases. So I would emphasize not to underestimate the importance of that.

COMMISSIONER OSTENDORFF: Thank you, Mr. Chairman.

CHAIRMAN JACZKO: Commissioner Svinicki?

COMMISSIONER SVINICKI: I want to thank all of you for your presentations as well, and I think I'll follow on a little bit on some of the questions that were asked. We did hear the term -- I think at least one of you mentioned the term "obsolescence." And as I think about the Commission meetings in my time here that I've attended on Digital I&C, my sense was some of the Commission's early urgency on the issue going back to 2006, and I think this is especially for the operating fleet, was this issue of obsolescence of analog systems and supply chain issues. And so if I go back to the SRM that the Commission issued in 2006, you know, it talks about developing the project plan and establishing a regulatory framework that, you know, would allow licensees and applicants to forward fit these digital enhancements. And I think there was some urgency about that.

I also see that somewhat enshrined when I look at ISG-6 on the licensing process where it says that we're trying to develop a system here where we will review compliance with the regulations and that public health and safety will be protected. Then it goes on to say it's not intended that the review or audit activities by the reviewer, include an evaluation of all aspects of the design and

implementation of the I&C systems, so as I think about the comments about level of detail that I'm trying to think from previous Commissions, I think it was along the flavor of, "Are we getting to a framework where if you're submitting a design to the NRC for a digital watch, are we looking at whether or not that watch provides accurate time and is reliable as opposed to critiquing your design of the watch that you sent us."

So I think, Mr. Ray and Mr. Patterson, I might ask you what your sense is in terms of the kind of level of review that we're doing. And the other comment I'd make is that NRC has a really good practice of doing pilots, and I think the real challenge often, even after successful pilots, of the review of something, is taking the lessons learned from that because the level of review that we do in a pilot kind of review is, you know, the deep dives where we look at the areas that are most relevant to our regulatory review, but we've got to synthesize that learning. You do a different review in two pilots than you might do in 30 license amendment requests, or I could see a future again with this obsolescence issue where NRC might have a fleet operator come in with a fleet-wide amendment to make digital upgrades. And so I would ask you of your sense of our review, of level of detail, of our readiness, given the obsolescence urgency of where we need to be as an industry and a regulator, and just throw that open for some general commentary in my remaining time.

MR. RAY: I can go first on that. From Oconee's perspective there was a great level of detail in the review. We submitted 36,000 documents -- pages of documentation to be reviewed. Even though the number of official questions, about 111 official questions, a lot of back and forth between the staff -- the two staffs, I think they had a very good working relationship. We actually set

up a file server so we could pass documents back and forth, keep the reviewers in the loop of everything that was going on. There was some, you know, evolving guidance at the time, so we had to stay on top of that. But being a first plant, we understood the amount of review that needed to be done, but it was significant. The SER came out later than we wanted it to in order to meet our first schedule, we ended up delaying the project one refueling cycle about 18 months, one unit, the last unit, I think it ended being delayed two years, and the cost ended up being almost twice as much as we originally expected it to be. But looking back on it, I would say the relationship between the two staffs was very good. They worked through those issues of being a first time plant. And it's understandable, and I would hope that before we have set up processes that are more efficient to allow the two staffs work through those quicker.

COMMISSIONER SVINICKI: Mr. Patterson, did you draw anything from the pilots in terms of preparing for your activities?

MR. PATTERSON: Well, we're still in the process of developing the documentation and the level of detail necessary for that. But based on the conversations during some of the task working group meetings and understanding the regulatory side, the viewpoint from them, and having them having to make a reasonable assurance claim on the result, I can understand because of the complexity of digital they want to know more and more about the digital platforms and software to be able to be comfortable with that. And I think once we get through a few of these vendor topical report approval, and they become more familiar with that, they can back off and be more comfortable with that assurance. The first few that go through, obviously they're going to take more time to do a more thorough investigation of what's going on. There's

always a question of are they looking at more of the design or more of the regulatory effect of you know, of the design. So it's an equilibrium. I think once the knowledge level comes up, and obviously if the complexity level comes down, it will be a much easier determination, and less level of detail will be required.

COMMISSIONER SVINICKI: And from the new reactor perspective would either of you like to comment?

MR. PAULSON: I must preface this by saying it is from maybe a little more commercial approach to this, but let me put that aside because I do think there is a comment that is relevant here because we have done some studies as to what is slowing the process of upgrades. As you know, we have the capability. We've done a lot of digital upgrades already in Japan, and they've gone very well. We think that there are possibly two basic issues, and I think I've picked up on this with Mr. Ray's comments also in his process. One was that they focused on the risk, and the other was cost, and you can't separate the two, actually. They have a tendency of running together. My understanding of the process, and I'd be glad to give the floor to someone that understands this better than I do, but my understanding of the process is that there was much more detail required in terms of final design information for some of the previous -- specifically the Oconee upgrade. And then there is -- as part of the 52 process. Not that we don't require a lot of detail there, too, but detail of final design information is not required. And I understand that some of that was required for the Oconee process. And then, too, that there was no final approval until the factory acceptance test, which is much later in the process and also adds that element of risk late as opposed to early for a utility. You know, we've looked at

cost on that, and just a rough cut says it's probably 33 to 50 percent increase in cost based on the additional time associated with the additional work that has to go on upfront, the risk associated, and the probable delay that that will cause, maybe as much as a year. And I think you said 18 months, so that's probably wasn't a -- maybe even an under estimate looking at 12 months. I would say Mitsubishi would say two issues that we can improve upon, based on the 52 process, would be risk and then ultimately final cost.

MR. SLIVA: And I really don't have much to add because our experience has been the same. We had the privilege of supporting Duke in their application and I think that Tom Ray framed our experience correcting in his presentation. We learned a lot from that first effort.

COMMISSIONER SVINICKI: Thank you. Mr. Chairman?

CHAIRMAN JACZKO: Well thank you and I think it's been a very interesting session. I remember going back to the year 2006 is a very different picture than we have now but it's funny because a lot of the discussion seems the same as we were having in 2006. I'm not sure why that is, but, of course, in 2006 we had an Oconee application that had originally come in, been withdrawn because it just wasn't possible to get through the review process. We were relying on branch technical position, whenever it is 19-7, whatever it was, which was -- again I think presented an ability to do a review, and I think again, but didn't necessarily provide an optimal review so the staff had a lot of work I think to address a lot of issues, has documented all the interim staff guidance that have been developed and preceded. So I look at the situation and I imagine we had a meeting with the different set of vendors here we might have a very different meeting. In the course of the last five years the staff has reviewed

applications for several digital systems, so we've obviously approved Oconee, we have approved Wolf Creel, the field programmable gate array which I can say, but can't understand, and we, of course, approved the ESPWR or at least at staff level and Westinghouse digital system so I am always wondering, and I don't want my colleague, Commissioner Ostendorff is a lawyer by training, so this is something I learned from lawyers. Sometimes, I'm not sure, you have to be careful with difficult situations, and difficult situations, and I think the term is something like difficult situations make for bad law or something like that. I'm not sure if the situation we have now and perhaps MHI and Areva are difficult reviews or if it's a problem with the review process itself and I'm not sure how we distinguish that. And obviously Oconee we did complete the review and work through that. It really was the first time for a new digital protection system. I'm wondering if you can comment on that. What do you think was different about, perhaps I don't know if you're familiar with Westinghouse and GE Systems, or what you could say was different about those that the staff was able to work through those reviews in a way perhaps that one would get the impression from this meeting staff isn't able do what the others. I don't know if you want to comment on that?

MR. PAULSON: Once again I don't want to overstate my understanding of what went on with the Westinghouse review, but what I do understand, maybe in a very cursory fashion, is that there was a lot of commitment in that document to future DAC approaches. The design that we're putting forward basically is up and running, and so the design is much more detailed so you can't rely on a future promise. And that to a certain extent extends the upfront review process which we've taken into account and accepted

that because we think it will improve the review process once our customers get their point of trying to finalize their plant design and how much we'll ultimately end up with addition ITAAC or whatever. Or a later process where Westinghouse will have to address those DACs somewhere later on and could cause problem, so we've taken that risk up front which is where we think to do, so I think that's one of the issues.

CHAIRMAN JACZKO: Mr. Sliva do you have any thoughts?

MR. SLIVA: That's a difficult question to address I think because of the timing of the different submittals and obviously not having detailed knowledge of the competitor's submittal, I will say, from Areva's standpoint we submitted what we thought was a state of the art design. It was projected forward from the technology that was licensed at the operating plants at Oconee, this is the next generation because we are looking at the next generation of reactor. And I think, probably as a total industry, we weren't adequately prepared for the challenges of taking into account the complexity of that technology and then being able to work backwards from it to arrive at, in some cases, what now appear to be a very simple analog system that we were comfortable with. And provide safety and liability for, you know, decades. We've learned a lot through the review, I think we've learned a lot from the staff. I think the staff has learned a lot from us. Certainly has developed into a very interactive process and while taking longer than anticipated probably on that watershed 2006 meeting, I think, going forward I do see us completing the process. And I think when we come to the next round of licensing of I&C applications the entire industry will benefit from what we are learning now. I can't really put it into context to the other two designs, but from Areva's standpoint, I think we underestimated the challenges on industry in

presenting digital technology into the environment we have.

CHAIRMAN JACZKO: Well thanks a lot, I appreciate that. I know this certainly has been an area of challenge and newness and with that there is always difficulty, but as I said I think we've come a long way. Mr. Paulson one thing I did just want to ask you about; I know in your original presentation you talked about 2006, 2007 earlier submittals. But just, I think that there is something I just want to make clear for the record. We didn't actually docket and accept for review the MHI application until sometime I think in early 2008 because at the time there was no budget to review the application. So, you know in fact, and I think Commission Magwood you may have made the comment, the clock doesn't really go back to 2006 for MHI I think it really starts sometime I think when the final schedule the staff provided was sometime in June or so, or May/June of 2008 and that's really when the review actually began in earnest for the MHI application. So, it's not been a five year process necessarily there, but more of a concerted effort in three years.

One of the questions, and I thought I would ask this generally. There has been some discussion about level of detail in design reviews. I know, I think in their October letter of 2010 ACRS made a point of commenting on the detailed review. One of their recommendations was that parts of, in particular this reference the ISG-6, the licensing process, and one of the comments they made was that in section B of that document that it should be revised to include a discussion that while process is important it is not a substitute for a detailed review of the hardware and software architectures to ensure that they meet the fundamental principles identified in this section.

I'm wondering if you're familiar with that particular aspect of the

interim staff guidance on the licensing process and if you have comments on ACRS's position. Do you think ACRS is in the right place, or not, on their idea about detailed review and if that's consistent or inconsistent with what you're talking about for detailed reviews. I was wondering if you have any comment on that.

MR. PAULSON: I don't think their fastidiousness is misplaced by any means. I think that as Tom said, that there is an issue here of us understanding the complexity as we go through the process and it's a learning process on our part for sure. And the fact that ACRS has asked for a level of detail to satisfy themselves is not surprising to me at all based on their attitude toward this new technology and the fact that that's their job is looking at that independently, so I'm not surprised although it's still a struggle.

MR. SLIVA: I agree with Keith's assessment. It's not a surprise and it is a struggle.

CHAIRMAN JACZKO: Any others want to comment? Dr. Holzmann, I don't know if you have familiarity with some of the positions that our advisory committee has taken or if that statement I read rings true to you or you see that as an appropriate approach to dealing with some of these issues.

MR. HOLZMANN: No, I'm not familiar with the details of the process or what is required right now. I'd be surprised if the elements that I emphasized were part of that process. Probably a review of that process would not be misplaced in my view.

CHAIRMAN JACZKO: Well, again, I want to thank everyone for being here and providing your thoughts and your insights and we will now turn to the staff. Thank you very much.

[break]

CHAIRMAN JACZKO: Bill, we'll start with you.

MR. BORCHARDT: Thank you. I'd just like to acknowledge the activities and the efforts of the Steering Committee, as they help to coordinate the NRC staff's activities across the various program offices. I think they were instrumental in making sure we had a consistent approach between new reactors and the operating reactors. Had the very important support from the Offices of Research and NSIR -- NSIR is related to cyber security. So, I think what they've done is made sure that we've come out with a very technically correct position. They've helped us to move forward, make good progress, and we're looking forward to transitioning to make this more of a routine mainline activity. Jack will begin the staff briefing.

MR. GROBE: Thank you Bill. Good morning, Mr. Chairman, Commissioners. This morning we will update you on the progress that we've made in stabilizing the digital instrumentation and control regulatory infrastructure. I'll talk briefly about the activities of the Steering Committee and the task working groups. Pat Hiland is the director of the Division of Engineering in NRR. Pat will talk about successes and challenges in the operating reactors arena. Tom Bergman is the director of the Division of Engineering in new reactors and he'll do the same: successes and challenges in the new reactor arena. Stu Richards is the deputy director of the Division of Engineering in our Office of Research. And Stu is going to present an overview of the progress that we've made in implementation of our five-year research plan. That research plan was developed in collaboration with the project offices and the Office of Research, and he will particularly highlight the issues that the Commission has

expressed its specific interest in. And then finally, Dr. Steven Arndt is one of our senior level advisers in the digital instrumentation and control, and he will talk about the international activities that we have undertaken and the advantages that we've gained from those activities. Slide three, please.

Four years ago -- it's surprising that it was four years ago -- the Commission directed the staff to establish a project plan to facilitate the deployment of digital technology at operating reactors and in new reactors. And the project plan was to include short range and long range objectives and goals, and we should seek industry input on that project plan. The executive director established the Steering Committee comprised of executives from NRR, New Reactors, Research, Nuclear Security and Incident Response, as well as the Office of Nuclear Material Safety and Safeguards for fuel cycle facilities.

The goals of the Steering Committee were to interface with the industry, to oversee and facilitate resolution of technical and regulatory issues, and to ensure effective interoffice coordination within the agency. Under the guidance of the Steering Committee, a project plan was developed to establish regulatory stability for new and operating reactors as well as fuel cycle facilities. The development of that project plan included extensive engagement with the industry -- all aspects of the industry -- and other public stakeholders. It actually took quite some time to finalize the project plan. The outcome of that was very positive. We had very clearly defined problem statements that everybody agreed to and understood and that facilitated effective progress in developing specific milestones, deliverables, and accountabilities to address those problem statements.

The Steering Committee established seven task working groups.

And those were comprised of staff from across the agency. The industry developed an executive oversight committee, as well as working groups to interface in parallel with the various infrastructure that we established. During these past four years, the NRC has augmented its staff with over two dozen digital experts and those experts came from digital vendors, operating organizations, nuclear operators, other industries including automotive, aerospace, and military, as well as entry level staff coming out of the universities. We have a highly qualified, robust, and capable staff that is addressing the digital challenges we see today.

The task working groups conducted over 100 public meetings with our external stakeholders and directed nearly 30 FTE of direct effort from the staff in developing the short term deliverables, completing those, as well as many of the long term deliverables. Interim Guidance has been developed in all seven areas. Slide four, please.

That Interim Guidance, as you'll hear shortly, has been used effectively in both operating and new reactors. Pat will talk about successes at Oconee and Wolf Creek, as well as the ongoing work, and Tom will highlight successes with the Westinghouse AP1000 and the General Electric ESBWR, as well as ongoing work.

This past January, we had a meeting with the industry executive group and the staff in the industry agrees that the Interim Guidance has improved the predictability, stability, and effectiveness of our reviews. The Interim Guidance is, of course, one approach to resolving the key technological issues associated with the use of digital technology. It's commonly referred to as the fast lane, but it also clarifies those critical attributes of the technology that need

focus for industries -- or for applicants that choose a different approach to solve those problems.

The licensees are satisfied with the Interim Guidance and also look forward to additional opportunities to refine that Interim Guidance through the public comment process as we translate the Interim Guidance into durable regulatory infrastructure documents. The Steering Committee and the industry executives have agreed that it's time to sunset the expanded or enhanced oversight that we've been providing. The staff continues internally with active interaction between the various offices. Pat and Tom and Stu meet biweekly on issues of interest to the Divisions of Engineering in the various offices and frequently, if not always, those biweekly meeting agendas include digital issues.

Pat and Tom will initiate executive level meetings with the industry. The industry has agreed to begin with quarterly meetings and this will be the continued interface and structure that we'll have in place to replace the Steering Committee activities. In addition, we're establishing a technical advisory group, and this is not a unique aspect of the way we do business in the NRC. We have many technical advisory groups. Typically they're led by our senior level advisors and this one will be led by Dr. Arndt and Mr. Santos, and Sushil in NRR, New Reactors and Research. The focus of that technical advisory group will be to facilitate continuing consistency across the offices, support resolution of emerging issues, and coordinate staff level initiatives. At this time, I'd like to turn it over to Pat to talk about operating reactors.

MR. HILAND: Thank you. Slide five. As we mentioned, you know, the infrastructure, we believe, has been improved through the Digital I&C Steering Committee. We just issued, as noted before, Interim Staff Guidance

number six. We call it revision one, but our draft revision was 55, just before we issued it. And so, it was quite an accomplishment over the two or three years that we worked on it to reach a consensus that made it a final document. But, of course, involved in our process are topical reports. The topical reports as you're aware are there to streamline both the staff as well as industry's review time. And I'm going to talk about a few that we currently have under review.

New technology, you've heard, Wolf Creek, which is the field programmable gate array design. That was approved about 18 months ago for installation for the main steam and feedwater isolation system at the Wolf Creek plant. Oconee is an analog to digital system that we approved -- and I believe we're one year and one day from that approval. I think it was January 31 of last year that that system -- or that amendment request was approved. That uses a Teleperm process. That had a topical report submitted and I'll just mention the reviews that we did on the update of that process. Slide six.

We currently have some ongoing reviews in process. Grand Gulf has elected to use a General Electric nuclear measurement analysis and control device, commonly referred to as a NUMAC. That NUMAC is going to be the first time use in a boiling water reactor 6 -- BWR-6 system is going to be used in its oscillating power-range monitoring system.

Crystal River. Crystal River plans to come in with an extended power upright in the future, and along with that, they're contemplating the use of digital systems and a fast cool down function that will be needed to support the extended power uprate. They've come in and talked, and you'll hear me talk about a Phase 0 meetings -- in a Phase 0 meeting to discuss that concept.

At Columbia. Columbia also has elected to upgrade their nuclear

instrumentation system with the General Electric NUMAC. And we held a Phase 0 meeting with that licensee last month.

Watt's Bar, the Nuclear Unit 2. That review has included three safety-related digital systems. It's ongoing, but those three systems -- the Westinghouse Eagle 21 for the reactor protective system, an engineered safety feature system. The Westinghouse Common Q for the post accident monitoring system, as well as the Sorrento digital high-range monitor. But in addition to the, safety-related systems, our Standard Review Plan suggests that we look at those systems that are also important.

I've termed it balance of plant, but the three systems that we're looking at are a loose parts monitoring system. The rod-position indication system, as well as a Foxboro control system. All three are certainly important. Slide seven.

Some new platforms that we are reviewing. The first one is HF controls. They're HFC-6000. Our technical review is complete. It's currently scheduled to be out through the licensing phase in the spring of this year.

The advanced logic system from Westinghouse does use a field programmable gate array technology. That is scheduled to be issued by us in the fall of 2011. And this is one of those systems that will support Diablo Canyon.

And then lastly, the Spinline-3, it's another platform that uses a field programmable gate array technology. We're just in the start of our review of that and we've completed our acceptance review of the Spinline system. Slide 8.

Update the topical reports -- one of the lessons learned at Oconee was the topical reports that had been referenced on that submittal were about 10

years old. And some of the components in their microprocessor had changed. They'd gone up to a different level of revision. And when we started to look at them, we identified that these were manufactured under a different engineering processes and verification processes. So it did cause some additional review of a topical report that had been reviewed and approved 10 years ago. But right now we have two topical reports that previously had been approved but they're going through a review -- the Westinghouse Common Q is going to be used on Watts Barr Unit 2, that's under review. As well as the Invensys, it's the Tricon topical report. And we've targeted the spring of this year. And again, this is the second digital system that Diablo Canyon is choosing to employ.

The software validation tool, SIVAT: SIVAT verification and validation tool, we first were introduced to that tool when Oconee first came in with Areva for their submittal. SIVAT was a new tool, one that we've never approved before. While we've not -- we weren't able to approve it in the original Oconee submittal we have received the topical and our technical review is complete. And I expect that acceptance and safety evaluation report to be issued shortly. This is the first time that we've approved a code verification tool. Slide nine.

As we've mentioned, Diablo Canyon will be a pilot. As you heard, our third Phase 0 meeting is this Thursday and we're all set to look at the Oconee -- Oconee lessons learned have been incorporated into the Interim Staff Guidance No. 6. We actually had a workshop in May of 2009, with industry, to go over some of the lessons that we had learned through Oconee and hopefully we'll learn more in the pilot program to even further streamline our processes.

As I mentioned earlier, this is -- I hadn't mentioned, but the Diablo

Canyon is a digital-to-digital replacement. They currently have the Eagle-21, and as you heard earlier, they're going to the ALS and Tricon systems. We expect their amendment request, as we heard, this spring, to be issued. And we're going to use the pilot to further enhance our review processes. Slide 10.

Challenges. I call them areas of focus. Moving forward, what are the operational issues. Mr. Grobe continuously challenges me: "What am I going to do next? What are you going to do when these are out in the field and up and operating?" Well, we've looked at that a little bit: 50.59 that allow licensees to change out systems without our approval, if it meets certain criteria. We had approved an industry standard NEI-0101 and the numbers alone tell you it was developed 10 years ago. We've worked with NEI and have suggested that we go back and revisit that standard, and make sure that it is up to date with the current requirements that we expect.

Also in the maintenance rule -- the maintenance rule and its application to risk inform maintenance activities in the plant. As you know, we have no real risk guidelines in the digital world. And so, that might be an area that we'll need to look at with how that process is used in operating plants.

As well as the inspection and start up testing of the revised facilities. Region II -- and we have supported our regional inspectors with our design engineers; have developed an inspection plan that they will implement on Oconee. And we hope to take -- well we will take lessons learned from that on Diablo Canyon.

And then, technical specifications are another area that could be a challenge in the future, particularly in the determination of operability when a system or component is degraded. With that, I'll turn it over to Mr. Bergman.

MR. BERGMAN: Good morning. Slide 11 please. As you know, the staff has completed its safety review of the AP1000 and ESBWR designs and we're awaiting approval, so we can issue those proposed rules. Both those designs are modern, fully integrated digital I&C systems, and both those reviews were conducted without controlling the overall schedule for the designs. Next slide please.

With respect to ongoing reviews, we have two design certifications still under review with the EPR and APWR. In general, there isn't a digital I&C review as part of a combined license review, they incorporate the certified design by reference. South Texas is the exception to that generalization, they dictate departures from the certified design. We have essentially completed the staff's review. We will be briefing the ACRS next week, we will be explaining our acceptance of that design as well.

We've continued to -- all these applications did use, and the staff used the ISGs as appropriate for the individual application. We've continued our dialogue on DAC for I&C systems which we briefed you, and the ACRS briefed you in November. Subsequent to that, we've continued those discussions. They did issue a letter in November that would indicate is a licensing construct. We've achieved a common understanding as to what it takes to use DAC and make the safety finding during licensing proceedings. There still remains the open issue as to their precise role post COL. Next slide please.

As we discussed in that meeting, we have submitted the complete DAC I&C inspection procedure, draft inspection procedure, to the ACRS for their review. We are continuing to test that inspection procedure with the South Texas applicant, with the next inspection, which is on the planning phase to be

completed in early March. And as we committed at that meeting we do have a I&C staff from my division, as well as a participant from the I&C staff in the Office of Nuclear Reactor Regulation, participate on those inspection activities. Next slide please.

The challenges and I am not trying to trivialize the issue, because the story might be a little silly, but as we've been through these challenges on some of these reviews, it actually takes me back to when I coached little league. And we would have practices and let's say all the players weren't necessarily fully engaged in the game. But come game time, you know, they'd say, "Hey I want to play shortstop." Now, my answer was just, "No," because it was a safety issue. But the guy I --

CHAIRMAN JACZKO: That's a regulator in the making, right…

[laughter]

MR. BERGMAN: -- wasn't very satisfying to the child. But the friend I coached with, he had a much better answer, which is, "Don't tell me, show me." Show me in practice you know how to do it, and then we'll talk about doing it in the game. So we understand that the applicants have tremendous capabilities and their staff are highly qualified and have great confidence in the designs and that designs very similar to these have been approved for use in various places in the world, including the United States. But that isn't a basis upon which we can certify a design.

We need the application that we're reviewing to provide the safety basis that shows it meets the NRC's safety requirements. And that -- the principal document in that is the design control document. It's important because -- right now we have a lot of dialogue with the applicants. Even if we use that

dialogue to fill in the gaps, the design control document provides the basis for safety, not just today, and it provides the regulatory control mechanisms over that design, for the life of the facility. And when we're talking Part 52, you know the time between certification and termination of operations could easily be 80 years. So, things are going to change, the designs are going to change, the vendor is going to turn this design over to the COL holder. We're going to have staff changes, they're going to have staff changes. The public needs to understand what was our basis upon which we determined this design was safe. And that is included in the licensing basis that we certify today. So we do focus on the safety, making sure that the documentation provided to us demonstrates the safety of the design. And the principle impediment to making that safety finding has been, in our view, the clarity and completeness, or what you'd sort of call quality issues in the application itself. When we've identified errors or omissions in those applications, we generate requests for additional information. We issue a lot of what we call RAIs, we issue a lot of RAIs. They can be very complex, depending on the gaps in the application. Frequently that results in an incomplete answer, which is the second round of RAIs, this also represents rework, not just for us, but for the applicants themselves, and rework is inherently inefficient. But in order for us to make the safety finding, we do need a clear and complete licensing basis.

On complexity, again, we understand how some additional complexity enhances operations. I mean, that's a good thing. And the design still needs to meet the safety requirements and when we talk safety requirements, we really are talking fundamental safety principals and again you heard these in November from the ACRS; independence, redundancy, defense-

in-depth and diversity, determinism, and those are embodied in our regulations and guidance and those safety principles are really consistent around -- with all regulators, it's not unique to us and they're certainly consistent with ACRS positions.

Now, simplicity is not a requirement. It is a design principal, and Steve will get into international activities in more detail, but the multi-national design evaluation program is about to publicly issue a common position on simplicity in I&C design, where all the participants in that program have endorsed this common position, including the staff from the United States, France, and the Japanese regulators. So it is moving there, and, in fact, if there's a trend in safety system I&C design, it is towards simplicity, with complexity there where necessary for the safety functions. And that's basically the path we've been driving. And, to their credit, both Areva and MHI, as they acknowledged this morning, are changing the designs, so that they can demonstrate they meet our safety requirements.

On the last point on schedule, sometimes I fell like inserting "or" there, you can get an efficient schedule or a thorough review and to me it really is an "and," it can be safety "and" timely. Obvious, or in general, simple systems are going to get quicker review, because it's easier for the applicant to demonstrate the safety of the design and it's easier for us to reach the same conclusion. But we can license complex designs. They are, in general, going to take more time, simply because it requires more information to make the safety case. Complex designs that fully follow our guidance, without exception, get a shorter review than designs that depart from that guidance. And that isn't unique to I&C, anywhere in the plant, where you depart from established methods,

you're getting basically custom work, and that takes longer. I mean the poster child for that would be the AP1000 shield building A truly custom feature outside of the I&C system.

But I don't want to focus too much on safety and complexity, because, again, I think the real driver on the schedule, from the staff's perspective, is the quality, the completeness, the clarity of the licensing basis that they presented to us. Thank you very much. Dr. Arndt? I'm sorry, Stu.

MR. RICHARDS: Good Morning I'm Stu Richards with the Office of Research and thank you for inviting us to be at the table today. It's a great topic to talk about. The Office of Research, you know, we do research for the program offices our customers on digital I&C issues and we also aid in the development of new and revised regulatory guidance.

We should be on slide 15. Our research is guided by our digital research plan. It's a five year plan covering the period from 2010-2014 and as Jack already mentioned, we reviewed this with the program offices and they agreed and concurred in it, we presented it to the ACRS and through that presentation to the ACRS we also provided it to the public and we did get some public comments.

The research plan is broken down into four areas. The first safety aspects, as the title implies, looks at how digital systems can impact the safe operation of our facilities. That includes failure modes, we look for new analytical techniques that may aid NRC reviews. And we look at digital system modeling and PRA research. Security aspects look at the unique security issues that result from the use of digital systems and the impact that external threats might have on the digital systems that are put into our nuclear power plants.

Advanced nuclear power plant concepts, that has to do with the Next Generation Nuclear Power Plant, NGNP, and we're looking at advanced instrumentation and advanced controls. And finally, knowledge, management, research, collaboration, captures things such as capturing digital I&C knowledge, supporting collaboration, both domestically and internationally, and operating experience.

Next slide please. We work closely with the national labs on digital I&C research. The labs bring both the combination of knowledge of nuclear power plant operations and digital systems. So they're well-prepared to work with us in this. As you can see, there is a list of a number of labs that we work with and just briefly -- Oak Ridge has been involved with us with digital diversity and defense-in-depth, highly integrated control room work, communications within digital systems, FPGA, failure modes and updating Reg Guides, which includes research and test reactors. Sandia has brought to the table a unique capability on cyber-security, so they've done some cyber-security testing for us. They've also looked at the impacts of electromagnetic pulses on digital systems. PNNL has also been involved in the cyber-security, and they helped us to conduct an expert elicitation on digital system failure modes that we'll talk about a little bit more in a minute. Both Brookhaven and Idaho have been involved in PRA work and INNL has also been involved in advanced reactor work.

Our work with the labs is also complimented by work with the universities and interactions with our international partners. For example, we have worked with the University of Virginia, the Ohio State University. We have collaborated with the IRSN in France, in the Korean Atomic Energy Research Institute and the Halden Project in Norway.

Slide 17 please. The next two slides list four of our products that we've provided, to provide a sampling. We have a much longer list of products we could provide if asked. But the first one is -- you know, I got to tell you it's one of my favorite NUREGs. So, recommend it to you for your reading, if you like. It was produced by Mike Waterman, who's here with us today, but it has to do with diversity in digital systems and what this did is it went on and looked at what was done in international nuclear power plants, but also looked at what was done in other industries within the United States, including aerospace, aviation, the chemical industry and the rail industry and then it developed an evaluation technique, in effect scoring the different diversity measures that you use, and you know, for better or for worse coming up with a number. We can argue about how you weigh things, but it is a way of taking in all of those diversity measures and trying to come up with an indication of where you stand relative to other industries. So it is interesting reading to see how other countries have done it with nuclear power plants and how the other industries have incorporated defense-in-depth and diversity and this information was also used in development of ISG-2. so it helped us that way.

The next NUREG-7006 has to do with the field programmable gate arrays, it looks like design practice is for FPGAs and based on the program office request, we're presently working on turning some of that information into a Regulatory Guide, and we're also using that to work with a consensus standards development that's going on in this area also.

Next slide please. NUREG-6991 design practices for communications and highly integrated control rooms. When we're talking about communications here, that's communications between digital systems, between

channels, between safety and non-safety so it's the idea of sharing digital data within. This NUREG looked at how on the digital systems, the communications aspect of digital systems was addressed in international plants. It also reviewed consensus standards on this topic area and it was used as part of the development for ISG-4. And the last bullet on slide 18 mentioned before that we've done some cyber security at SNL. They did assessments on the Tricon, the Teleperm, the Common Q systems, assessing you know, their vulnerability to hacking, if you will. And this is supporting some of our licensing reviews and some of the development of guidance. Additionally, research led the development efforts for Reg Guide 5.71 on the cyber security programs, that was quite an extensive effort. Slide 19 please.

The next three topics are to address issues that the Commission specifically asked us to bring to the table today. The first one has to do with software failure. Just -- for me this was an eye opener, when it was explained to me that software in itself, basically does not fail, so when we're talking about software failure we're not talking about the software suddenly not cycling like a valve, not turning on like a pump, not changing state like a relay, what we're talking about is that the software -- either the requirements to develop the software are incorrect or the requirements if correct were inappropriately programmed into the software or, as a system that's updated or modified over time, that you introduce reduce those flaws. So software failure -- the software's going to do what the people tell it to do. The question here is, what degree of assurance do we have that that software has been properly defined and implemented, and maintained through its lifecycle.

One of the techniques that we went to look at is the failure modes,

effects and analysis technique, to see if that would provide some insights on software. We found that FMEA is useful for hazard review, which is more of a high level review that's done early in the development process. We did conduct that expert elicitation clinic that I talked about in 2010 where we brought in experts from different industries and from around the, you know, well we had some international participation, I believe it also included Dr. Holzmann, who talked to you this morning.

We have worked with IRSN and France on this issue, and specifically for FMEA, we found that it's useful as far as hardware goes within digital systems and it may be helpful for hazards analysis, but it isn't particularly useful for software. There is one example in Korea where they did use FMEA on a very small portion of a critical part of the software, but again, this was a very limited application.

Slide 20 please. So, FMEA is not particularly useful in applying it toward software. The reason for this is that there's simply too many combinations of inputs, and the order in which those inputs could occur in a software system, the number is just huge. Additionally, as I mentioned before, software faults seem to driven by the system requirements, implementing those requirements into the software and then maintaining it. We have two products in this area, one is a NUREG with the French that is in review, has not been issued yet. And the other is a series of three research information letters, that's coming out of the expert elicitation that we did. The first of those was issued in January, and we're working on the other two. Next slide please.

Just as with our traditional operational experience that we apply to operating plants now, we recognize the value of OpE for digital systems. The

challenges are several in this way. There have been some digital systems in U.S. nuclear power plants, but those are not what you would call the current generation of modern plants. Some people mentioned today the combustion engineering core protection calculator, which is in CE plants. The General Electric 21. But they have limited applicability to what we're looking at putting into plants today.

Because of the limited data and the current state-of-the-art regarding software failure modes, it makes the use of quantifying OpE to be somewhat challenging and not particularly meaningful at this point. Nonetheless, operational experience is important. We have been able to look at individual events, understand what happened, and bring that information into our regulatory guidance and the work that we're doing. We do have a memorandum of understanding with the Electric Power Research Institute, and with that memorandum of understanding we have been able to have access to events and lessons learned details from industry, which has helped us in our regulatory role and we hope that will continue.

Next slide. We're also reaching out beyond the domestic industry; the first thing listed here is COMPSIS, that's computer safety -- computer system's important to safety, which is an NEA sharing of information, we're working with them. I mentioned already that were working through EPRI with the Koreans and we hope to also have dialogue with the French. Non-nuclear digital operating system experience is also very important. We do have a working relationship with NASA and through that we've been able to gather a lot of information that we haven't analyzed yet, but it holds some promise for the future, to learn some things from that. The last bullet on Slide 22, we are

gathering an inventory of the kind of equipment that's being used out in the nuclear industry, so we can better apply OpE, when we do have it available to us.

Nest slide please. The last two slides I have address the use of PRA in digital systems. As it's been mentioned already we currently have a deterministic process but in 1995 the Commission PRA policy statement said we should use PRA, to the degree that the state of the art allows it. So we are working on seeing if we can develop that and to use that as part of our, you know our risk tools. We have completed -- as the second bullet notes, five NUREGS on various aspects of trying to look into using PRA. Both dynamic modeling and static modeling. This work did identify a set of desirable characteristics, but it wasn't able to basically deal with software, so that is still a challenge. Hardware, I think we're having more luck with, not so much with software, and Slide 24 please.

The research that we have done so far, has identified some additional things that we're working on, specifically defining or better defining the failure modes. We need to work on the methods and data needed to address software reliability. We need to have better data on hardware failures, and in moving this ball forward, Brookhaven working with our staff, has reviewed existing quantitative software reliability methods, and we're in the process of approaching a proof of concept study to see if some of those methods can be applied. But nonetheless there's a lot of work that remains before this can be applied to any of our nuclear plant PRAs. And with that I will turn it over to Steve.

DR. ARNDT: Thank you Stu. Today I'm going to talk to you at a very high level, make a couple examples of some our international interactions in the area of digital instrumentation and control. We are extremely active in the

international community. Of all the different international activities we have in the United States, this is probably the single largest technical interactions that we have. We have multi-lateral programs, we'll talk through those a little bit, bilateral programs with a number of different countries. And we also actively engage in the international standard setting process; extremely important because we have vendors that are working to a number of different standards, the IEEE standards, the IEC standards, and to a lesser extent the IAEA safety guides.

So being part of that program is extremely important, to both improve our consistency across the international organizations, but also to understand why people are designing things in particular ways.

We're also very active in understanding what other industries are doing. You heard both from Dr. Holzmann and others today that there's a lot of work going on in other organizations, both in the regulatory side and the actual development side. Next slide please.

In our multi-lateral programs, the largest by far is the Multi-National Design and Evaluation Program. We are active both at the staff level, at the management level, and the executive level in that program. As you know, it's broken down into technology-specific issues, such as digital I&C and also specific vendor applications. We're active on both sides of that.

We chair the digital I&C Committee. It's been very active. It is currently finished with and awaiting public distribution of four common positions in the area of data communications, diversity, simplicity, that was talked about earlier, and also software tools, which is a very big issue, as you've heard. They are also working on a number of other specific policy issues or common positions that are ways in which you can actually understand what common technical

understanding is between the various regulators As we all know, it's easy to talk about it, but once you have to write it down, that's when you really figure out what the differences are, so we've been very effective in that area.

In the areas of the specific vendors we've had the opportunity to work through a number of the differences between our different regulatory structures. Our technical positions, as we talk to each other, we find are very, very similar.

We also have had the opportunity to work for other multi-lateral programs, such as the European I&C program, which is a Western European regulators organization. It's an outcropping of the old four country agreement that was put together in the late '90s when we were developing our current SRP to try and get a feel for what other regulators were doing and that program is an ongoing program as well. Next slide please.

In terms of bilateral changes, I've listed a few of the countries that we've been most active in, but we've been active with a number of countries. For example, Taiwan, as you know, has an ABWR that they're licensing and building. We've had a number of interactions with them, very positive interactions in their review of the ABWR, but also in their use of some of our regulatory structure. They use our ISGs, and we were there last fall to discuss with them what we meant when we wrote them and they also gave us feedback on how they've had challenges and successes in their use.

In China, we've had a lot discussions associated with the licensing of AP1000 and EPR. But we've also had a lot of discussions with their experience in using digital systems. As you may or may not know, the T1 plant which is a VVER has a fully digital Western control room designed by Siemens

and we're getting data on that operational issues.

In England, we've had a lot of interactions with NII both on the regulatory structure and how they're resolving technical issues associated with a number of the new plants. Next slide please.

As I mentioned, we're doing a lot of work associated with international standards. Some of this has been input to updates to the standards, it's been working on driving consistency between the standards bodies. IEEE which is the basis of most of our regulatory structure, IEC which is the basis of many of the other regulatory structures are structured a little bit differently. But there's a lot of common positions, and we have been strongly encouraging what is known as dual logo standards, where the same standards would be published by both organizations. We're had some success in that, in the area of cable monitoring and electrical distribution associated with earthquakes. We're having some success in terms of diagnostics and surveillance testing, and we're working toward other areas. In terms of IAEA, they are redoing their safety guide for digital systems this year. And one of our staff was just there two weeks ago to help them work through various issues and try to get the first draft of that document put together. Next slide please.

So, in brief, what we're getting out of this is not merely a better understanding for ourselves, and a better understanding of what other regulatory bodies are doing, but also a wonderful opportunity to share experiences, an opportunity to influence the design process, through standards and through standardization and harmonization, but also increased access to what the research programs are doing. You've heard Stu talk about our work with KAERI and with other organizations to look at the research aspects, what needs to be

done, as well as what is being done and where you can go in the future.

I know I'm slightly over, but I'll make one more point: We are very proactive as individuals, as professionals, in the organization. We're not just regulators by night. We're also researchers, analysts, and we're very active as a staff in terms of understanding what is going on in the cutting edge. Point of fact, one of my personal research activities is in pro coupling which you heard about earlier with Dr. Holzmann. With that, Bill.

MR. BORCHARDT: That completes the staff's presentation. We're ready for questions.

CHAIRMAN JACZKO: OK, thank you. We'll start with Commissioner Magwood.

COMMISSIONER MAGWOOD: I'd like to thank all of you for your comments. It was very helpful to understand where things stand. Let me start with you, Steve. One of the things, I'm glad you mentioned Dr. Holzmann, because he had some thoughts about advanced methods for verifying software. And I wonder if you could give us your thoughts about where the state-of-the-art of verification really is today and whether we're using it and whether others overseas are using it. And just give us some perspective.

DR. ARNDT: Okay, I don't want this to be a long dissertation, but, in short --

COMMISSIONER MAGWOOD: It could have been a dangerous question to ask.

[laughter]

DR. ARNDT: In short, a lot of the things Dr. Holzmann talked about are already embedded in our review process; in some cases, in a more simplistic

and rote fashion, as opposed to the automated tools that he's advocating. Things like code review, things like validation of standards, things like understanding exactly the issues that go into what makes things complicated and how they're coupled and the independence between systems. There are certainly some areas where we can improve and learn from other industries. In terms of the nuclear community, we're probably on par, if not ahead in most areas from other regulatory bodies; there's obviously a couple of exceptions associated with that, but we're by and large on par with our regulatory counterparts. As you know, we update our regulatory guidance on a regular basis. And we're, I think scheduled to update our SRP, Standard Review Plan for digital, next fiscal year and Office of Research and others will be inputting into that area, to see whether or not we should move some of these more advanced tools into our regulatory process.

COMMISSIONER MAGWOOD: Thank you. One other question for you. One issue that comes up quite prominently in these discussions is, I think almost everyone here has mentioned at least briefly, is the bi-directional communication between safety, non-safety systems. And just again, looking overseas, has there been any different view on this matter, that specific matter, from other regulators versus how we've been looking at it? Is there some insight you can gain as to, you know, why they think the way they think and why we think the way we think, and if you can give us some view on that as well?

DR. ARNDT: Okay, I'll start and maybe Tom can finish on this one. I think our technical views are very, very similar, the basic technical safety issue is that it's a lot easier to assess something that doesn't have bi-directional. What you're concerned about is an action, or a lack of action on the non-safety side

causing a disturbance on the safety side. And if you only have one-way direction. it's a lot easier. If it's two-way directional, there's a lot of technical ways to ensure that is not going have a problem including how you pass messages and whether or not you allow memory to be accessed by one system or another and things like that.

The various countries have very similar approaches. As Tom mentioned, it's more challenging to review those systems if they have more complex solutions to that particular technical problem. Some regulatory bodies, either as a matter of policy or as a matter of proficiency, will have more a stringent requirement than the NRC. By and large, we look at it from a, "If you give us enough evidence that you've done a good job, then we are willing to move forward." The regulatory structure makes it more difficult if that information is not yet available in the Part 52 as opposed to the Part 50 arena. But there's really very little technical difference between the technical sides internationally. There's a lot of issues associated with schedule and policy and how we best implement the particular regulatory structure in that particular country. Did you want to add?

MR. BERGMAN: I mean, I can't comment on the technical aspects, this is definitely not a technical area of mine. It is the adverse effects, I do understand that, but we haven't said you can't have bi-directional communications. Mr. Sliva in his presentation, you know, said that as well. In fact, ISG-4 is specific to communications, including bi-directional communications in one of the NUREGS as well. It's the ability to demonstrate that you're not adversely affecting the safety function, when that's uni-directional that's very easy to demonstrate. In fact, according to my staff, the entire write-up, the

Westinghouse AP1000 design is strictly uni-directional communications. The licensing basis justification for that fit a page-and-a-half, and the review was measured in hours. We still don't feel we have a complete licensing basis for bi-directional communications exist, and those review are taking months and hundreds of hours by comparison.

So, it's a question of can you demonstrate how to keep it uni-directional? And it really becomes problematic where software are providing that protection. The equivalent of a diode, I don't really know how one works, I know it's excess electrons and deficient electrons, but the people who need to know how a diode works, and when we see something called an isolation device in a design and say, "How does that work?" And they say, "It works like a diode." "But how?" And they say, "Well, it's software-based." And we say, "Well, how does the software provide the same types of functionalities as a diode?" Which is just based on physics. And they can't answer the question because the software hasn't been written yet, so when you say, What is my licensing basis? How do I know that that's going to provide that same function and not get changed over time? We need to know that in order to say, you're right, you do preserve the uni-directional communications from a safety standpoint of not causing an unintended fault in the safety system.

COMMISSIONER MAGWOOD: This actually leads to a question I have for you and your answer's actually kind of interesting because I think I heard you say earlier, and sort of made me reflect on something I heard from the vendors when they were talking that it's -- to sort of paraphrase what somebody said earlier, it may very well be true that the evidence that something works does exist and maybe even has been talked about, but until you see the DCD it

doesn't really matter, in effect. And I wonder when you're talking about, you know, whether you can have the software diode -- I would love to see what that might look like -- how -- what do you need to see, as a reviewer, to confirm that that will actually work? Do you need to see the code? Do you need to see the entire code reviewed in detail? Or is there something short of that you can get that will convince you that this software diode will actually work?

MR. BERGMAN: That hasn't been completely determined, I mean, ideally you can have a sufficiently detailed description of functional -- the functions it will provide, such that it can, but when it comes to software it isn't clear whether or not that will be sufficient, or the code itself does become part of the licensing basis. Because if it's providing a protective function, we need to know that it's going to maintain stability over, again, the life of the facility. It doesn't mean it can't be changed, but we may need to reengage in the future if it does change, so at a minimum you're going to need enough functionality description to say, "I'm confident that provided the software's developed in accordance with a quality process, it will always provide that functionality, or with a high degree of assurance, provide that functionality." So you may not need the full code, but we haven't been provided a substitute yet that provides that assurance.

COMMISSIONER MAGWOOD: Let me ask the, sort of the hanging question there then, that I'm sure the vendors will hate, is there a reason we shouldn't require the full code before approving a design?

MR. BERGMAN: I actually have written software in my background, and the thought of putting -- I mean, these systems are very large, I mean, million lines of code. What would we do with it? It's very hard to interpret

another person's code if you weren't intimately involved. That would be, in terms of licensing, that would be very problematic as how do you understand when a change has been made that triggers a 50.59 which triggers a license amendment. We really need to see how they're going to provide through quality processes controls over the software.

MR. GROBE: I'm glad Tom mentioned 50.59, the licensing basis needs to be sufficiently descriptive such that the licensee can feel comfortable moving forward under 50.59 to know what changes they can make without coming back to us and what changes they need come back to us. We have reviewed code. At Oconee, one of the functions -- it was important to the safety involved reviewing certain sections of the code. The real answer to your question is it depends; it depends on how the licensee is choosing to design, how the vendor is choosing to design the specific attributes to the system and how critical that attribute is to the safety decision.

COMMISSIONER MAGWOOD: Is the code subject to inspection?

MR. GROBE: We haven't gotten there yet. That's an interesting question.

[talking simultaneously]

MR. GROBE: Within the context of 50.59, I think --

MR. BERGMAN: Not within 50.59, but certainly we have the authority as a regulator to inspect what they used to build their plant and that would include software.

COMMISSIONER MAGWOOD: And you're not enthusiastic, so I assume that that's something we would actually do if we felt it was necessary?

MR. BERGMAN: If we felt it was necessary, yes. I think getting to

50.59 -- my bigger concern probably is as these systems change with time, will the licensee have the capability to understand whether the changes -- how they affect safety. That's really the first step. I mean, we can check, but -- and verify what's being done, but we're not 100 percent in there, we do rely on the licensee understanding the ramifications of that, and that's probably the bigger question. When you get a new board or you get a new disc, do you understand all the implications upon the designs, especially for these highly integrated designs where you've got controllers embedded in pretty much every component out in the plant, all the sensors. How does that all tie together, what's the effect on that integrated system when I change one piece part of it? Again, if you're overly reliant on software, I think Dr. Holzmann's point about latent defects are key, you can only know so much.

And as an example of that -- and I can't say the design because it's always hard to talk about this without proprietary but, the initial design for the prioritization module had so many inputs, to fully test it, to eliminate latent defects, would have required approximately 10 to the 18th tests. Now, I did some crude math over the weekend and that would be a billion tests a second, which isn't achievable, it would take 30 years. Now they simplified that design down to where only five -- a little over 500 tests would be necessary to fully test every possible combination of inputs. The design still has the same capability from a safety perspective, but you've eliminated the uncertainty over how much of the design you can actually test in terms of hidden faults within that one facet, it's not even a complete design, it's just one facet of the design.

COMMISSIONER MAGWOOD: That's an interesting insight, thank you very much. Thank you, Chairman.

CHAIRMAN JACKZKO: Commissioner Ostendorff?

COMMISSIONER OSTENDORFF: Thank you, Mr. Chairman. I found this very helpful, especially the discussion bi-directional versus unidirectional. And I know a little bit about the diode. A long time ago, I can remember when I went in my fourth submarine -- my fifth submarine, we went from a computator inverters for rod control to SCR fired systems for the SXG plant, and it was a huge technological leap to understand when you're training your reactor operators and the watch officers, so I can appreciate the complexity challenge here as these changes were made. I'm going to start out, I think, with Steve and Stuart and ask a question on the international/other industry area, and then come back to Tom and Pat on a question.

I'm very pleased to hear about the extent of the international involvement, it's extraordinarily helpful and I'm very pleased to hear what those activities to date have been. I guess the question is, is there any conceptually different approach that is very different from how another country is approaching some of these digital I&C regulatory issues compared to what we're doing here in the United States?

DR. ARNDT: There is one conceptually different thing and it varies to a certain extent between different countries, it's a lot more dramatic in other industries, and that is involvement in the early part of the design process. In the aviation industry, the regulators are involved very, very early in the design process, and sitting with the designers and working through those issues. That is very different from what we do. We expect the licensees and the vendors to work through the design issues and the basic fundamental concepts and then present us a design for review. Some other industries, in particular in some other

the countries, are more involved in actual development. So, that's a different design concept or review concept. The other one --

COMMISSIONER OSTENDORFF: Before you leave that one, this kind of ties back into Commissioner Magwood's comment, are you seeing in other countries that there's an expectation of greater maturity of design prior to regulators taking this to look at it?

DR. ARNDT: I don't know that it's more a mature design, but it's an earlier involvement in the design process as opposed to a review of the adequacy of the designs.

The other difference in some countries is the use of third party dedicate -- third party assessors, such as in Germany the use of the TUV organization to assist by dedicating -- not dedicating, but assessing a system, so they actually do some of the testing, as a third party tester on some of the assessment, it would be similar to the -- what was done in the Air Force a number of years ago with the software maturity model and things like that. So, it's a slightly different structure, but by and large of those two aspects, the review process is very similar, obviously a different review structure in some countries. Stu, do you want to amplify on that?

MR. RICHARDS: That was the only point I was going to bring up, but if you're asking do they use the same, basically the same basic I&C design criteria as we do, you know, Steve talked about the review process, but if you're just talking about the hardware and software, is that part of the question?

COMMISSIONER OSTENDORFF: Well it could be, you know, regulatory approaches or, you know, you mentioned I think earlier one of you mentioned the quantification of software liability, you know, is there a different

approach being used in other countries on reliability that is significantly different from the NRC's views?

MR. RICHARDS: My understanding is that it is not. One of our tasks has been trying to find somebody who's been able to quantify software reliability and we haven't identified anyone. Again, it's deterministic, it's like Steve said, and Dr. Holzmann, what you do is you make sure that there's a lot of processes in the development on the front end of the system to try and eliminate as many of the defects as possible and make the system fault tolerance, even if there are faults, the system's still going to work. But there's always going to be latent faults in these software programs.

DR. ARNDT: I think the one exception to that would be the British, they tend to be a little bit more risk-informed than us, but that's a structural reason because they compare risks across technologies, not just nuclear but other energy generations. But by and large the way we do it in terms of assessing regulatory acceptance criteria is very similar.

COMMISSIONER OSTENDORFF: Okay. Let me turn to a question -- I've going to start off with Pat, then go back to Tom, but it's the same kind of question. We've heard from the previous panel some notion of perhaps complexity of systems, especially systems that are in use in other countries, not, basically making it through the NRC's regulatory framework the way they experienced overseas. And, you know, from the NRR's standpoint and then from NRO, I'd be interested in any comments you might have on that topic as to whether or not there's been any -- I used the phrase with the previous panel, question about sub-optimization of digital I&C systems based on having to alter the design of the system to fit the regulatory framework used by the United

States NRC.

MR. HILAND: I'll just give you an example. You heard us talk about the Wolf Creek and the field programmable gate array review that we did. When that originally came in, they were referencing FAA standards. They did not reference the IEEE standards that are endorsed, not just endorsed, but required by our regulations, IEEE 603. Now, as you are aware there's nothing wrong with that, but we would have been very challenged to go and compare the FAA standards that they referenced in that original submittal to what we would find acceptable under our standard of review plan guidelines. The end result was that the manufacturer went back himself, the design engineer, and did that work, and then several months later presented it with referencing the IEEE standards. I'll just throw that out as an example for an item. Tom?

MR. BERGMAN: We're not -- I'm not aware of where we -- and it just doesn't seem like the NRC to say reduce the level of safety. The problem is with complexity is we haven't been convinced that there's a safety enhancement with the complexity, and even if there is, even if it's equivalent level of safety, we're OK with it. We had discussions principally over the summer -- we're just looking at the trajectory of the two reviews and the desired schedules by the applicants. We were saying, "If you continue on this design path, we just don't see how we're going to meet the schedule you want. We can continue the review on the design we have in front of us and the schedule needs to change, or you can change the design such that you can make the safety case easier and we can maintain the schedule you've got." But certainly if an applicant, any applicant, came to us and said, "Hey, this feature actually enhances safety," that's something the NRC is going to listen to with open ears.

COMMISSIONER OSTENDORFF: Thank you. One final question. Jack, I'm going to ask you this and Bill, you may want to chime in, this deals with human resources of the NRC staff, I know there's been a lot of hiring over the last five or six years, and a lot of ramping up, bringing on some very talented people to work in these areas, are you satisfied that we have an appropriate level of expertise in this area going forward?

MR. GROBE: It's a continuing challenge, you know, some of our staff are more advanced in their careers, I think, we try to make sure we don't say "old," but we just lost Bill Kemper to California, he's our reviewer in the field, he's going to be teleworking and assisting us with the Diablo review and that will be his last activity before he retires. So, continuing that pipeline is a challenge, but right now we have sufficient resources and I think I can speak comfortably for New Reactors as well, that the reviews are progressing, the development work that we need to do, the interaction with Research is progressing, so we're in good shape. It's a continuing challenge.

COMMISSIONER OSTENDORFF: Thank you. Thank you, Mr. Chairman.

CHAIRMAN JACKZKO: Commissioner Svinicki?

COMMISSIONER SVINICKI: I want to thank you all for your presentations, I'm puzzling over something that since I heard it I've been kind of fixated on. Pat, I don't know -- it confuses me that Jack Grobe would have to continually ask you about how you intend to occupy yourself. I would think that the Division of Engineering in NRR isn't really in danger of having a whole lot of idle hours that you just have to while away, so there's some story there perhaps I'll learn about it at another time. But one other thing, I think, I would more

seriously ask you to clarify is that, in response to Commissioner Magwood's questions he got a couple of responses, just to paraphrase like on the issue of looking at code or inspecting the code and the answer was, "Well, we really are still looking at that issue." Now we have approved some things, so what am I missing there in terms -- we have some significant unanswered questions about our approach, but yet we've approved some amendments and things.

MR. GROBE: It was a fascinating question that we really haven't tackled yet. We're in the middle -- the context was inspection, what our inspectors in the field are going to do --

COMMISSIONER SVINICKI: But it was also in the review, because there was discussion, I think Tom said, "Oh, I wouldn't want to look at all that code," and then Jack, you said, "Well, we have reviewed code and it has been the basis of our approval of some things."

MR. GROBE: Where a licensee and the specific issue is the -- at Oconee, it had to do with the service module and how that was connected and the communications. The independence of the communications was assured through a certain set of code and that was the way the licensee wanted to design the system so we looked at the code to make sure that it met the safety requirements. I made some notes here that I hadn't thought about before and we have part of the ROP is an inspection called the SSDI and I'm struggling right now for the acronym, that it's our triennial design inspection, very complex inspection, we're going to have to develop an expertise to look at changes in the digital system. That expertise, at a code level possibly, and that expertise I don't think exists right now in the Regions, so that's --

COMMISSIONER SVINICKI: Couldn't you start by looking at the

integrity of the configuration management and controls? Wouldn't that be your starting point instead of just diving right into the code?

MR. GROBE: That's right, that's exactly the foundation for the SSDI. It's the configuration management and how the licensee has chosen to manage that, and then diving down deeply into the design, it's a very deep, narrow inspection where certain things are validated. That we have the DAC inspection that is being piloted right now, as well as the pre-op and operational inspections that are ongoing at Oconee, so there are three different kinds of inspections that we're going to have to continue monitoring and then developing the expertise -- continuing to develop the expertise in the Regions.

COMMISSIONER SVINICKI: Okay, thank you for that. And Pat, as you described, the reviews underway right now and the other things that you might have on the horizon, I would ask you two questions. The first is it sounds like those are all -- they can differ substantially one from the other and you mentioned that Diablo is a digital to digital conversion, I'm not sure I knew that before you said that, so you have a lot of variability there, is that a challenge in terms of your resource modeling for going forward? The second part is how much do you know in terms of letters of intent and other amendment requests that you might be receiving over like a 2 to 5 year timeframe?

MR. HILAND: Let me address the first -- the last question first, letters of intent, I have no letters of intent. We did, in one of our digital I&C Steering Committee meetings, the industry's representative mentioned that he had in his fleet 17 sites that he had planned to go with digital upgrades once, you know, the dust has settled and there's predictability in our process. If next month, somebody sends me in 17 amendment requests --

COMMISSIONER SVINICKI: He didn't say, "Here I've got them in my briefcase."

MR. HILAND: No, he didn't say that, he said he's not going to --

COMMISSIONER SVINICKI: At 30,000 pages apiece that would be pretty bad.

MR. HILAND: That's right, if that type of an increase in applications came in I certainly would be challenged. Right now with the reviews we have about 6 to 8 on ongoing reviews of topicals that are ongoing in the group plus we have the Diablo Canyon and a few other minor ones that are ongoing and I have sufficient resources for the next two years. But looking out, using 2 to 5 years, if I get information that industry is going to increase and come in in multiple, I could probably handle two major upgrades with the current staff along with the routine work, 3 to 4 would be a challenge. Anything more than that would be a real challenge with me. I think I answered your question?

COMMISSIONER SVINICKI: Well, I asked about they can all look quite different, so the variability, how do you develop a resource model for that? Does it vary substantially depending on what you're looking at doing, what kind of -- what the review would entail?

MR. HILAND: We have, as you know, a Standard Review Plan. Chapter 7 in the Standard Review Plan, to date it covers all of the applications that we've received over any -- and that Standard Review Plan is up to the branch chief and staff in discussions with me, is what areas they should cover and what areas are not applicable. So, we're fine with the guidance documents today.

COMMISSIONER SVINICKI: Okay. Well it sounds like, from your

answer to the first part of the question, that if the dust settles in ways that people feel positive about, you might be a victim of your own success, and suddenly there would be a lot of interest in submitting things. That's very challenging for us, obviously we can't fluctuate and so it may be an area that would potentially lend itself to an NRC engagement with industry about, you know, they'll need to do some coordination, maybe, and look at pacing those out in a way that's going to make some sense from a resourcing standpoint. It sounds like you haven't yet begun those discussions, but you're beginning to get some sense that they may be necessary?

MR. HILAND: Yes, I agree.

COMMISSIONER SVINICKI: Okay. And another area that was touched on, I think, by our representative from Oconee, was talk of reactor operators, of training, of simulators, and I know it wasn't technically a topic for today, but I'm sure someone could give some sense of how we're keeping a pace on issues for operator licensing, and digital control rooms, and things that -- it's just something that I haven't heard about in awhile and I don't know that we have our direct expert at the table, but just generally, are we working through that process with applicants and operators?

MR. HILAND: I'll start. Region II has a responsibility for direct operator licensing. Of course the program office exists in NRR, but ever since we issued the license amendment request and we knew what the schedule was, the Region developed what they call a project plan for inspection. That project plan looked at the simulator, or will look at the simulator activities and then underneath that is a very, very detailed inspection plan. It's not the -- if you look in the inspection manual, there's one module that says, "Go look at modifications

every two years and spend about 100 hours on it." That's not the inspection plan that they've created for Oconee. As a matter of fact, it could be 10 times that amount of effort on Oconee. Now, we did send one of our design engineers, during the site acceptance test, down with our inspectors and as you heard in the Safety Evaluation Report, we highlighted some 40 plus items that we suggested the inspection staff in Region II look at. I don't know all the details of the simulator, but I know the operating examiners are aware that the simulator has been upgraded, I just don't know the timing of when they're going to follow up and do their onsite review.

COMMISSIONER SVINICKI: All right, thank you. Jack, did you want to add something to that more generally or in new reactor space, just following the issue of preparing to be able to license operators for a new digital control room?

MR. GROBE: I wasn't going to add something on the specific operators, but the translation of that is to our staff as well and I can't remember which Commission meeting it was on digital -- we've been having them roughly every six months -- but we presented the Technical Training Center's plan for upgrading to digital training for our own staff, and the utilities are doing the same thing, and it's going to have to be a key component of our ongoing licensing of specific operators as well as inspection.

COMMISSIONER SVINICKI: OK. Thank you. Thank you,

MR. GROBE: Tom, did you have any --

COMMISSIONER SVINICKI: Oh, Tom?

MR. BERGMAN: I'm not the right person, it would be the Division of Construction Inspection and Oversight Programs. It is the training of operators

though, construction of the simulator, is very important to meeting a construction schedule. We do have a nice graphic that illustrates that timeline and we can just send up to you that with the specifics for the plants that are entering construction.

COMMISSIONER SVINICKI: Okay, thank you, thank you -- appreciate that. Thank you, Mr. Chairman.

CHAIRMAN JACKZKO: Tom, maybe I'll start with you, you briefly touched on the issues with the discussions with the ACRS on DAC and the DAC closure process. Could you give a little bit more of a detailed update on where that stands, and what you think the remaining issues are that need to be resolved?

MR. BERGMAN: Well, again, I think the remaining issues are really with the post-COL inspection activities of the DAC. The remaining designs that have yet to come to the ACRS have either a few or no DAC. The ESBWR was -- the ABWR -- it's hard to quantify because you can count so many ways. ABWR has a lot of DAC, so they may be interested in that, but that's the one we're piloting -- testing the inspection procedures on. The ESBWR has a large number of DAC, but until we enter the construction phase, there's probably not going to be further engagement on it. So, again, not only us but the applicants now understand the specific concerns of the ACRS, so when the designs are presented to them for ACRS approval, they make sure the application and the explanations in that meeting make it clear how the safety finding can be made with the existence of DAC.

CHAIRMAN JACKZKO: Do you anticipate there being potential scheduling challenges, if, in the future, ACRS is looking to see if we're in a post-

COL, DAC close out, ITAAC closure process -- will there need to be a scheduling coordination with ACRS, if ACRS is going to have a role in reviewing some of this DAC closure?

MR. BERGMAN: Yes, the nature of that role would affect how difficult that is, I mean, we coupled with NRR license renewal power uprates. We fully booked the ACRS calendar, and so scheduling anything new is always a challenge, but we have a very good relationship accommodating each other's needs because things have moved around. I mean, where the staff ended was, "Hey, you know, let us do informational briefs with South Texas on what we learned during the inspections and see if that satisfies the ACRS concerns." And certainly those types of briefings are not that difficult for us to support and to schedule with the ACRS.

CHAIRMAN JACKZKO: Well, I appreciate that and I certainly -- I would rather see us trying to resolve this as much as possible now, because I would hate to get into a situation in which we're going through a very complicated review process for ITAAC closure and then we have some unresolved interests on the part of ACRS, and so I think it's something we'll take a look at and perhaps in one of these upcoming design briefings.

MR. BERGMAN: And I think we are briefing them on the results of this inspection in March and May timeframe, so we'll get some feedback from that presentation if that approach, initial feedback, one data point – is sufficient.

CHAIRMAN JACKZKO: One of the issues, maybe Jack, you can comment on this, as you start to sunset the Steering Committee and move to a new kind of more traditional regulatory model for digital instrumentation and control issues, maybe you can just talk on how we will continue to ensure

technical consistency or review consistency between the Part 50 side of the house and the Part 52 side of the house?

MR. GROBE: Thank you. When we formed the Office of New Reactors, that was previously all under the Office of Nuclear Reactor Regulation, we established a joint procedure in both offices on technical consistency. And we used that aggressively in the digital arena, it establishes different levels of review by the two offices, up to complete and full parallel reviews, to peer reviews supporting the other offices, and lower level reviews, depending on the importance of the document that's being reviewed. Some of the topical reports that have been submitted to support new reactors are also applicable to operating reactors, and Pat and Tom have worked out a way in which the reviewers work together, and those procedures have existed -- one of our senior level advisors in NRR is responsible annually to put together a report on technical consistency between the offices, Ken Karwoski in our Division of Component Integrity, and he does a lot of evaluation and serving of the staff and the branch chiefs both in NRR and NRO to ensure that that's a robust system, that it doesn't have any gaps in it. So, it's an area that we particularly focus on.

CHAIRMAN JACKZKO: Well, certainly as we go forward that will obviously be an important area and I encourage you to continue focusing on that. The last question, and Tom, maybe this is probably an unfair question, but I'll probably ask anyway --

MR. BERGMAN: Sure you don't want to ask Stu that?

[laughter]

CHAIRMAN JACKZKO: Stu, do you think we'll ever --

[laughter]

CHAIRMAN JACKZKO: -- think we'll ever approve a design with bi-directional communication?

[laughter]

CHAIRMAN JACZKO: I wouldn't vote for it.

[laughter]

MR. BERGMAN: Again, I think we can, and, you know, we'll see what the future bears, we know there's more applications coming in over the horizon and small modular reactors may take that further with multiple units feeding into one control room. So, again, it's possible, we just haven't seen a licensing basis that makes the case yet.

CHAIRMAN JACKZKO: Well thanks, I appreciate that and we'll certainly continue our dialogue with the applicants I'm sure in that area. I would just note I think that it does raise a whole interesting set of questions I think, as Commissioner Svinicki raised about, to what extent source code would ever become part of licensing basis or inspectable and I know having done my own code development that it becomes a very personal activity and it's very rare you can imagine a situation perhaps 10 years later -- whoever developed the code, it takes a tremendous process to ensure consistency in modifications and updates to that code and somebody looking at it, brand new, from my experience in this area, would very likely recode the entire process because this is often too difficult to sometimes figure out what a particular software developer was doing when they were coding something and it takes a tremendous process to ensure knowledge and understanding of that code base to be able to modify it and maintain it in that way. So it's certainly an interesting area, but I think more that, I think as Commissioner Svinicki indicated, that the more that we're relying on the

processes there to ensure appropriate change processes and consistency in the code, probably the safer we'll be -- well not safer, but the better off we'll be. That's always a difficult word.

Again, I want to thank you all for your presentations. As I said at the beginning, I think we have come a long way, I think, from the first meeting we had on this subject in 2006 and I think it's really a good sign to see that we're moving into a more regular -- regulatory approach for this in sun-setting the Steering Group and moving into a more traditional review type process. So I think it's certainly a testament to where we've come, the completion of the Interim Staff Guidance I don't think when we started would have seemed really possible, I think in a lot of ways. But we've come a long way and updated a lot of guidance and I think now the challenges as I hear them are actually now taking that and implementing it and I suspect as we go along there'll be improvements and enhancements and I think we got some good information this morning from some of the people involved in the process about ways to continue to refine that and make it better, but in the end, obviously safety's got to be the number one concern, and we'll continue to make sure that's the case.

We have a few minutes if there are items any Commissioners wanted to talk about. Well good, I want to thank everybody and we're adjourned.

[Whereupon, the proceedings were concluded]