UNITED STATES NUCLEAR REGULATORY COMMISSION

BRIEFING ON DIGITAL INSTRUMENTATION AND CONTROL

+ + + + +

WEDNESDAY

JULY 18, 2007

+ + + + +

The Commission convened at 1:00 p.m., Dale E. Klein, Chairman presiding.

NUCLEAR REGULATORY COMMISSION

DALE E. KLEIN, CHAIRMAN

EDWARD McGAFFIGAN, JR., COMMISSIONER

GREGORY B. JACZKO, COMMISSIONER

PETER B. LYONS, COMMISSIONER

PANEL 1: STAKEHOLDERS

KEN BROWN, Invensys VP Global Supply Chain and Measurement and Instrumentation

AMIR SHAHKARAMI, Senior VP Engineering & Technical Services, Exelon Corporation and Chairman, NEI Digital I&C and Human Factors Working Group

CHUCK WELTY, Technical Executive, Nuclear Power Sector, Electric Power Research Institute (EPRI)

CYNTHIA McGINNIS, Manager, Nuclear Systems Engineering, New Plants Engineering, Westinghouse Electric co.

THOMAS BOWE, Executive Director of Reliability Integration, PJM Interconnection

HOMAYOON DEZFULI, System Safety Manager, Safety and Assurance Requirements Division, Office of Safety and Mission Assurance, National Aeronautics and Space Administration (NASA)

PANEL 2: NRC STAFF

LUIS REYES, Executive Director for Operations

WILLIAM BORCHARDT, Director, Office of New Reactors

RICK CROTEAU, Deputy Director for Engineering Research Applications, RES

JACK GROBE, Associate Director for Engineering and Safety Systems, NRR, and Chairman, Digital Instrumentation and Controls Steering Committee

MICHAEL MAYFIELD, Director, Division of Engineering, NRO, and Digital Instrumentation and Controls Steering Committee Member

MARK CUNNINGHAM, Director, Division of Risk Assessment, NRR and Digital Instrumentation and Controls Steering Committee Member

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

CHAIRMAN KLEIN: Thanks for coming today. We look forward to an issue that's near and dear to all of our hearts on Digital Instrumentation and Control. One of the things that Commissioner Lyons has been active in and I certainly support is I think as a Nation we really need a major academic program that is looking at digital interface and controls that addresses needs not only for the NRC but for the industry, for other agencies like DOD, DOE and others.

I think when we look at Digital Instrumentation and Control it's an area that's really important and I think in some respects we're lagging behind what some other countries have done. So we're certainly anxious to hear from you today on what we need to do and what we need to do better.

Any comments from my fellow Commissioners before we start? You can begin. Thanks for coming.

MR. BROWN: Thank you very much. My name is Ken Brown. I'm with Invensys. I'm Vice President of a number of areas. One of my areas of responsibilities is to complete quality program overall for IPS inclusive of our Nuclear Quality Program.

Invensys itself is a company that has 30,000 employees and we operate in 60 countries globally. Invensys Process Systems is the area that focuses on process control and we have some great brand names that have been out there such as Foxboro, Triconex and SimSci-Esscor. With that base, we've been

servicing the nuclear industry for some 50 years.

We believe in the nuclear industry. We support it and we're working hard in terms of many of the projects that are active right now to make sure we continue to support it going forward. Let's go forward to the next page.

The issue today in terms of Digital Instrumentation and Control from our perspective we are dealing with – right now I'm on page three for those who are following along – we're dealing with issues such as D3, the diversity and defense in depth, the risk informed digital I&C, operator training, cyber security, and last but not least some references in terms of lessons learned that we've seen in other process industries we've supported globally. I'll talk to each one of these issues briefly and then wrap up within the allotted eight minutes.

First off, in terms of D3, our perspective of this is that one of the areas to address this issue is through the use of technology. Within IPS we have our Triple Modular Redundant System that is appropriate and proved in terms of RPS and ESFAS, with a diverse digital controller of I/A for the non-safety PLC requirements.

So we have a technology base that can be used to help solve this problem. We do not anticipate the need to challenge the license base or the operation position. On to page five.

In terms of D3, there's an issue that we have and a concern both for Invensys as well as for all the stakeholders in the industry is that we need to have a workable and understandable position in terms of the issues of concern and

understanding the position from the NRC. Having a delay with this and having a lack of clarity can create confusion and concerns and delays overall with the process.

One of the elements that we would like to have a discussion on is relative to Common Cause Failure. There are many industries that have dealt with this and have dealt with the use of control and digital control for critical processes. We need to leverage the diagnostics and the highly developed platform to help manage this risk.

A second item to discuss is in regards to Risk Informed Digital I&C. The first bullet – now I'm on page six – the first bullet that I talk to here is relative to the consultative teaming relationships. This actually goes to the core of how we like to address certain industries and certain requirements. We realize that as much as we have some strengths in technology, we also need to make sure we are listening correctly to the other stakeholders and to the direction set forth in the industry and its best to do that collectively overall.

We believe that the TMR technology which has been applied correctly and safely on safety mission critical systems and life critical systems and this particular technology currently supports very high PRA numbers. As we look at the process going forward, we'd like to make sure that we evaluate and take credit for the methodology using this technology, looking at what's been done in other countries and other industries globally. On to page seven.

In terms of Operator Training, one of the great benefits in terms of the

digital I&C is the ability to get issue specific diagnostics and fault tolerant diagnostics information to the operators. We can now, at a much clearer level, describe what is operating in the plant and describe to the operators. This reduces the requirements of some of the training and releases some of the burden for those who are operating the plants in terms of the ongoing training. We know that this can be used on important to safety and safety related applications minimizing the training requirements. On to page eight.

In terms of cyber security, the Invensys perspective is that we are committed to the industry leading cyber security initiatives. We understand the issues. We understand the requirements and we believe they are valid issues to be addressed as we progress in the digital I&C.

From the Invensys perspective, we'll utilize the Wurldtech Securities Achilles Level 1 assessment as a test for the cyber security benchmark. That's the process we'll use and we'll work with the overall industry as we get better clarification in cyber security. On to page nine.

In terms of lessons learned from other industries, this is one area where the breadth of exposure for Invensys Process Systems really helps out. We've got applications and technology on many critical continuous process applications. The Triconex TMR System that's in place is by far the most trusted safety system that's in use in continuous processes worldwide. We'd like to leverage that further in terms of helping to solve problems in the nuclear industry, specifically with the guidance in requirements of the NRC.

A second point, and this is something that we've worked hard and it's part of the DNA of IPS, is in terms of obsolescence. We know that as you start and you get a licensing going through, that's just the first step. There's a very long process in terms of how those plants are operated over 20 or 30 years. Our history and our technology has been such that we support the platforms and we support ways to migrate forward as it takes place.

It's a digital technology. We need to make sure that we're supporting it now and we will support it over the duration of the facility. We are proud of the use of the digital off-the-shelf technology that's inherent in the Triconex TMR system to help generate a solution under the 10CFR50 Appendix B program.

And again, the platform that we're using to address many of the requirements within NRC within the nuclear area are based on strengths that we've had and we have been using for many years in other elements of the process industries.

In conclusion, we're very pleased with the progress that's taking place as of late with the recent working groups and the discussions with the staff. We'd like to, within Invensys, help to facilitate the transfer of knowledge from other mission critical and high reliability industries and how we can apply that to the nuclear area.

We believe that the staff should continue, as appropriate, to develop consultative relationships with the other stakeholders, many of us around the table and others in the industry to make sure that we're working together on the right

items.

On the last page, page 11, we, within IPS, encourage the staff to engage on the I&C design early in the COL phase for the new builds. It can be a gating item. We look forward to working with everybody to mitigate the impact. We are committed to supporting this industry. We've supported it for 50 years and we'll continue to support it for many years to come. We look forward to helping resolve the issues not just on the new builds but also on the brown field facilities that are out there and that do require upgrades to digital I&C. Thank you very much.

CHAIRMAN KLEIN: Thank you. It turns out that I was not properly trained on the exact order of the starting. I'm normally accustomed to the victim that's in the middle is the one that starts. So I had assumed that that was the order and I now see that there is a participant list that I should have started first with Amir. So we will restart – you don't have to give your presentation again.

MR. BROWN: If you want me to, I can. I'd be glad to do it.

CHAIRMAN KLEIN: Sorry for that activity. We'll get back on the order. Thanks, Ken.

MR. SHAHKARAMI: Good afternoon Chairman Klein and Commissioner Lyons, McGaffigan, and Jaczko. It is my pleasure this afternoon to present industry perspective on the application of digital technology to U.S. nuclear power plants. And to me this is a follow-up meeting with you since we met several months ago about where we are and where we need to go. Definitely been impressed with the level of interaction with the staff and the sitting committee

meeting that we have held several times.

The topic I'm going to discuss on page two is the objective of what we do; the communication project plan that has been developed and then wrap it up with conclusion. Page three.

We believe the application of digital technology is essential for the future of nuclear industry. That includes the digitized work force that's going to come to our industry. Digital control and protection systems are an integral part of new plant designs as well as new fuel processing facilities.

Digital technology is important for current operating units in addressing obsolescence and will enhance safety, availability and reliability. We certainly agree with Commissioner Lyons' statement at the IAEA technical meeting of common cause failures held this past June where he stated that we must keep the safe in Digital System design. And with that to do, we must find the appropriate ways to apply the concepts of redundancy, diversity and independence. Page four.

In my capacity as Chairman of the NEI Digital I&C and Human Factors Working Group, I want to emphasize that this working group provides the focal point for the integration and coordination of industry activities involved in the application of digital technology in existing and new nuclear power plants.

We are also making sure fuel facilities are aware for activities and involved. We recognize that NRC may receive different messages from various industry resources. If those messages are different than what are communicated and what

NEI brings to the table to NRC, then we need to respectfully request NRC to contact us for the necessary clarification.

A key element of success is correct and timely communication. The Digital I&C Sitting Committee provides an excellent mechanism for resolution on conflict in messages as well as providing management attention to the issues. On page five.

The project plan provides a disciplined framework that should allow industry and NRC to achieve resolution and closure on the technical issues that have been identified. As you know, we have a mirror organizational structure in a working group similar to NRC with six steering committees, with six task force work groups and a sitting committee that have met on several occasions.

We must be vigilant in our effort to maintain the necessary focus on safety. We must be cautioned not to let near-term action impact our ability to achieve longer-term objectives. The reason I'll make that statement is we really need to be careful not to establish arbitrary dates, such that we get a product that doesn't meet the final outcome and we get into this loop of revision.

I think we need to plan the work and work the plan, even for the short term deliverables. The project plans that have been made publicly available points us in the right direction, but the journey to success has just begun.

Industry and NRC must apply this tool to assure the required level of management oversight and coordination to achieve ultimate success is accomplished. I really think your oversight, your interest and potentially semi-

annual update be appropriate to see how we progress through all the work that we have to do because we have a lot ahead of us.

On the last page, conclusion. I can tell you that progress has been made. The involvement today compared with six or seven months ago is much different. We're getting experts, we're getting academia, we're getting vendors, we're getting industry, and your staff, and really talk about issues. We may not align on all the issues, but that's okay. That's a healthy environment and I think that helps us to put the issues on the table and work through it.

Significant effort must continue to be extended to successfully achieve the objective of a stable, predictable and timely licensing process. We must maintain the flexibility to integrate lessons learned and other improvements as we pursue the longer term activities.

Continued management will be necessary to ensure that our longer-term goals again are achieved. The industry supports the efforts toward safety focus application of digital technology to current and new nuclear plants.

One of the issues, and we have discussed this several times in our sitting committee, is we have these six task forces and each task force that's establish what the deliverables are; the key deliverables, both near term and long term. What I have been asking is an integrated plan that brings all of this together with the priority and with the ownership, who's going to own it, by what date, and be a vehicle for oversight to make sure we understand what resources are required. Because we don't look at this as a project with a start date and end date,

populated with the demand of resources, I think it's going to be a tough journey.

I think we need to appreciate what it takes to go through all these elements that are discussed and be successful. This completes my presentation. And if you want to hold this for the end for question, I'll be happy to do that.

CHAIRMAN KLEIN: I think what we'll do is we'll go through the presentation and then we'll have questions. Chuck?

MR. WELTY: Good afternoon. I'm Chuck Welty. I'm a technical executive in the EPRI Nuclear Program. Would you key the EPRI slides, please? I appreciate this opportunity to provide an overview of EPRI's role in the application of digital I&C technology. Slide Two, please.

This is a list of the acronyms that appear in the presentation, which I will make every effort not to use more than a few.

CHAIRMAN KLEIN: That will be appreciated.

MR. WELTY: EPRI, NEI and I&C I will probably use. The rest I will try to stay away from. Slide three, please. EPRI has been investigating key Digital I&C issues since the mid-1980s. At that time, we were deeply involved in the development and implementation of digital feed water control systems. In the early '90s we were working on guidelines for licensing digital system upgrades, software verification and validation and electromagnetic interference testing.

More recently our work has concentrated on the evaluation of commercial digital equipment for safety applications, control room modernization, application of risk methods to I&C systems, and the implementation of wireless technology for

equipment monitoring and diagnostics.

Research is guided by an extensive and knowledgeable utility advisory structure, which includes experts in instrumentation and control, risk, human factors engineering and advanced nuclear technology. All of the U.S. nuclear utilities participate in our programs and additionally there are ten international utility participants.

Mr. Shahkarami is Chairman of one of the committees, in fact the senior level committee, that provides oversight for this I&C program.

In addition to being the basis for consensus technical positions, a number of the documents that have come out of this earlier work have been reviewed and accepted by the staff through safety evaluation reports, generic letters, regulatory issue summaries and incorporated into the Standard Review Plan. Next slide, please. Slide four, actually.

This is a listing of the specific areas in our I&C program where we are addressing digital I&C technology in one form or another. Much of the already completed work in these areas is directly applicable to current issues; at least that's our view. Our current focus, the focus since probably the fall of 2006, has been in preparing position papers and reports that draw from these existing results and feed in through the NEI working group and the industry task working groups to help facilitate resolution of the key issues that have been identified and are currently being identified. Slide five, please.

This lists the four specific areas of focus. In defense-in-depth and diversity,

we are preparing two position papers that provide an integrated approach for assessing common cause failure vulnerability. This approach considers a combination of design and defensive measures as well as diversity to protect against common cause failure with the goal being to establish reasonable assurance of adequate protection without being overly prescriptive in the design.

In the risk informed area, we are again preparing two position papers. We believe that valuable risk insights can be extracted now even without precise knowledge of failure probabilities and without new modeling techniques. Insights such as the fact that I&C is a minor contributor to plant risk and even with high assume failure rates, the digital I&C contribution remains small.

Risk methods can also provide results that identify events that may be safety significant from an I&C perspective as well as situations where the addition of diverse backups might actually have an adverse impact.

We believe that this use of the risk methods is consistent with the recommendations of the 1997 National Academy and National Research Council Report which was mentioned at least in passing in the last Commission briefing in November.

In the human factors area we are preparing three reports; one on minimum inventory of human system interfaces, one on guidance for creating and using computerized procedures and one on a graded approach to human factors engineering. Several of these position papers have been completed and some have been given to the staff. The remainder are scheduled for completion this fall

and they will all be given to the staff.

The final item up there on slide five pertains to our examination of INPO, that's Institute of Nuclear Power Operations, that wasn't in my list, by the way, and NRC reports of digital system failures. We expect to capture insights on the types of design and diversity attributes that are most important in practice and possibly obtain some failure statistics. Right now we have 500 event reports that we are reviewing and we expect to have preliminary results from this review sometime this August. Slide six.

In conclusion, our interaction with the staff, EPRI's interaction specifically with the staff, has increased during this past year. We believe there's opportunity for more improvement in that area. We will continue to work with the staff to more closely coordinate and integrate our programs.

We support the NEI working group and the related interaction with the industry task working groups to develop a comprehensive strategic plan for digital instrumentation and control. We are aware of the staff's actions to issue interim staff guidance documents and we consider that only a starting point for a comprehensive solution and we continue to want to work with the staff and our utility funders continue to support the fact that we should work with the staff to achieve comprehensive and complete resolution on all the issues that have been identified. That completes my prepared remarks.

CHAIRMAN KLEIN: Thank you. Cynthia.

MS. McGINNIS: Good afternoon. I'm Cindy McGinnis. It's my

pleasure to represent Westinghouse this afternoon and talk with you about the AP1000 Digital Instrumentation and Control. May I have the Westinghouse slides, please; slide two. In looking at the scope of the design certification for the AP1000 I&C, a number of issues were resolved for the AP1000 design during the design certification, including the functional design, identification of the regulatory guidance that would be used going forward and also the basic architecture.

Some of the key licensing issues were included in the design certification scope and were resolved during NRC review. Those include branch technical position 19, definition of the I&C minimum inventory and also definition of the diverse actuation functions for the AP1000 plant. The design certification originally did not include a commitment to a safety platform; therefore, the design certification did include design acceptance criteria for the safety related I&C design. Westinghouse is continuing to develop the detailed design and has selected the Common Q platform for the AP1000 safety platform. Next slide, please.

The AP1000 plant design for safety is a very simple, passive safety system design. The plant safety systems require one time component actuation to perform their safety functions. Components are actuated once; no modulation or further control of the components is required. This simplified safety design results in straightforward I&C design.

As previously discussed, the Common Q platform has been selected for the AP1000 safety system I&C. The Common Q system has been generically

reviewed and approved by the NRC. The simple plant safety system design going to be implemented by an approved platform results in a simple digital I&C system.

The detailed design implementation of the I&C is underway and Westinghouse has submitted technical reports to the NRC for review of the detailed design. The detailed design implementation is being developed in accordance with the existing requirements and guidance.

Westinghouse is interacting with NRC staff to gain acceptance of the detailed design under the premise that the existing NRC requirements and guidance are applicable and sufficient for the determination of a reasonable assurance conclusion. Slide four, please.

The fundamental aspects of the AP1000 safety system I&C are the same as that in Westinghouse operating PWRs. The functional basis used is simple, straightforward algorithms. These direct algorithms result in direct and transparent safety I&C functions allowing for straightforward implementation, pre-operational testing, as well as surveillance testing during plant operations.

The architecture basis is also the same as operating plants. Divisional independence, safety/non-safety separation and isolation are key elements included in the AP1000 safety I&C System design.

The communications and architecture for the AP1000 are driven from the existing operating plant design along with operating experience. The result is that the transition from analog to digital implementation does not impact these fundamentals. Slide five, please.

There are some areas where digital has some more direct impacts that we haven't really seen on our existing analog systems. The requirement for diverse actuation functions is an example. For AP1000, the functionality of the diverse actuation system was resolved and certified in the design certification rule.

Due to the flexibility of a new and passive plant, the diverse functions for AP1000 are designed to use separate sensors and for the most part separate actuators than those used by the safety systems. The simplified safety design of the passive plant results in a fairly contained set of diverse functions and the new plant allows for flexibility in providing these diverse functions.

Another example of digital implementation consideration is the priority when safety and non-safety systems can interface or actuate a safety component. The AP1000 philosophy grants priority to the safety system actuation. Lastly, cyber security is an issue that is evolving. Slide six, please.

The AP1000 licensing effort is well under way. AP1000 design certification resolved many of the key licensing issues using AP1000 specific design information. Westinghouse has been working to develop and submit technical reports and recently AP1000 design certification document revision 16 to resolve some of the I&C design acceptance criteria.

Interactions with the NRC staff to resolve the design acceptance conclusion criteria are in progress and Westinghouse has submitted a number of technical reports, including reports on communication, architecture, and Common Q implementation. The interactions are focused on establishing what level of detail

design is necessary to establish sufficient information for the staff to reach a reasonable assurance conclusion. The existing NRC regulatory criteria and guidance are sufficient for the review. Slide seven.

Westinghouse has prepared and submitted a technical report on the AP1000 Cyber Security Plan. The plan is consistent with the NEI-04-04. Westinghouse is working both with NRC and NEI to establish an acceptable program. All of the technical reports are a key element for revising the AP1000 design certification rule.

Westinghouse has formally submitted a request to amend the rule and is working with the staff to satisfy their reasonable assurance requirements. Westinghouse has been working to support resolution of the AP1000 I&C issues by spring of 2008. Next slide, please.

In conclusion, it's important to recognize the significance of the work that was evaluated during the AP1000 design certification. The design certification documented and resolved many of the I&C issues for the AP1000 design. The regulatory basis established in the design certification continues to remain valid.

Westinghouse's position is that the existing regulatory criteria and guidance are sufficient and applicable to the evaluation of the AP1000 detailed I&C safety system design. Westinghouse has proposed to resolve portions of the design acceptance criteria during the NRC review of the proposed DCD amendment. The result is intended to be the elimination from the design certification rule of those design acceptance criteria associated with the design scope added in the DCD

Rev. 16. Of course, this is contingent upon successful NRC reasonable assurance conclusion.

Lastly, although this presentation has focused on the AP1000 I&C licensing, Westinghouse is also an active supplier in the Operating Plant I&C upgrade market. The issues for an operating plant are different than those for a new plant. The AP1000 overall safety system design simplicity along with the new plant design flexibility results in these significant differences. Thank you.

CHAIRMAN KLEIN: Thank you.

MR. BOWE: Good afternoon. Thank you for having me. My name is Tom Bowe. I'm the Executive Director for Reliability Integration at PJM. Though I have that particular role now, my comments are really coming from three previous assignments I've had at PJM; one being the Manager of Real Time Operations for four years, then a subsequent temporary assignment to NERC and the Bi-National Investigation for the August 14th, 2003 Blackout, where I was the root cause team lead, and then lastly my previous assignment as PJM's Chief Security Officer.

I really see the purpose of my presentation is to talk to you about how PJM as a great operator has been employing digital I&C in real time grid operations. To that point, may I have the second slide, PJM'S Mission.

PJM's mission is all about reliability, but it's also about safety and as our CEO often times likes to point out, the reason safety is in our mission statement is because of our close relationship with the nuclear plants within our footprint. That relationship is maintained in a number of forums, whether they be user group

forums, operator training and as well the development enhancement of various protocols. May I have the next slide, please?

For those not familiar with PJM, our footprint extends from Chicago roughly to Newark and down to North Carolina where we serve approximately 51 million people with 1,400 generators and available capacity of some 170,000 megawatts.

If you just look at PJM some four years ago, we were a third the size. So we've clearly grown in our capabilities. We've clearly grown in the complexity of operations and one of the reasons we've been able to do that is the way in which we've leveraged I&C technologies. Next slide.

If of that 170,000 megawatts of installed capacity, 25% is roughly from our nuclear fleet. The operator who maintains load generation balance minute to minute of every day is represented in this next slide. Before that Operator is a wide array of visualization. Nine years ago when I went into this control room for the first time it was all analog, very hard and fixed, not flexible, not adaptive to system conditions.

If we were to manage the greater complexity that we do manage today with the same analog technology in front of the operator, we would not have the flexibility needed to respond to the everyday changes within system operations. I'd also like to note that the preponderance of those displays were as well designed and built by the operators themselves. The next slide, please.

We go from generation operations to transmission operations. The slide before you represents the map board in front of the operators. It's merely a

reflection of the tens of thousands of data points that we receive from our members every two to four seconds. We utilize that data to estimate the system and how those conditions are changing minute to minute. We do contingency analysis on thousands of lines and facilities every two minutes and we're always operating the system for that next failure.

So we really do survive on the information that we receive from our members and as well that we exchange with our members. And on that note, I'd like to go to our next slide, backup capability.

If information is so important to us and digital control and instrumentation are so important, how do we make sure that in spite of problems we can maintain reliability and safety on the grid at all times? And that's with detailed backup procedures.

Y2K: a lot of people saw it was a waste of time. It was anything but. Our planning for Y2K and our plans to say what happens if we don't have any digital visibility, how will we see the grid and how will we manage? We completed those plans. Y2K was of course a sleeper for all of us. But then on August 14th, the actual plans that my operators and I implemented within 15 minutes of the second plane hitting the tower was the Y2K plan.

We dusted it off. We implemented it. We made the system far more stable to respond to the loss of any Max Cred situation, Max Credible Disturbance, and as well the loss of visibility to any of our key data points.

August 14th, 2003, the Northeast blackout, is a perfect example of when

entities lose situational awareness and haven't spent the time in training operators to be able to respond to crises that may occur. Since we do exist on our data, we're always ensuring that we have multiple data streams. Physically you can see that just in how the asphalt is torn up all around our facility. It's coming in from different physical methods. It's as well coming in from different carriers. We always can ensure that we have multiple ways of getting our data into our primary and our backup facilities.

And as I spoke to the greater flexibility that digital I&C provides, based on system conditions we can adapt to what our operators are looking at so they do have that greater situational awareness of what is actually before them. The training that we spend with our operators one week out of six, so that they can respond to whatever we throw at them, whether it be the loss of a particular system, a particular contingency that may occur, operators are always thinking and ready to respond to the unknown. Next slide, please.

I speak to the importance of open and flexible architecture and the value of that to operations. On the other side of that continuum is if it's open, how secure is it? In contrast to maybe a nuclear plant where potentially you could isolate the data streams within it, just by the very nature of grid operations, we're always exchanging information with our neighbors, with our members, whether they be transmission operators or generation owners, so we have to keep our systems very open. So cyber security becomes critically important.

The industry after the 2003 blackout really took up the charge to create a

base line set of standards, which we call CIP or Critical Infrastructure Protection Standards, 002 to 009. These are now – they haven't been yet approved by FERC but shortly may be approved such that they're mandatory and enforceable for the entire industry.

What they say is first you need to identify the facilities that are most critical to you. What do you really need to keep the system reliable? And based on that, what of those critical facilities actually have cyber linkages? And then based on that, here are the standards that you need to be able to protect them from a physical standpoint, from a cyber standpoint, and then what are you doing in terms of your business continuity planning to ensure that for the loss of that facility you can quickly adapt?

So those standards have really been a nice benchmark, but that's it. They're just a benchmark that hopefully every entity will continue to push beyond. Next slide, please.

Grid operations will only become more complex as load grows, as transmission lines do or do not get built, and in our case we plan on having them built. But with greater complexity on the system, we need to be able to have the systems in place such that our operators are very capable of adapting to the situation.

One of the things that PJM is doing is standing up a second, full-time advance Control Center so that instead of just merely having a primary site and a backup site, we're going to have two control centers continually synchronized with

one another with different data streams coming in, but capable of accomplishing our mission minute to minute. With that, that concludes my presentation.

CHAIRMAN KLEIN: Thank you.

MR. DEZFULI: Good afternoon. My name is Homayoon Dezfuli, Systems Safety Manager, Office of Safety and Mission Assurance at NASA Headquarters. Thank you for the opportunity to address the Commission concerning safety and reliability challenges we are having at NASA related to use of computing systems.

At NASA, we have begun using the term "computing subsystem" to refer to “digital subsystems”. The computer subsystem includes computer hardware, complex electronics, firmware, and software. Next chart, please.

Computing subsystems are key elements of a space system. They're used in both robotic and human space missions to perform safety critical and mission critical functions that include power management, telemetry, data and information handling, communication, hardware automation and control such as proportion and navigation control.

While they have played an increasingly important role in NASA's mission, they have their share of mishaps and have contributed to the following space accidents: Ariane 5 launchers in 1996; Delta III launchers 1998; Titan IV upper stage failure 1999; Mars Climate Orbiter spacecraft, that was a NASA mission in 1999; North Poler Lander spacecraft in 1999; DART spacecraft, very recently in 2005; and lastly Mars Global Surveyor 2006.

The investigative reports for these accidents identified software related issues as primarily or critically contributing proximate causes for these accidents. In the case of Titan IV and Mars Climate Orbiter, there was software data specification and entry errors. For Ariane 5, Delta III, North Polar Lander, DART and Mars Global Surveyor they were software design errors. So naturally software aspects of computer subsystems are receiving more attention at NASA and this is why I will be focusing on that topic in the remaining part of my presentation. Next chart, please.

NASA is pursuing a multi-prong approach to deal with the safety challenges associated with using computing subsystem information. The increasing functionality of the computing subsystem in particular their software elements demand sound system engineering and integration approaches. Software often is only way to meet functionally and weight constraints of the space systems.

An effective system engineering approach would insure on one hand the critical subsystem functions are supported by sufficient level of failure tolerance, and on the other hand that the unnecessary complexity and functionality and a “creeping featurism” in the software design of safety and mission critical functions do not occur. This in turn should reduce the likelihood of software design errors, the reported cause of 5 space system accidents.

NASA is actively improving its system engineering processes where simulation based and holistic evaluation of the hardware, software and human interaction are being promoted.

The second component of this approach is continued reliance on the software process and product assurance as well as test and traditional V&V, verification and validation processes.

Focused and integrated testing of the flight software functionality during transient phenomenon is essential. The software assurance processes have been effective when focused on analyzing early life cycle processes and products. They have been effective in preventing software errors and can be effective in reducing the likelihood of the data entry errors, the cause of two accidents, one NASA and one DOD, which both occurred in the 1990's during the so-called faster, better, cheaper days of NASA.

The third aspect of our approach is applying risk assessment techniques to inform the system engineering assurance process which I mentioned above. With respect to these activities, I have to say that we are still in exploratory stages. Next chart, please.

NASA has sponsored several research projects in the area of software risk assessment. It is important not to lose sight of the key objectives of these research activities which are to develop practical and definitive models to prioritize risk scenarios and evaluate or bound with some confidence the likelihood of mission failures due to latent software errors.

These evaluation models are intended to be used for risk informing the following system engineering assurance processes: risk management decisions such as doing design trade studies, prioritizing testing regimes, and for risk

acceptability decisions such as showing that the probabilistic safety requirement has been met.

The evaluation problem I stated above is inherently a very difficult one. A key aspect of our challenge is to essentially model potential design faults. I might add that software latent defects are not static as development and testing proceeds. Stated differently, we have significant uncertainty in the definition of the success criteria and the boundary conditions for software functionality.

At this time, based on research results to date, we think that a combination of the technique is needed and should be developed to handle this difficult problem. Last chart.

Research and experimentation with several techniques is ongoing with the objective of converging toward practical modeling techniques in support of risk-management and risk acceptability decisions. With respect to risk management decisions, we are exploring the application of a scenario based accident modeling techniques to identify mission critical configuration, flight mode changes, and flight transients. This information would then be used to prioritize computing subsystems testing processes.

As to supporting risk acceptability decisions, we are exploring methods that would impose an initial limit on the software reliability claims based on a scheme that takes into account attributes such as code complexity, software quality and V&V process considerations. This reliability claim would be modified as V&V and risk informing testing and other performance data becomes available.

I want to underline and emphasize one important point that we are still exploring the feasibility and technical merits of these methods. NASA remains interested and cooperation with NRC and it's research office in all above areas as well as other possible areas of common interest related to safety and reliability of computing subsystems. This concludes my presentation. Thank you for the opportunity to appear before you.

CHAIRMAN KLEIN: Thank you very much. Just a clarifying question on the space ships that go up. Do you have a lot of digital I&C on those, like on the shuttles?

MR. DEZFULI: Yes. Yes, indeed. We're going to be having a lot more in the new generation of the space crafts.

CHAIRMAN KLEIN: Great. Thank you very much for a very helpful presentation. Obviously, digital I&C is certainly of interest to us and we'll start our questioning with Commissioner Lyons.

COMMISSIONER LYONS: Thank you, Mr. Chairman and thanks to Commissioner Jaczko for suggesting that I perhaps I take the lead in the questioning. I have been very interested in the digital I&C, but I think that's fair to say that the entire Commission has also been extremely interested in the opportunities that digital I&C offers to still further enhance safety and certainly it's also an area that we simply have to be moving into as we're well beyond the days when the analog instrumentation continues to make sense.

I found it particularly striking as I've traveled overseas on some occasions

to see the extent of digital I&C in a number of other countries. I just returned late last night from Lithuania, Bulgaria and Romania. At least in two of those three countries, which certainly are relatively small nations, I was extraordinarily impressed with the quality and the capability of the digital I&C, particularly at Cernavoda and Ignalina. Just very, very impressive digital I&C systems and I honestly hadn't anticipated seeing that.

So, in some sense I think the U.S. is a bit behind the power curve on this and certainly I think we're very, very interested in catching up. I do very much appreciate all the presentations. There were very, very interesting.

By way of a first question, I would certainly go to Amir, but I'm guessing that a number of you may want to comment on it. I've been interested as the NRC moves ahead with our various guides and regulations, whether we are enabling the right amount or whether we're providing the right degree of detail in our specifications and requirements without losing the flexibility that I am anticipating that all of you are going to need for technology that's changing rapidly. I'm trying to understand a trade-off between the detail that we provide and the flexibility that I believe you're going to need.

I was curious, Amir, and then others if you would comment on whether you see that the current process that's going on between the NRC and industry as moving appropriately to provide that balance.

MR. SHAHKARAMI: I'll start by discussing some of the deliverables that we have put in place. I don't know if you had an opportunity to look at the

project plan for the six working groups. I think that puts the foundation of really what is the problem. What is it that we're trying to solve? I think we all align on a statement of what is it that you're after. That's settled.

The difficulty is because of timing we put some interim guidance in place almost in every one of those task groups and I think even though that's going to help the first wave of resolving some of the issues, I don't think it's going to address the long-term outcome as you have witnessed overseas of really how can we use the optimized configuration of digital I&C.

What I have seen between the working groups, definitely a lot of collaboration. We're getting EPRI involved to do a lot of technical papers as well as the research. I think it's doable. I think we can provide that flexibility. What worries me the most is establishing – again, I've said that in my presentation – an arbitrary date to get to the outcome rather than understanding the scope of the outcome and then let that drive it to provide the required flexibility to go through.

Once you put the box around something and say you want it, I think you're going to get a much tougher requirement, rather than plan to work, work the plan. I think that's where I see we are at this time.

COMMISSIONER LYONS: How about others? Chuck?

MR. WELTY: From our perspective, the process and at least the concept of what we're trying to do through the industry task working groups and the developing of the plan should get us to the point of having the flexibility. Until we see the plans completed and see that in fact we're getting the proper review

and input and getting the ultimate output from the next step beyond the interim guidance positions, I don't know that we can fully answer that question.

I'm aligned with what Amir was saying. We're working very closely together to try and work with the staff to in fact arrive at adequately flexible solutions to the various issues.

MR. SHAHKARAMI: Let me just add the emphasis we put on five out of six task groups is merely technical. Is it defense and diversity, is it communication. We have not spent enough time on the licensing aspect, which provides the vehicle of that flexibility, so I think that's one of the groups we may have to put more focus on.

COMMISSIONER LYONS: Ken, do you or others want to comment?

MR. BROWN: I'll add just a little bit. There is a fairly good amount of dialogue that's taking place right now with the current activities. I might present your question a little bit differently on the very long term considering how long these facilities will be running and with the digital world and the transitions that will take place over the next 20 to 30 years.

That's a set of discussions premature to have right now, but I think that needs to start building into both all the stakeholders in terms of how we address the long term and obsolescence as well as the acceptance to a new generation that will come on to make things even safer. It's premature to talk the real long-term, but it's something I think that needs to be into the scope of discussions long term.

COMMISSIONER LYONS: I appreciate that. Did you want to comment, Cindy?

MS. McGINNIS: No comment, thank you.

MR. BOWE: I have a comment. Though I can't comment on the process and how the process is moving along, one of the points I would like to make is when it comes to cyber security, I know one of the things the Federal Energy Regulatory Commission is struggling with these new CIP standards is there's a great deal of management discretion written into them.

How do you make a mandatory and enforceable standard when you have management discretion? But at the same time if you were to hard wire a solution for a particular threat, no sooner have you hard wired the solution and the threat is evolved to overcome that particular solution. So as your process moves forward, I would urge that in looking at the cyber security piece that it does have to be written with a great deal of flexibility, such that operators could assess the threat, show that perspective assessment and then evolve their current practices to address that ever evolving threat.

It's not physics that we're dealing with, but you always come to probably the same answer. You're dealing with a threat with an incredible number of unknowns.

MR. DEZFULI: The comment I have about the flexibility, I think at NASA when we are asking vendors to come up with – basically, we tell them this a mission we want. We want to go to the moon and stay a few days and come back,

come up with your best shot. They are going to come basically with the mission. What we want them to do here is to somehow tell us what is the risk associated with that mission.

In the past, basically software or the digital system would get a free ride. Now we're saying "no way" because we have seen the past that it was a contributor to accidents and you really didn't have to show us that risk is negligible. You've got to follow some processes and NASA has established some processes to follow these processes and come back and tell us whether you're meeting those probabilistic goals. In other words, it has to be a safety case, essentially, for it.

COMMISSIONER LYONS: I have many questions, but my time is up. I hope we have another round.

CHAIRMAN KLEIN: Commissioner Jaczko?

COMMISSIONER JACZKO: I guess I have several questions. First of all, I guess I would say we had a meeting on this a couple months ago - I don't remember how long it was – I heard a lot of allusions to issues to concerns. Maybe Chuck and Amir, you could go through what specifically are the areas where you see issues at this point?

Again, right now I think reading the slides I get the impression that everything is moving along fairly well, which maybe is true, but I would just hate in a month or so to hear that there are substantial areas of disagreement.

MR. SHAHKARAMI: I think, as I said, good progress has been made and a lot of it is because Mr. Grobe's leadership in the sitting committee and

myself leading the industry talking not just when we meet face-to-face, but on the phone to really drive a lot of issues. I would say not understanding what it takes to resolve all the issues we have put on the table from a resources perspective, I don't have a good feel for it. I don't think we have populated every one of those deliverables of who's going to do it, when it's going to be done, and what it takes to do it. I think definitely that's one area that is a concern of mine.

COMMISSIONER JACZKO: What I'm trying to get at – what are those fundamental underlying issues? Are there some specific – if there were three things that you had to name that you foresee areas and challenges and resolving them., where there is disagreement right now?

MR. SHAHKARAMI: In a technical area are you talking about?

COMMISSIONER JACZKO: Yes, absolutely.

MR. SHAHKARAMI: I would say definitely diversity and defense-in-depth is an issue that we just cannot apply the way we apply it to analog. We need to change our paradigm and then deal with that. That's definitely an area that are different opinions on how you want to approach it. I would say that the lack of focus – at one time we actually talked about not pursuing the licensing aspect of digital I&C and that's back again. I think we haven't put enough focus on that.

That would be the second area that I think becomes instrumental for the utility to follow through with understanding what it takes to license one of these systems.

COMMISSIONER JACZKO: On defense-in-depth, going back to that one, we have an draft interim guidance on defense-in-depth, which looks at essentially 30 minutes seems to be the time of concern. Where are the disagreements? Where do you see the concerns with that approach on defense-in depth?

MR. SHAHKARAMI: I think the question about manual action, Operator action. I think there was some questions in that area. I think one of the areas that we started earlier is how long you're going to let it decide for you. When you have to stop and intervent and make sure you're on the right path? Those are really the key areas I would say in that. Others may be able to add more to it.

COMMISSIONER JACZKO: Chuck, you did say in your slides "interim staff guidance documents are only a start. Our advisers expect to continue to work with NRC to resolve the issues completely". What are the issues that our out there?

MR. WELTY: The first one is defense; diversity and defense-in-depth. We are concerned that perhaps the interim guidance came out too soon before it had completely been reviewed but we're working with the staff on that.

COMMISSIONER JACZKO: What are your concerns with the interim staff guidance right now?

MR. WELTY: Can I ask one of the people that I work with?

COMMISSIONER JACZKO: Absolutely.

MR. TOROK: My name is Ray Torok. I'm with the Electric Power Research Institute. You asked specifically about this 30 minute criteria and I guess the concern here is that any time you come out with new guidance or revise old guidance in such a way that it's specific and deterministic, it's very difficult to anticipate all of the side effects that you might get into, all the nuances that might turn out to become important.

COMMISSIONER JACZKO: That 30 minutes may not be the right window?

MR. TOROK: Thirty minutes in particular, once that came out there are all kinds of questions raised in regard to previous regulatory precedents that may be contrary to this one, for example, or may conflict with it. To the effect that beyond design basis event of common cause failure would actually have more stringent requirements in regard to operator action times than some design basis events where they credit shorter operator action times.

This is not something that can't be resolved, but it became a lot more confusing than originally anticipated, let's put it that way.

In regard to more on the technical side of this, there were concerns that when you have a specific deterministic criterion like this one, like 30 minutes, it can have an adverse effect in that it can actually shift the focus away from safety. In this case, the 30 minute criterion draws more attention to very rare events that are very low contributors to plant risk as opposed to higher frequency anticipated operational occurrences, for example. There's always that kind of concern as well.

COMMISSIONER JACZKO: I appreciate that. As I said, I was certainly hopeful to hear more about the specific issues so that we can try and begin to work through these and get them resolved. I appreciate you filling me in on some of the more details. I know I don't have any more time.

I would just say if we do have another round, I certainly have some questions on the tail end of your statement about how we're incorporating some of these things from a risk perspective. So perhaps we'll have another chance to do that or if not, I'll ask the staff.

CHAIRMAN KLEIN: A question initially for Ken. If you look at what industry and what country do you think is the leading edge on Digital I&C?

MR. BROWN: That's a fairly broad question, looking at all the industries we serve. I think I would hold off and get back to you on that particular question. There's some specific ramifications in how it gets answered. Remember, I do not pick out – I'll get a phone call when I get back to my office -- I need to be careful about that.

I would say, clearly in certain areas the Europeans in the broader aspects, the Europeans have done an excellent job in terms of risk and risk assessment and implementing digital I&C consistently across the broader community. There are standards that drive that discussion at a different level than what generally is happening in United States and in some areas of the United States we're catching up.

That's not in the nuclear industry but also in some of the other process

industries. Those standards are now becoming globalized. So in general, I would say that the Europeans have done a better job on some of the European regulations. Those cover a large number of industries. I wouldn't say it's a specific industry per se and if you'd like further clarification, I can get that to you.

CHAIRMAN KLEIN: I think what's important for the Commission is you always want to have who you look to to be cutting edge, who has implemented it well, and what are they doing that we should be following.

One of the questions that I have often times asked when I was on the INPO accrediting board is what utility do you strive to be like? Who's your role model? Who do you want to be like? Who's your mentor, so to speak, to look for? I think that's the question that is always good to ask is what industry is doing it right, what technologies are they using and how can we learn from that to do it better.

MR. BROWN: There's also another industry that's slightly separate from the process industry but has done quite well is in terms of the high-speed rail. If you look at similar issues in terms of speed of response and reliability, all digitized control, that's an area you don't often think about, but it's another area to look at.

And again, in certain areas European, because of their predominant use of high speed rail, has done a fairly good job at those regulations and getting them pervasive throughout the industry supplying them.

CHAIRMAN KLEIN: Chuck, a question for you is when I was in another previous position, electromagnetic field was a big concern for other assets

that the military has. What's EPRI doing to look at EMF protection against our plants?

MR. WELTY: I will have to get back to you on that. I don't have it. I don't know what the power delivery sector is doing in that area. To my knowledge, we're not doing anything right now. I will get back to you.

CHAIRMAN KLEIN: That's an area that as the technology changes we just have to be aware of what can the bad guys do that we would prefer them not to do so that our safety systems will always work.

Amir, a question for you. This is one I know you have an answer to. Obviously, I think our staff and the industry is working together to come up with a path forward. When you look at the four of us on this side of the table, what are the top two things you want the Commission to do to push I&C forward, digital I&C?

MR. SHAHKARAMI: I think your continued focus and bring us here once in awhile and get our insight about what we think is happening remains one of the crucial parts of our how successful we're going to be. Having an interim guidance is not the end. It's the beginning. I just hope your passion for what you've shown us stays because this is an important piece of what we're going to be doing. That definitely would be one. Your engagement going forward as it has been in the past to drive it.

The second topic, I would have a vehicle for you that you can actually see how we are making progress. And today we don't have that. We have it in a

piecemeal fashion, but again, I'll go back to my original discussion about integrated schedule planning. Some kind of indicator that you can look and actually see are we really making progress as you expect or not.

We can solve technical issues. You put it on the table, get the right people together, we're going to solve the technical issues. I have no doubt about that. There's more dedicating the right resources, right skill sets and become very efficient from a human perspective. We definitely don't want to do the research that EPRI is doing or has already been done in Europe for the third time. We need to be very efficient with our resources. That's what I've been driving so much about tell me what it takes to go do it and we go do it.

CHAIRMAN KLEIN: Thanks. Commissioner McGaffigan?

COMMISSIONER McGAFFIGAN: Mr. Chairman, I'm getting some cognitive dissidence today in looking back to the November meeting. I think there are different messages being sent as to how quickly we need to resolve things. The Westinghouse representative basically says you've got all you need and just judge us against that. I remember the representative from AREVA or whatever that group is going to do the EPR, they wanted something by this spring last fall so that they could design their simulators.

I'm hearing all sorts of cautions about the staff's interim guidance. Commissioner Jaczko brought up a very important issue; this issue of this plant being able to take a 30 minute hit before operator actions can come in. That would seem to advantage the ESBWR and the AP1000 because they're passive

and maybe they can do that. But as you point out, this is more than we do sometimes in design basis space.

Then I listened to the fellow from NASA and he talks about five or six accidents in the last decade that he can attribute to digital instrumentation control errors, which we can't afford five or six accidents with new plants that are catastrophic. His things are flying in space and there's no 30 minutes issue or five minute issue or 10 minute issue. If they are headed to the wrong place, that's the end of the mission.

It strikes me that this diversity and defense-in-depth issue that we talked about last November that I think is central today is still central. You have some skeptics. I know nothing about this area. I'm a previous generation person, I still do everything in writing. I hate computers. I don't carry one of those BlackBerrys.

There are several messages that aren't quite clicking for me at this point. In the Commission, you can blame us. I think in one of our recent SRMs we said we'd like to see this interim guidance because of issues raised by – the staff basically said we'll deal with ACRS issues later and we'll just do interim guidance in the meantime.

We gave an SRMs and said we would sort of like to see something by the end September, I think it was -- that’s September of this year, in interim guidance. That's less than 60 days away and nothing much happens in bureaucracies and working groups and all those things that we're talking about in 60 days. So I suspect that 30 minutes is going to be in an interim guidance. Tell me why I

shouldn't be as confused as I am? Anyone?

MR. SHAHKARAMI: I heard that statement from Westinghouse in respect to the current NUREG and BTPs we have in place will give me enough guidance to make this a success. I'm not there yet. I would say I'm more with AREVA needing a clear approach to how I'm going to design a system and bring it to you. So I think the staff has acknowledged that definitely something needs to be done differently from what –

COMMISSIONER McGAFFIGAN: That was last November.

MR. SHAHKARAMI: That's right. I think we're working toward those. I had this in my presentation putting a date out there and saying you're going to issue this with that date may not be as appropriate as do we fully understand the scope –

COMMISSIONER McGAFFIGAN: NEI would have contacted us if we had put down September 30, 2010 and said in the interim will deal with COLs in some mystery faction. I think we probably would've gotten a letter from the Admiral or something at that point. You can't have it both ways.

We're going to start receiving COL applications. We received half a COL application just on the environmental side, I think the other day from AREVA for Calvert Cliffs. Everybody's telling us there's a tidal wave coming in this fall and we sort of have to be able to do it.

MR. SHAHKARAMI: We discussed that. There is an exception taken that for the first wave of reactors, we may have to put a more stringent

requirement because of timing so we can go on and get those things through and process them. I don't think that's going to address the long term vision that we have for the use of digital I&C. Industry can support that.

The reason I set a date that we need to meet – we need to prioritize to see which one of those is really something we need to do by September or December rather than saying all these things are needed by September. That was my take to fully understand what's needed today so we can focus.

We can't focus on everything at the same time. I don't think we have the resources to do it. I think we can systematically identify what are the real things by September. We will deliver that to you.

COMMISSIONER McGAFFIGAN: All I can say is I think you should expect conservatism on the first application and maybe in 2015 or something all these other issues will be solved. I can't imagine my colleagues and the staff not being conservative on the first applications.

CHAIRMAN KLEIN: Let me just give you a caution about a first wave, standardization. We have 104 reactors, about 104 different ones. We don't want to go down that path again.

MR. SHAHKARAMI: We don’t, I agree with you.

CHAIRMAN KLEIN: Commissioner Lyons? Round Two.

COMMISSIONER LYONS: Part of me wants to follow-up on the same direction that Commissioner McGaffigan was just going because I'm somewhat puzzled too, Amir, in that I thought we heard previously about the need

to really push forward and get interim standards out there and now I'm kind of hearing the other. But I'm not going to go down that path, as interested as I am because there's too many other things that interest me.

A question for Tom and Homayoon. We talk a lot at this table about diversity and defense-in-depth. If I understood correctly in both of your presentations, there were many elements of defense-in-depth in terms of redundant systems. What I didn't hear was diversity.

I'm curious if in your fields of focus you worry about things like common mode failure by having simply multiple redundant systems, whereas I've been hearing from our industry and I guess getting trained to think not only of defense-in-depth, but also of diversity based on a concern about a common mode failure. I hope I've said that well enough. Where is common mode failure in your thinking?

MR. DEZFULI: Let me address first the design of the space shuttle. We haven't had any accident related to the software in human space flight. I don't know to what we can attribute that. I would say that the computer system and the shuttle they have five boxes. They have five general purpose computers. Interestingly, four of them have one software loaded on them. The other one is completely a different software. Basically, the four sets of computers that are operated using one software are redundant. In other words, if one goes out basically it will void it out and we have three remaining.

If you're losing all of the four because of some commonality in the software error, then the crew has an ability to basically switch to the so-called backup

computer that has a different software system. From that point of view, I believe the design of the shuttle introduces diversity to deal with the software unknown. But if you're going to be doing that for new generation of space craft we're still designing, we don't know, but I think that's something of interest.

COMMISSIONER LYONS: I appreciate that. I hadn't realized you had that diversity.

MR. DEZFULI: We use diversity with respect to the software in the design of the shuttle. They have a lot of redundancy for the computer boxes, but software diversity.

MR. BOWE: I won't talk in great detail about our cyber security, but from a defense-in-depth perspective, if you layer different vendors' applications in that defense-in-depth such that if an attacker exploits the vulnerability of one vendor, you will probably within that defense have the next vendor that doesn't have that same vulnerability thereby providing you those multiple layers of defense such that we have diversity through the wonders of competition of vendors coming to us and saying this is the strength of our application and this is where it should be and by layering those, almost like a patchwork, you don't see a common failure going down through your network into you most critical systems.

COMMISSIONER LYONS: So in your case, too, there's a focus on both in defense-in-depth and diversity?

MR. BOWE: I don't find diversity as much as being a priority as the defense-in-depth, but when we do look at vendors in terms of our energy

management system and our market systems and things of that nature, we look at do we want to have everything from one vendor or do we want to have multiple vendors. The final decision is based on not diversity but on the quality of the product in terms of providing us that real time view of the world. But it is a small consideration in our assessment.

COMMISSIONER LYONS: I could go on, sir, but out of time.

CHAIRMAN KLEIN: Commissioner Jaczko?

COMMISSIONER JACZKO: I left off with a brief comment about some of these risk informed ideas. I probably won't ask a question and just make a comment on that. We had an interesting discussion, I think with ACRS recently where we talked about the ideas of doing modeling with digital I&C systems and there's some inherent limitations of doing risk based work with that given that these are design errors and not necessarily probabilistic failures.

If you have a design fault, you have a design fault. Every time you execute whatever set of conditions gives you that fault, you get that fault. And then also hearing what I heard from Mr. Dezfuli about NASA’s very early stages of trying to do this or in exploratory phases of trying to do this in a risk informed way, I get a little skeptical when I hear comments that we're risk informing this and we're looking at these things from a risk informed way. I just say that I'm somewhat skeptical of hearing those comments.

The one thing that I did hear that seems to be new to me, and again I think comes from the experience that NASA has had is your comments, Mr. Dezfuli,

about – ultimately, you found that software seems to be the problem, guess more than hardware. I guess I would ask Amir or Chuck or anyone else or Cynthia on the nuclear side, is the focus of what we're doing more hardware, looking at diversity and defense-in-depth from a hardware perspective or is it looking at the software aspects or is it really both?

MR. SHAHKARAMI: I think it's a combination. We haven't really had a lot of safety related digital I&C implementation. There have been a few, but when I look back on all the operating experience, the majority of problems has been on the software side more than the hardware.

COMMISSIONER JACZKO: So from all these issues of defense-in-depth and diversity, the diversity and defense-in-depth I guess if there's any risk information or any information we could take from NASA's experience is that if we're going to prioritize resources that we certainly want to make sure we're looking at software failure?

MR. SHAHKARAMI: As I said, just based on my own experience of the event that I have seen on known safety related application, we had some kind of template that wasn't loaded right and when it goes to pick it up it doesn't pick it up; it trips. We've seen a lot of that.

In respect to the hardware, I don't think there's any difference from what we have today. We have a composite on a card that is not functioning. It takes it out. I think the digital system becomes a question of how would you go about programming and building the redundancy within a program. I would say from my

perspective it's more on the software than hardware.

MR. WELTY: I'd say go to Ray – is that correct. He's the expert on this area.

MR. TOROK: Ray Torok, again, from EPRI. We're looking at a number of operating event reports from both NRC and from Institute of Nuclear Power Operations. I think it's going to turn out to be upwards of 500 events that are associated in some way with digital systems and we're looking at them from a number of different ways.

One is, is it a hardware failure or software failure? Was it a hard system failure? Did it really result from a coding error or was it a requirement specification error, which may be much more common actually. A lot of things that are called software bugs are really requirements problems. So we're looking at those kinds of things.

Was it a logic error, for example? The other thing we're looking at is what kinds of defensive measure is built into the software, for example, would have been effective in avoiding it or what kinds of diversity attributes might have been affected. We're looking at all those things.

I would say the emphasis is probably more on software and what we called digital system failures than on hardware because these new redundant hardware systems like the Triconex TMR system that was described are very robust in regard to hardware.

COMMISSIONER JACZKO: Thank you.

MS. McGINNIS: Commissioner, I'd like to ask one of my colleagues to comment, please.

COMMISSIONER JACZKO: Sure.

MR. COOK: Hello, my name is Bruce Cook. I'm a consulting engineer with Westinghouse. I guess I would like to underscore and reiterate what Mr. Torok has said. The focus has been on software because it was the unknown, but what we've learned is that it's really pushing us back to look at the design process. It's errors in the design process that are being turned up whether it was requirements errors or other mistakes.

COMMISSIONER JACZKO: I hate to be naive on this, but what is a requirement error? Is that too much memory needed or something like that?

MR. COOK: It could be that the specification was incomplete.

COMMISSIONER JACZKO: That still doesn't help me.

MR. SHAHKARAMI: Let me give you a quick example. We have full filtration system and it's all digitized. When you put it in a latent design, that means you're working on a piece, now you’re in an area that is latent; it is sitting there. The program was supposed to put the valves in a safe position and it didn't. So the specification did not outline the actual logic and process. I think what you're talking about is even deeper than that.

MR. COOK: The specification may consider one plant operating mode and not give enough consideration to what happens when the plant is shutdown. Those kind of errors can be built into the system if they're followed

blindly.

COMMISSIONER JACZKO: Okay. Thank you. Thank you, Mr. Chairman.

CHAIRMAN KLEIN: I guess I'll follow on a question that's been raised earlier. The last time we had a digital I&C meeting it seemed like there was a sense of panic that digital I&C was on a critical path. You needed to order simulators and so decisions had to be made in a very timely manner. I guess from what I am sensing now, have we solved the schedule problem? Are we on the right schedule?

MR. SHAHKARAMI: I just want to go back to what I said. By no means did I say there is no sense of urgency. There is a sense of urgency. What our caution was we need to evaluate putting a date and try to put a document out there in all cases is it the right way to do it. We can prioritize. We can understand what is it that we want by some day. We can deliver that. Globally, I'm not just in a position to say let's just issue interim guidance for everything.

In the diversity and defense-in-depth, definitely. That's the critical issue. We have to have a position there. The only reason we do interim guidance is because we don't feel we'll be able to produce the final product in a timely manner to support some of the activities, again, by itself as an interim guidance. We support that.

I think there is a sense of urgency. A lot of it is coming because of training, like you said. It's building a simulator, training the trainers and then training the

staff. You put that together, we're definitely on a critical path.

My statement was more let's not put an arbitrary date and then say we're going to march through to make it happen and have questions about side effects of 30 minutes or manual action and other things.

CHAIRMAN KLEIN: I've oftentimes warned my staffs in various positions I've had. Sometimes we don't have time to do it right, but we have time to do it over.

MR. SHAHKARAMI: This would be the case.

CHAIRMAN KLEIN: It is good to do it right. Commissioner McGaffigan?

COMMISSIONER McGAFFIGAN: Thank you, Mr. Chairman. I may be too influenced by the latest *Die Hard* movie where a neglected person who knew all the vulnerabilities and was working for the government goes basically and attacks the United States. My knowledge of digital instrumentation and control is about the same as the cop who takes down planes this time rather than just helicopters.

It strikes me that we're going to end up with something here that is, as I said earlier, very conservative. One of the things you all said, and I forget which one, maybe it was Chuck, that this doesn't contribute much to PRAs. Is that because you're going to have this wonderful digital system that the operators are going to have in the control room and it's going to wow us all, but if it goes out there's some good old analog control panels somewhere where they can bring the

reactors safely down and not affect the world? I'm not naive. What is the backup?

MR. WELTY: I will ask my colleague Ken Canavan. He is the risk expert.

MR. CANAVAN: I'm Ken Canavan from EPRI. I think the primary reason why it doesn't contribute that significantly to risk is the fact that the operating hardware of the plant is less reliable than the extremely reliable either analog or digital I&C systems. There also is a significant amount of diversity and redundancy built in.

COMMISSIONER McGAFFIGAN: I'm not a digital expert, but can't you get a catastrophic failure of the digital technology? When you guys talk about defense-in-depth is there going to be a backup? Every reactor we have today we have backup panels where people can go and deal with the event as its emerging. In our emergency exercises oftentimes they're necessary.

MR. CANAVAN: I think there is the possibility, although extremely remote, for very rare common cause failures of digital systems to take out large parts of the system and in that case operators and operator training can operate the systems. That is sort of the juxt of the 30 minute rule.

The only thing I would caution on in that particular case is that here we have a 30 minute rule where there's if you have more than 30 minutes operators can take action. Most of those scenarios are scenarios that involve normal operating expected transience where you have a lot of time. In that case, we would not put in a diverse system.

There's been some discussions of a diverse system for the case where we have very short-term operating transience, maybe like ATWAS or a large LOCA. In those cases we put in a redundant system. If you look at the combined probabilities at the very low frequency event, ATWAS or LOCA, combined with the very low frequency event of catastrophic failure of the digital system combined with the fact that operators could indeed act within a certain amount of time, maybe less than 30, maybe not with the highest probability, we need to combine those three things and then the diverse system would take over.

Well, putting in the diverse system operates on a very small part of the reliability equation, but it also introduces the possibility of spurious actuations and producing more frequent events, such as the normal operating transience. That's the other part of the risk equation. There's the risk reduction part and then there's the risk increase part.

COMMISSIONER McGAFFIGAN: I'm glad my fellow Commissioners look as confused me.

COMMISSIONER LYONS: Put me down as confused, too.

COMMISSIONER McGAFFIGAN: Our time is probably – we have to get to the staff.

CHAIRMAN KLEIN: Thank you very much for your participation and helping educate all of us on digital I&C issues. I'm sure this will not be the last meeting we have on it. We will follow Amir’s suggestion and periodically do this. This is an area where all the Commissioners have a very strong interest and we

do need to move forward on the science and how we can do things better.

I have seen a lot of new applications. If you look at the simulators that pilots have today and you look at the controls for the new Navy submarine fleets, clearly we're going digital I&C. That's the way the technology is, analog systems are not available anymore. So we need to go that way, but we need to do it right. So we appreciate your participation and we look forward to future meetings.

CHAIRMAN KLEIN: Now we get more education on digital I&C. It's nice to see Rick here. It's nice to see there's life after serving on a Commissioner's staff. So, we look forward to hearing from the staff, where we are and where we're going on digital I&C. Luis?

MR. REYES: Good afternoon, Chairman and Commissioners. The staff is ready to brief the Commission and update you on where we are with Digital Instrumentation and Control. Can I have slide number three, please?

Just briefly the agenda. Bill Borchardt, the Director of the Office of New Reactors will talk about readiness for new reactors. Rick Croteau, the Deputy Division Director of the Division of Fuel Engineering and Radiological Research, in the Office of Research, will talk to us about the platform research activities with digital I&C.

Jack Grobe, who during the day is the Associate Director in NRR, but part time is the Chairman of the Digital Instrumentation Steering Committee. He's

going to talk about the steering committee activities.

Mike Mayfield, the Division Director of Engineering in New Reactors is going to talk about your favorite topic defense-in-depth. And then Mark Cunningham, who was recently appointed Division Director for Risk Assessment and Nuclear Reactor Regulation will cover the integrated control room and the digital risk assessment.

Before I turn to Bill Borchardt I just want to emphasize one thing. We gave you a copy of the project plan. The industry referred to it. We do have a plan to deal with the issue at hand. It has deliverables, milestones and accountability. The staff is taking positions on all the issues that were being discussed earlier this morning. Some of those positions are not very popular, but in 30 years of doing this I think that we need to take a position and then have the different stakeholders give and take and work around to it. I see that as a big milestone, the fact that we have put a proposal on the table what we think it's necessary and then let's work around that and resolve the issue.

With regard to the speed or the criticality of getting decisions resolved, it's really the industry – it's an industry driver, as you heard from the simulators and the training. How quickly we resolve that or how quickly we not resolve that or come to an agreement may have an impact on the applications that are forthcoming. We'll talk about that during the presentation and the question. With that, Bill.

MR. BORCHARDT: Thank you. Please go to the slide on new

reactor licensing applications. This is a current picture of new reactor applications and the reviews by the staff. We last briefed the Commission in April of this year and our next Commission meeting on new reactors is scheduled for August 22nd. During that meeting, we'll focus all the time on the infrastructure rulemaking activities. So I'm just going to take a few minutes this afternoon to give you a very brief update.

The in-house work is progressing on schedule and we understand the COL applicants are likewise making good progress in finalizing their COL applications.

COMMISSIONER McGAFFIGAN: Could I ask one clarifying question? You're crediting UniStar with the Calvert Cliffs application. That's the complete application? You're showing March of next year, so you're not crediting the half –

MR. BORCHARDT: That's right. It's not a full application until it's a full application.

COMMISSIONER McGAFFIGAN: That's fine. I just want to make sure we all know what the rules were.

MR. BORCHARDT: Some of the publicly announced changes that are reflected on this chart include TXU, selecting the USA PWR design at the Comanche Peak site, Vogtle announcing that it is revising its Limited Work Authorization in order to match up with the revised LWA rule. Calvert Cliffs submitted the environmental reports portion of the COL application recently and Pennsylvania Power and Light has selected the EPR for the Susquehanna site.

Next slide, please.

Some of the infrastructure that is making good progress now. Part 52 revision has received OMB approval and will be published in the Federal Register soon. A Limited Work Authorization rulemaking is with OMB and will begin its review shortly. The final Reg Guide 1.206 on the COL application requirements was issued on June 20th after extensive stakeholder interaction. We think there's a very good understanding throughout the industry on the expectations for the application. Next slide, please.

We've completed the final wave of staff transfer from NRR. The Office of New Reactors is now at about 350 staff. It will continue to increase using the normal Human Resources personnel selection process.

COMMISSIONER McGAFFIGAN: Did you leave anybody behind for Jim?

MR. BORCHARDT: There's high-quality, sufficient number of staff in NRR.

COMMISSIONER JACZKO: If Jim were at the table –

MR. BORCHARDT: He would disagree completely. I think it was a very productive process that the two offices went through and we really appreciate NRR support and cooperation throughout the difficult situation.

We're populating the licensing program plan. If you remember, this is the software scheduling system for resource loading and scheduling for the reviews. That is being populated with standard review schedules and resources. We're

also going to be using it for continuing work on the Vogtle early site permit, the ESBWR activities that remain and the AP1000 amendment that you heard a couple seconds about earlier this afternoon.

The COL application acceptance review guidance is being revised. This is in response to the task force report and the Commission's SRM that authorized the staff to use a 60-day time period to do a far more thorough examination of the application. So we're coming up with specific guidance for the reviewers on how to do that application. We're very hopeful and I'm confident that that will result in a lot of efficiencies down the road throughout the review.

We'll identify where the application is weak and if we need to send it back, we'll send it back because once we start we want it to be a very firm, a rigid schedule that we'll meet. Next slide, please.

The staff has been fully engaged in a wide range of pre-application activities. These include on-site environmental and safety meetings, public outreach in the vicinity of the proposed sites, and using the design centered working groups to broadly discuss issues and guidance documents as they've been developed.

The international community remains very interested in NRC activities in new reactor area and those activities have been continuing through the Multinational Design Evaluation Program through bilaterals and through specific training activities that we have coming up next month with China.

We're also in the process of providing the design vendors with safeguards

information to help them do an assessment of their designs relating to aircraft. Rick Croteau will now continue the presentation.

MR. CROTEAU: Good afternoon, Chairman and Commissioners.

COMMISSIONER JACZKO: Mr. Chairman, I just have one quick question on the new reactor issue. Do you want to do these questions now?

CHAIRMAN KLEIN: If you want a clarifying one, we can do that now. Otherwise, I'd rather wait till we hear the whole thing.

COMMISSIONER JACZKO: Well, maybe I'll ask it. If it's a simple one, we can go on and I'll save it for later. I just have a question on ABWR. Does ABWR have a design center working group, since there's only one licensee right now?

MR. BORCHARDT: We're having the same kinds of interactions with them. I think officially, yes they do. That's my answer.

COMMISSIONER JACZKO: The question I have is I had some point got some information – the source of it I can't remember to be honest, that they were anticipating tier one changes to the certified ABWR design. Is that the staff's understanding right now?

MR. BORCHARDT: I'm not aware of any changes. I can check and we can get back to you.

COMMISSIONER JACZKO: If there were tier one changes, is that a significant departure from a certified design?

MR. BORCHARDT: It undoes the approval of the staff and opens up

for litigation of those changes. So they eliminate some of the benefit of the Part 52 process by doing that.

COMMISSIONER JACZKO: Okay. Thank you. That was the only question I had.

CHAIRMAN KLEIN: Rick?

MR. CROTEAU: Good afternoon. I'm here to provide an update to the Commission on our progress regarding integrated digital instrumentation and control and human machine interface test facility. This is on slide 10, please.

We are on track to conduct public workshops in September regarding conceptual approaches for a test facility. Additionally, we're not waiting until workshops to seek stakeholder input on this subject. We've been in contact with many internal and external stakeholders, including government agencies, vendors, National labs and universities in advance of the workshops. We'll be issuing a request for public comment in the Federal Register soon to seek public comment on the possible approaches, also. This will give us an additional opportunity to get a lot of stakeholder input before we have the meetings.

We're also conducting both site visits and phone interviews with a number of similar facilities in the communications, aerospace and process industries. The workshops themselves we're going to have a two-day public workshop on September 6th and 7th in Atlanta. That will discuss the technical issues.

Technical issues include: should the facility be reconfigurable? Should it be used as an advanced reactor training facility for staff and what technical

challenges have been experienced by other similar facilities?

In addition to the two-day workshop, we're going to have a one-day workshop on September 11th in the D.C. area to discuss the non-technical issues. Those include legal, budgetary and oversight aspects. Results of the workshop will be communicated to the Commission later this year in a paper. This will include the recommendations on a path forward for possible implementation of the facility.

I'd now like to turn the briefing over to Jack Grobe who will update the Commission on the staff's progress on regulatory infrastructure challenges associated with deployment of instrumentation and control at operating reactors, new reactors and fuel facilities. Jack?

MR. GROBE: Thank you, Rick. Slide 11, please. Good afternoon, Chairman and Commissioners. We are pleased to be able to update the Commission on the staff's progress in addressing regulatory infrastructure issues related to digital technology, including the activities of the Digital Instrumentation and Control Steering Committee and implementation status of the NRC's Digital Instrumentation and Control Project Plan.

The Steering Committee is monitoring staff implementation of the project plan. The staff and industry are on track to resolve the key technical and regulatory issues on a schedule that supports the industry and staff needs. Slide 12, please.

The staff last briefed the Commission on digital issues in November 2006.

Following that Commission briefing, Luis Reyes established the NRC's Digital Instrumentation and Control Steering Committee. I chair that committee. Also on the Steering Committee are senior executives from all of the affected program offices, including Mike Mayfield from New Reactors, Jennifer Uhle from Nuclear Regulatory Research, Joe Giitter from Nuclear Materials Safety and Safeguards and Scott Morris from Nuclear Security and Incident Response.

The committee is supported by the integrated effort of over 40 NRC staff and managers. The committee has several purposes. First, to interface with the industry, to facilitate consistent resolution of digital, technical and regulatory issues, to provide oversight and guidance to the NRC line organizations, and to assure timely resolution of any strategic or policy issues associated with further deployment of digital technology.

The Committee advises the Directors of the key program offices to assure consistent alignment of activities across the NRC and timely resolution of digital issues. Slide 13, please.

NRC staff has effectively used current guidance to review and approve the application of digital technology. As the technology continues to evolve and is applied more comprehensively in safety systems, NRC regulatory guidance needs clarification to maximize the efficiency and predictability of our licensing processes.

The Steering Committee has established a project plan describing a public approach for developing interim staff guidance that will be available to support

staff and industry near-term needs. In the longer term, the NRC'S regulatory infrastructure will be updated further refining and incorporating these interim positions into NUREGs, Regulatory Guides and the Standard Review Plan.

The industry is also committed to develop appropriate revisions to consensus standards for staff review. The Office of Information Services has provided excellent support to the Steering Committee, establishing a useful public website, providing key information and links to relevant resources.

The Steering Committee has integrated the efforts across the various NRC offices, maximizing the effectiveness of the agency's talent necessary to address the digital concerns. The Committee has also facilitated affected interface between the staff, the industry and other external stakeholders to address high priority issues in a timely manner, supporting staff and industry needs and to learn from and use relevant operating lessons and experience from domestic and international counterparts in a practical way.

The NRC staff has had extensive domestic and international interactions regarding digital technology over the past two decades. Further, since the last Commission briefing, the staff has expanded these interactions. Several examples include meeting with the Navy and participating in full-scale fire tests of fiber-optic cable, hosting an international symposium sponsored by the International Atomic Energy Agency on Digital Common Cause Failures and meeting with the staff from six other regulatory agencies to discuss diversity and defense-in-depth.

In addition, the Committee conducted one of its public meetings at the Westinghouse facility in Pennsylvania where they are developing the AP1000 digital control room simulator. Slide 14, please.

There are a number of near-term licensing activities involving digital technology regarding operating reactors. Oconee anticipates submitting an application in late 2007 to retrofit its reactor trip system and engineered safeguards actuation system with digital technology. This represents a more extensive application of digital technology than previously utilized at operating reactors.

Wolf Creek recently submitted an application to retrofit certain systems with digital controls utilizing field programmable gate arrays. This technology is a first of a kind application at operating reactors.

In addition, a vendor anticipates submitting a topical report regarding digital control system for use in safety related systems. Regarding new reactors, we have new reactor vendor topical reports under review today and we anticipate additional design certification and combined operating license applications later this year.

Regarding fuel facilities, General Electric and AREVA anticipate submitting license applications in 2007 and 2008 for enrichment facilities using digital technology. Each of these applications involves different technology applied in different ways and will benefit from a more predictable licensing process. Slide 15, please.

The Steering Committee interacted with the industry to understand the areas of greatest concern and identify jointly with the industry's six focus areas. The Committee established six task working groups in these areas. The task working groups are led by agency managers and staffed with over 40 agency experts. The industry has likewise established counterpart teams to interact with the NRC's task working groups.

Interactions with these industry counterparts has been very effective. The Steering Committee has approved the NRC'S Digital Instrumentation and Control Project Plan with near-term deliverables and deadlines for these six task working groups. The project plan is an effective tool to plan and monitor staff activities addressing digital technology. Mike Mayfield and Mark Cunningham will be providing you more detail on the specific technical issues being addressed by three of these task working groups. Slide 16, please.

The objectives of the project plan are based on direction from the Commission and from the Executive Director for Operations. The near-term objective of the project plan is to issue interim staff guidance to clarify staff positions on a time frame to support staff and industry needs, assuring a high level of predictability in the NRC staff reviews. The interim staff guidance approach has been successfully used in other aspects of NRC licensing activities such as license renewal and early site permits.

The longer term objective of the project plan is to complete additional technical development work further refining the interim guidance as appropriate

and incorporate that guidance into NRC'S existing regulatory framework using our standard revision processes. A significant amount of effort expended by the task working groups and the industry has led to a very clear definition of the issues or problem statements needing further refinement in NRC guidance. Development of interim guidance to address those issues is well under way.

We're on schedule to complete the interim guidance and will continue working with the industry to refine that guidance and revise our existing regulatory tools. Slide 17, please.

To develop the project plan, define the problem statements and begin developing the interim staff guidance, the Steering Committee and task working groups have conducted 30 public meetings with industry representatives. These meetings have been highly effective in gaining clarity on the industry needs and concerns and in developing the interim staff guidance.

Also during 2007, the Steering Committee and staff have benefitted from several interactions with the Advisory Committee on Reactor Safeguards. Recommendations of the Advisory Committee have been incorporated into the project plan and are being implemented.

The staff plans to provide periodic updates to the Digital Instrumentation and Control Subcommittee of the Advisory Committee on Reactor Safeguards. The staff also continues to extensively interact with domestic and international counterparts.

Several additional examples include participation in the Multinational Design

Evaluation Program meetings to discuss digital instrumentation and control design criteria for new reactors, participating in the Nuclear Energy Agency digital instrumentation and control inspection counterpart meeting, participating in National Aeronautics and Space Administration workshops to develop methods for assessing software-based system reliability, and participating in the pharmaceutical industry workshop on good practices for automated systems.

At this time, we would like to provide you additional detail on the issues being addressed by three of the task working groups. Mike Mayfield will discuss diversity and defense-in-depth issues and Mark Cunningham will discuss aspects of electrical communications within highly integrated control room designs and risk assessment.

MR. MAYFIELD: May I have slide 18, please. Good afternoon, Chairman and Commissioners. Diversity and defense-in-depth, as I'm sure you've gathered from the earlier presentations, has been a subject of considerable attention, not only by the Commission and the staff but by the industry over the last several years. I'm just going to spend the next few minutes describing the current staff efforts in this important area. Slide 19, please.

Common cause failure is one of the key safety issues in digital systems and has been found to be credible, while common cause failure in digital systems is considered to be beyond design basis. Per Commission direction, digital reactor protection systems should be protected against common cause failures and this is a major consideration in the staff's guidance. Current staff guidance is provided in

the Standard Review Plan which was developed in part from the 1993 Commission Staff Requirements Memorandum. The Standard Review Plan has been used successfully in staff reviews and licensing applications such as the AP1000 design certification and reviews of digital I&C platform topical reports.

It is currently being used in the review of the ESBWR design certification and pre-application topical and technical reports for other designs. However, the industry has expressed a desire for additional guidance from the staff for clarity and regulatory certainty. The staff is currently working with the industry in a public setting to further improve the existing guidance.

COMMISSIONER McGAFFIGAN: Can I ask a clarifying question? Is this 30 minute issue handled in the 1993 guidance?

MR. MAYFIELD: No, sir. That's part of the clarification that came from the interim staff guidance. There have been five public meetings to date to develop and execute the project plan. The staff does have a clearly defined plan which is currently on schedule. Slide 20, please.

We have identified seven key technical issues regarding diversity and defense-in-depth and they are listed on this slide. The issues are described in much more detail in the project plan and in the interest of time I won't describe them further at this point. Slide 21.

Jack just described our process for developing and issuing interim staff guidance. The staff has issued draft interim guidance on acceptable diversity and defense-in-depth and the timing for operator actions. Commissioner, this is where

the 30 minutes came in. These were the first two of our seven issues in this area.

The draft guidance provides acceptable diversity and defense-in-depth criteria including operator action time and the need for automatic diverse back up. It has been made public and was discussed in a public meeting in June. The industry has recently provided comments and the staff will address those comments and issue the interim guidance in September.

The interim guidance is intended to supplement the existing Standard Review Plan and provide the industry with additional details on acceptable approaches to addressing diversity and defense-in-depth that would have a high likelihood of staff approval in the timely manner.

Draft interim staff guidance on the remaining five issues has been developed and is currently going through staff and management review. Once those reviews are completed, it will be made publicly available and discussed in task working groups meetings with the industry to gain their comments. The staff plans to issue this interim staff guidance on schedule in September. Slide 22, please.

The staff has described a clear path forward through the project plan and we're implementing that plan. This includes issuance of interim staff guidance by the end of September for industry use. Additional improvements will be made as necessary beyond September as the staff continues to gain new information, lessons learned and stakeholder feedback.

The staff envisions the interim guidance will be incorporated into the

establish regulatory guidance such as the Standard Review Plan or Regulatory Guides. We will continue to coordinate such efforts through public involvement. While the staff is working on development of the interim guidance and long-term regulatory guidance, we will continue to use the existing guidance, the Standard Review Plan and the Regulatory Guides, to make progress in the review and approval of licensing applications. This completes my remarks and I'll turn it over to Mark Cunningham.

MR. CUNNINGHAM: May I have slide 23, please. Good afternoon. As Jack Grobe noted earlier, I will cover two topics this afternoon: communications aspects of highly integrated control rooms and risk assessment. Slide 24, please.

The subject on the next five slides is one aspect of the new control room designs. Specifically, it's the proposed use of two-way communication for information transfer between safety divisions and between safety and non-safety equipment. Traditionally in this agency, no communications have been permitted between safety divisions and only one way communications between safety and non-safety; that is from safety equipment to non-safety equipment.

We believe that the new designs that include this increased communications can provide acceptable and perhaps even greater levels of safety than now exist. However, the proposed designs are not well covered by existing guidance and the staff is working to improve that guidance. Slide 25, please.

This topic has been the subject of seven public meetings since February. In these meetings, a number of technical issues have been identified. Four of

those that are shown on this slide emerged as those most needing guidance. They are inter-divisional communications; that is two-way communication between safety divisions or between safety and non-safety equipment. Command prioritization, which is insuring that equipment that responds to a safety signal in circumstances where multiple commands may be received. Multi-division control and display. Some of the designs include computer workstations that include controls for more than one safety division. And network configuration; that is the element of a design needed to ensure that safety information is properly transferred.

The task working group has made considerable progress on each of these issues as I'll discuss in the next two slides. The first two issues of inter-divisional communications and command prioritization. The staff has drafted initial guidance and acceptance criteria and released it publicly. The draft guidance on these two topics has been discussed at the past several DWG meetings. Slide 27, please.

Guidance on multi-divisional workstations is still under development. The specific issue of using non-safety work stations for safety control is one of the more challenging issues down inside of this issue. The staff expects to publicly release guidance on this issue this week for discussion at a task working group on July 27th.

The topic of network communications arose recently as a result of operating experience. The staff has just begun the interactions on this topic. Slide 28, please.

Considering these and all the other technical issues, staff plans to issue a revised draft version of the guidance on August 10th and issue this in final form by September 28th. Following this, the staff will develop plans to incorporate what's in the interim staff guidance into regulatory guides and the SRP using our normal processes. Staff will also be working with standards organizations to incorporate the information into their documents. Slide 29, please.

COMMISSIONER McGAFFIGAN: This may be a strange clarifying question, but you said the topic of network communications arose recently as a result of operating experience. Staff has begun interactions on this topic. Is that going to be in the September 28th and August 10th?

MR. CUNNINGHAM: Yes.

COMMISSIONER McGAFFIGAN: You can solve these things in two weeks?

MR. CUNNINGHAM: As best we can.

MR. REYES: We will take a position, sir. No question about that.

COMMISSIONER McGAFFIGAN: Your big into taking positions however unpopular they may be.

MR. REYES: Because then that gets dialogue and then we can resolve it. If we just study it to death, we'll never move forward. We're not in that timetable.

MR. CUNNINGHAM: I'm going to turn now to the issue on slide 29 of risk assessment. Both the staff and the industry recognize the value of expanding

the use of risk assessment in digital systems safety rules. This of course is consistent with the Commission's PRA policy statement that encourages the staff to increase the use of risk assessment in the agency's business.

In the past, risk insights have been used in design certifications in specific and more limited ways. In the future, we think that risk assessment can be used to improve the basic regulatory practices such as those associated with diversity and defense-in-depth. These improvements could apply both to the new designs and operating plants. We view the work of this task working group as longer-term, but nonetheless we're working to develop some guidance. Progress will be discussed in the next two slides.

In the shorter term, on slide 30, staff will be writing guidance on the acceptable use of risk insights and digital systems reviews. Staff will be doing this using information from the industry and two industry white papers from NRC's research program and from operating experience. And more generally just from lessons learned from the design certifications that have already occurred.

Over the next seven months, the staff plans to continue to interact with industry in public meetings to assess the information that we're gathering from these sources. Using the information that we expect to develop interim staff guidance and discuss this in public meetings with the industry and further task working group meetings. We expect to have this ISG issued by the end of March of 2008. Slide 31, please.

With respect to risk informing digital systems regulatory practices, from our

perspective a key point is what the current state of risk analysis technology in the area of digital supports. Put another way, what state of technology is needed to permit specific risk informed improvements in our regulatory practices?

As such, and as I mentioned earlier, we view this as a longer-term activity. We will continue to work with the industry and other interested stakeholders including the Advisory Committee on Reactor Safeguards to better define what needs to be done to improve the state of technology and then we'll work these issues and write the necessary regulatory guidance. This concludes my presentation. I'll turn it back to Jack Grobe.

MR. GROBE: Slide 34, please. Just a brief summary. The Steering Committee is functioning effectively, implementing the expectations in its charter. The NRC’s project plan is in place describing near-term deliverables and deadlines and long-term expectations. Interim staff guidance is being developed on a schedule to support industry and staff needs. I just want to emphasize that our existing guidance is adequate and has been used effectively.

Industry desired clarification on that guidance for a more predictable and clear transparent licensing process. This interim staff guidance is the first step in producing more clear and predictable guidance. Once we produce an interim staff guide, it's not locked in. We're going to continue refining that and then incorporated it into our regulatory infrastructure with input from the industry.

Our interactions continue with the industry and other public stakeholders. The industry is providing good support to the staff. The staff is aggressively

seeking knowledge from domestic and international counterparts and the staff is on schedule to complete our near-term deliverable.

This completes our prepared remarks, ahead of schedule, I should note.

MR. REYES: We're ready for questions.

CHAIRMAN KLEIN: Thank you very much for that informative presentation. Commissioner Lyons?

COMMISSIONER LYONS: Thanks to all of you for a very well done and very informative presentation. Maybe my first question to Luis or maybe it goes to Bill or Jack, I don't know.

The message that I think I got from the sum total of your presentations was that you're well on track. You've responded very effectively to the Commission's guidance to emphasize what I think we heard at our last meeting about the digital I&C being potentially one of the very, very important items on the critical path.

Somehow, I got a different impression listening to some of our industry colleagues in the first panel and several of us have commented on Amir's statement about don't let the schedule drive the programs. I, too, am puzzled as I think several of my colleagues were. I'm just curious if you could shed a little bit more light on this apparent diversions, difference.

MR. REYES: Let me try to start and I'll turn it over to Jack. I think where we're coming from is this was presented at critical path on the deployment of new facilities in this country. You have to remember when we finish with this topic there is another critical path that's coming. You're always going to have a

critical item coming down the road and we're trying to seek what those are and make sure we start working on them.

If you stay with this one that says this is a critical path for the deployment of a new fleet, we feel we put an aggressive effort in terms of the Steering Committee. We're queuing the industry to put out guidance.

We're not too different in the comments you heard this morning from the industry because when we did similar license renewal and other activities, our guidance needs to be refined. If you need something to move forward, we think we're going to have the key elements of it. Is it going to be published and final in terms of forever; we're going to use that with digital instrumentation? Probably not.

But what we want to do is put enough to try and alleviate this issue of this is the critical path. I think we're not that far apart on where we are. We understand their comments about don't make it so final that you can't refine it down the road. I wouldn't want to speak for the industry, but I think that's what they were trying to convey to us. Don't take a hard position that's not movable simply because September 30th is knocking on our door.

I don't think we're that far apart, but our experience has been we need to put something on the table. We need to have it criticized and commented on by a lot of people and we'll eventually come out with the final product. We're just trying to have a product that's good enough for them to move on with their projects.

Jack.

COMMISSIONER LYONS: You're putting a lot of an emphasis on word "interim". That what we are doing now is near-term, keep the system moving ahead, recognize that in the future we can have better final products.

MR. REYES: I can't speak for them. We don't know if our interim guidance is good enough for them to do the design. We think there's enough there now. Is it going to be the most economical design? Probably not. That's where the interim guidance needs to be refined to make sure you keep the safety, but then you don't require any more margin than is necessary. I don't know if you want to add –

MR. GROBE: Just a couple additional thoughts. The interim guidance was clearly not intended to be final guidance. It was responsive to aspects of digital technology that are different than some of the other issues that we deal with in a licensing context and that is that the diversity – not diversity and defense-in-depth – but the diversity in the way people are designing systems and approaching problem-solving and the rapid way in which the technology is evolving creates a lot of regulatory uncertainty.

Our prior guidance has been used adequately, but it's not a highly predictable environment. The principal purpose of the interim guidance was to deal with those sticky wickets that we've identified with the industry that need clarification and provide a very clear, transparent and predictable set of guidelines that we can refine as we do additional work going on into 2008.

But to put something on the table with industry input which is clear,

predictable, transparent and provides the additional detail that the industry requested based on our prior guidance in the areas that was not sufficiently specific.

MR. BORCHARDT: Can I just add from a new reactor perspective. We're in a position of needing to make final positions. We're certifying designs, approving combined license applications and so we are working with the vendors to find a mutually acceptable regulatory position on these key issues that will be finalized in the design for these facilities that get built.

We have done that for the certified designs already. They resulted in design acceptance criteria because the final design details weren't developed, but the fact is that we found the designs that have been certified to be acceptable and what remains to be done now is the detailed design work. I don't mean to minimize the significance of that. It's a lot of work that still needs to be done by both the applicants and the staff, but we are reaching final positions.

COMMISSIONER LYONS: I guess a question related to that, Bill, that I wanted to ask anyway but it may fit in well here. I'm just curious if in your mind are you comfortable that we're providing the right level of detail in the acceptance criteria without losing too much flexibility for technology that's rapidly evolving. I asked that same question to the industry, too.

MR. BORCHARDT: The whole reason design acceptance criteria was created, because it's not an original concept of Part 52, was in order to afford that flexibility. I think it very clearly does that. At some point, we have to lose the

flexibility and come up with a final design and we're quickly approaching that for the first wave of COL applications.

MR. GROBE: The interim guidance was certainly not intended to be the only answer. It was to provide a position on these difficult issues which the staff would find easy to accept; high likelihood of acceptance by the staff with minimal interaction. That doesn't mean there's not other ways to solve the problem.

COMMISSIONER LYONS: Thank you. I look forward to another round.

CHAIRMAN KLEIN: Commissioner Jaczko?

COMMISSIONER JACZKO: I guess the first question I would ask it seems that what I was hearing from the earlier panel, perhaps there's a difference that maybe Bill you hit on that for new reactors verses existing reactors upgrading their specifications. It seems like Westinghouse has said pretty clearly that they feel they're ready to go with whatever existing guidance is out there.

Certainly Amir's comments, I don't mean to characterize your comments, Amir, but for existing fleet there may be more issues in terms of doing these things. The nature of the plants is such that there may be more work. Does the staff find a similar split there? Hopefully, everybody heard what I said.

MR. REYES: We haven't had a lot of examples, but we have had some unsatisfying examples where existing fleet designs want to be upgraded for a lot of good reasons to digital and we found out that our expectations were not

met. I think it's Duke Power, Oconee, specifically. It happened to be an issue where the emergency safeguards actuation and the reactor protection system there we're a lot of communications and we didn't feel that it was adequate and the company took that back and it's going to come forward with a revision. I think it's doable.

We have had at least two plants that come to mind who have upgraded their reactor protection systems with new generation reactor protection systems. It's not a full digital system, but we have dealt with that before. There may be some differences, but I don't see why we couldn't accomplish it similar to the new fleet.

COMMISSIONER JACZKO: Maybe then turning to one of the issues that did seem to come up with the interim staff guidance. Maybe Jack, you can answer this. This issue of the 30 minutes; if action can't be taken within 30 minutes then there has to be a diverse and defense-in-depth. What's the origin of the 30 minutes? Is that based on previous technical work or is that new technical work?

MR. GROBE: It's certainly has become a lightning rod, hasn't it. We've approved a range of time frames in the past at operating reactors with analog technology, ranging from 10 to 30 minutes. As a matter of fact, in our Standard Review Plan specifically focused on inadvertent delusion accidents in a shutdown condition. Our Standard Review Plan specifies 30 minutes. The International Atomic Energy –

COMMISSIONER McGAFFIGAN: That's for a spent fuel pool?

MR. GROBE: Yes, It's refueling operations.

MR. REYES: When the reactor is in refueling mode.

MR. GROBE: Right. Refueling operations –

COMMISSIONER McGAFFIGAN: Time lines are much longer there than a reactor at power?

MR. REYES: It depends on the scenario.

MR. GROBE: We need to make sure we're talking about the same thing. The 30 minutes is the time frame that the system will function automatically and operator action is not necessary. Not the amount of time that the operators would have to take action. The system would have to function by itself for the first 30 minutes.

COMMISSIONER McGAFFIGAN: It's easier in fuel operations when the plant has been shut down than when the plant is at power. You tend to want operator actions more rapidly.

MR. GROBE: When the plant's at power, you also want the automated systems to function effectively, more rapidly.

COMMISSIONER JACZKO: The longer the time window, the more conservative.

MR. GROBE: That's right.

COMMISSIONER JACZKO: So longer than 30 is more conservative than less than 30.

COMMISSIONER McGAFFIGAN: Why do we use lower numbers for, as the first panel said, for design basis events?

MR. GROBE: The numbers are specifically related – I mean the time frames are specifically related to the specific casualty. The complexity of the situation that the operator would face in understanding that he's got a problem, diagnosing it, identifying courses of action to take and then taking those actions.

I was going to mention that the International Atomic Energy Agency has a guideline in this area and depending on those factors, the guidance says 15 to 30 minutes. We met with six other regulatory agencies earlier this month and three of them used a 30 minute or greater criteria. One used a 15 minute criteria and the other two did not have a specified criteria.

The complexity of digital technology makes these issues more difficult to deal with. In addition, we have some uncertainty in predicting the failure modes. Thirty minutes was a clear criteria that would be predictably something the staff could deal with and expect to approve if it was applied correctly. That's where the 30 minutes came from. There is some foundational basis for it, both internationally and in the United States and it's certainly not the last word. We've received industry comments and we're evaluating those.

MR. REYES: Make a point that that's for design basis accidents. The 30 minutes, right?

MR. GROBE: Which 30 minutes?

MR. REYES: The one the Commissioner asked about the 30

minutes for operator action.

MR. GROBE: No. We're specifically dealing here with common cause failures, which is beyond design basis.

COMMISSIONER JACZKO: So Mike –

Mr. May field: It’s common cause failure coupled with design basis

COMMISSIONER JACZKO: it would be applied – the digital failure itself is not considered design basis accidents?

MR. GROBE: That's correct, common cause failure.

COMMISSIONER JACZKO: I have some other questions and I think – I certainly think as a first stab, 30 minutes doesn't seem unreasonable to me.

MR. REYES: I think there's a point that industry made. I'm not sure it got caught by everybody. When you go beyond design basis accidents such as failure for the reactor to trip, ATWAS, you do not have 30 minutes to study the situation. They made some good points. We just need to wrestle with the points that were made this morning on the earlier panel. I don't want to dismiss those.

But in terms of designing and accepting design basis accidents and then superimposing some other failure on the digital system, we need to come up with the guideline. So we put a guideline down.

COMMISSIONER JACZKO: As I said, certainly from what I've heard, it seems to be a reasonable first approximation and certainly I'd be interested if there are any changes in that as we go forward. Thank you, I will certainly have more questions.

CHAIRMAN KLEIN: I'm sure there will be others that have more questions as well. Bill, a question for you in terms of the last meeting that we had on digital I&C. I asked this to the first panel. We sort of got the sense of urgency that there was this problem; the light bulb came on and a critical path. So from the staff's perspective, are we on track to have the first simulator when it's needed?

MR. BORCHARDT: I'm not aware of a policy issue that needs to be resolved in order for the licensee applicants to go forward and do their procurement. What remains to be done is an awful lot of detailed design work that will ultimately need to be reviewed by the staff. I believe it can move forward. If there is a policy issue, I'm not aware of it.

MR. REYES: That brings the next critical issue that we're going to end up discussing when it bubbles up. I'm already predicting what it is.

CHAIRMAN KLEIN: There's always a critical path.

MR. REYES: Then it's how you use it and how you train the operators and how we're going to examine the operators. So that's obviously the next phase to that.

MR. BORCHARDT: Maybe I should get a little more specific. We have not drawn final conclusions on the EPR or the USAPWR design. We don't have those applications yet for pre-application review activities. There are still a lot of things we don't understand. I'm not quite as far down the road on those two designs as I am on the other three.

CHAIRMAN KLEIN: Thanks. Jack, a question for the existing fleet.

Clearly, with the new reactors we have an opportunity to sort of stand back and say here's what they need. When I go into the existing fleet, you see a lot of analog systems and I guess that to me is as much of a concern in a way as the new fleet that's coming.

Could you tell me how are we proceeding with migration to digital controls on the existing fleet? Are we doing it in a standardized way?

MR. GROBE: Luis mentioned earlier Oconee was the first comprehensive retrofit of digital and it was not one of our best moments as far as clarity of staff position and ability to resolve the outstanding issues. I certainly don't want to speak for the industry, but I believe once we complete the Oconee review, which we expect to come back in later this year, we will have established a benchmark – they're kind of the leading edge right now as far as getting substantial retrofits licensed.

I would expect that following Oconee there will be significantly more movement in the industry to do massive retrofits of digital technology. Maybe that's a good question for Amir to respond to also.

MR. REYES: There's a lot of retrofit that has already occurred. Both feed water controls at the plants have been retrofitted to digital. Those are non-safety related, but they could induce a lot of transience and all that. So from an operational point of view, the industry probably has the same desires as we have looking at the safety side of the house.

There is a lot of hands-on experience in feed water control replacement

from analog to digital all over the fleet almost every place you go to. The question is going to be I think what the Duke submittal was, it was a major retrofit and you end up with the same list of issues that we just went through. The cross connection between safety related and non-safety related inter-divisional communication because what you basically are saying is that chunk of the plant is becoming a new plant, a new design when you do that major retrofit versus just retrofitting a part of the plant.

It's not clear to us if everybody is going to come with a major retrofit at the same time versus a section or phases of the retrofit. I don't think we have that intelligence yet.

MR. GROBE: It's clear that the work that we're doing under the Steering Committee is going to benefit new reactors, but it's also going to provide much more clarity for operating reactor retrofits and much more predictability. I expect there we're going to see a lot of those moving forward.

CHAIRMAN KLEIN: How do you interface with our colleagues from other countries on their retrofit? Do you have a committee, a group that's meeting with our international colleagues?

MR. GROBE: There's no standing committee and others can clarify this if I mess up. But I don't believe there's any standing committee as far as retrofits. There's a lot of interaction on research and developmental work on new reactors in those areas. But I don't believe we have any standing interactions on retrofits.

MR. MAYFIELD: Other than through the agency or the offices have a number of bilateral agreements and so there's discussion through those vehicles. There are mechanisms, but there isn't something focused like an NEA committee or an IAEA committee to deal with it.

COMMISSIONER McGAFFIGAN: Should there be?

CHAIRMAN KLEIN: That was my question as well. As we move in this direction, it might be worthwhile to take a look at that kind of a program. Commissioner McGaffigan?

COMMISSIONER McGAFFIGAN: The NEA approach strikes me that you'd have all the right parties if you were to have some sort of NEA program group.

MR. BORCHARDT: In fact, the CNRA has before them right now a proposal to create a subcommittee on new reactors which this would likely be one of the activities that would fall under that group.

COMMISSIONER McGAFFIGAN: This applies to both new and old.

CHAIRMAN KLEIN: Maybe you'd have a subcommittee on old reactors.

MR. BORCHARDT: There already is.

Commissioner Jaczko: There is a full Committee on that.

MR. REYES: Old Committees on old reactors, we don't have any new ones.

COMMISSIONER LYONS: It certainly isn't slowing down what

they're doing around world.

COMMISSIONER McGAFFIGAN: I wonder what sort of safety evaluation reports those other people write and maybe we can learn from them or maybe they'll learn from us a more careful approach.

As I said earlier, not being an expert in this area, I suspect that a lot of the staff positions are going to be positions that reflect the Chairman's origins that we're from Missouri and the Show Me State and we're going to be careful. I don't mind that.

I'm speaking for myself, but George Apostolakis has been listening to all this today and I know he had a recent time to talk to us, confuse us. Do you have any comments on the dialogue you heard today from your personal perspective. You don't have to speak – if I ask you to speak for ACRS, you'll be mute.

CHAIRMAN KLEIN: Faculty members are never mute.

MR. APOSTOLAKIS: No, Commissioner. I have no comment.

COMMISSIONER McGAFFIGAN: You have no comment that this approach is compatible with what you all envisioned and you're more interested in the end game then the interim guidance. Is that fair to say?

MR. APOSTOLAKIS: I don't know whether we'll have a chance to review the interim guidance.

COMMISSIONER McGAFFIGAN: You probably won't. The comments I thought I heard last time when you guys were before us is that you seem to be more interested in the eventual outcome.

MR. APOSTOLAKIS: In the risk area, yes. I think it's a very long-term project.

MR. GROBE: We're going to be providing the interim guidance to the advisory committee as we go through generating it and we plan on regular meetings every eight to 12 weeks with the subcommittee. I expect that we'll get into dialogue.

COMMISSIONER McGAFFIGAN: Are there meetings scheduled between when you publish this in August and when it's finalized in September?

MR. GROBE: I think our next meeting is the second week in September.

MR. REYES: The committee will have an opportunity when we certify a design or approve the COL, it clearly goes through them and part of it is this is a piece of what we approve.

MR. GROBE: All of our processes early next year when we start incorporating this into our existing infrastructure include ACRS review.

COMMISSIONER McGAFFIGAN: Mr. Chairman, I'm going to pass and let others ask questions. It's an area where conservatism is appropriate to start.

CHAIRMAN KLEIN: Commissioner Lyons?

COMMISSIONER LYONS: Rick, I was curious if you could comment a little bit on the level of interest that you're seeing on these workshops coming up in September. Do you anticipate there will be a fair bit of interest?

MR. CROTEAU: Yes. We're getting a great deal of interest and like I said, we're doing a lot of advance work going out to facilities and talking with folks. There's a tremendous amount of interest. I asked Steven this morning is anyone else looking to take the lead, perhaps a bigger agency or something like that. He said, "No. They all want to jump on our bandwagon and cooperate and participate."

We're seeing a lot of interest and that's one of the reasons why we set up a two-day workshop to discuss the technical issues because it didn't seem as though we would be able to address all those things in one day. The non-technical things we think we can take care of in one day and we split that out.

COMMISSIONER LYONS: I'll certainly be cheering you on in that. I do think if we can work towards a facility like that it could be very important for the country well beyond this industry. I appreciate that.

Probably a quick question for Jack. As I was reading the charters of the six different working groups, in a few cases I was puzzled about what is and what isn't in their charter. Let me just give you one specific example which would probably help me understand the way the charters were set up.

In the first working group on cyber security, it specifically excludes any consideration of fire walls and intrusion detectors. To me, those are kind of major things in cyber security. I'm puzzled. If you could comment a little bit about why – I maybe misunderstanding what the output of these working groups is supposed to be if something like firewalls and intrusion is excluded from cyber security.

MR. GROBE: I'm going to have to phone a friend on this one. I think I saw Mario. Go ahead.

MR. MORRIS: I may need a life line, also. I'm Scott Morris. I'm the Deputy Director of Reactor Security in NSIR. I happen to have cyber security under my control, I guess, for lack of a better word. The issue that we're trying to resolve in this technical working group is a singular problem statement that was derived based on the interaction with the industry. The industry raised a specific question. We aligned on what that question was and established as closely – as clearly as we could what the problem is that the working group was trying to solve.

The basic problem that was trying to be solved by this working group is what the industry perceived as inconsistencies between established regulatory guidance, namely Reg Guide 1.152, which was recently revised to address cyber security, but specifically for safety systems.

And what the industry has proposed, namely an NEI document, NEI-04-04, which is a program document that industry can use to establish a global cyber security program at their site, which includes not only safety systems, but also security related systems, systems that are needed for emergency response.

And so the industry's basic concern was there's an inconsistency between the Reg Guide that you've established and this NEI document which you have reviewed and thought was a good document and where ultimately we're headed in rulemaking space because you may be aware that the revised security regulations in Part 73 have a major new component in them, specifically cyber security, with 8

or 10 new elements in it.

So the industry has been very eager for the NRC to adopt the NEI Program Management document for cyber security as a means to implement all the requirements that are coming down the pike in this new rule. But they saw an inconsistency between what's already out there, and frankly, already been used to license safety systems looking at cyber.

I guess the short answer to your question is we focused singularly on identifying the gaps and overlaps and inconsistencies between the existing Reg Guide and the new NEI Program Management document and are exclusively focused on ironing out those issues.

That is to say, however, that my staff has those issues before us. The firewall issue, intrusion detection; those are all things that need to be addressed, but are going to be addressed not in this specific forum, but in another forum in the rulemaking and guidance development, et cetera.

COMMISSIONER LYONS: Okay.

MR. MORRIS: I know that's a very long answer to you question, but there's a lot of context there.

MR. GROBE: The Steering Committee and task working groups were set up to address the specific problem not to replace the entire infrastructure in the agency that's working on all these issues. That was to identify the specific significant areas of concern in our regulatory guidance and to define those and then solve them.

COMMISSIONER LYONS: I gather, too, that the working groups are coming up with broad policy statements in specific areas with perhaps not getting into the specifics at the working group level of a detail like firewalls and intrusion detection.

MR. GROBE: The working groups are coming up with specific guidance addressing those particular problem areas, not the entire spectrum of digital.

COMMISSIONER LYONS: I guess – certainly, you made me feel better when you pointed out that both of those areas in intrusion detection and firewalls are very much part of your focus. Probably my biggest concern was how could we not deal with those two?

MR. MORRIS: Our basic challenge is we don't have any cyber security requirements in 10 CFR right now. They just don't exist. That's why we've created this whole section in the proposed rule. Part of preparing the guidance documents that support that new rule are going to necessarily have to involve those sorts of issues.

COMMISSIONER LYONS: Okay. And again, I'm way over my time. Sorry.

CHAIRMAN KLEIN: Do have another hot-button issue that you'd like to – since we won't get all of them, but do you have one more hot-button question you'd like to ask?

COMMISSIONER LYONS: If I were asking one more question, it

would go to Bill. On the question of – you made the point earlier that the reason the DACs have been used in many cases is to try to recognize the rapid movement in technology, but in your mind are those DACs – it seems to me – the plan that those DACs will be resolved by the time one issues the COL; such that you've transitioned into an ITAAC mode instead of a DAC mode?

MR. BORCHARDT: That would be my personal preference, but that's not the requirement. That is one of the acceptable approaches. The way the DAC can be resolved is part of an amendment to the design certification rule, such as Westinghouse is doing on AP1000. They could address DAC issues, provide more design information, and in essence transition the DAC into design information plus probably some ITAAC that need to be verified after construction or during construction.

The second, well you can address a Design Acceptance Criteria as part of a combined license application, in which case the issue would get NRC review, it would go through the opportunity for hearing as part of the COL and those issues in my mind, some of them would also be transitioned into ITAAC.

The third way, which is equally legally acceptable, although it puts all of us at more risk, is to just wait until construction, address the DAC as part of that, and what's that really doing in my mind is delaying the design review until the latter stages of construction, which was not the objective of Part 52.

So is the least desirable, although legally acceptable way of resolving the DAC.

COMMISSIONER LYONS: Wouldn't that latter way also lead to far more potential challenges or far more opportunities for challenge?

MR. BORCHARDT: Yes. And uncertainty as to whether or not it's acceptable to the staff. We would end up into something not all that dissimilar to the old Part 50 licensing process where the plant is being built and there's still unresolved issues, technical issues between the NRC staff and the applicant, let alone any legal issues that might derive from it.

MR. REYES: And from a practical point of view, you're designing and ordering components and all that because you can't wait. So you're basically back in Part 50 space if you push it all the way to the last example.

COMMISSIONER LYONS: I would join you in hoping that we minimize hopefully to zero the number of cases where we move into that third option.

COMMISSIONER McGAFFIGAN: It strikes me that that's also not at all compatible with the design centered approach.

MR. REYES: Correct.

COMMISSIONER McGAFFIGAN: We follow design centered approach to the day we gave it the COL and now we're going to all abandon it because we've got these DACs still to resolve and each guy is left to his own devices to resolve them.

MR. BORCHARDT: I hadn't really thought about that, but there's no reason the design centered approach can't continue past COL issuance. It can

pull you through the life of the facility.

MR. REYES: The risk is still the same.

CHAIRMAN KLEIN: Commissioner Jaczko?

COMMISSIONER JACZKO: I just wanted to ask one question. You may not have an answer to and you can get back to me on it. We've been doing a lot of work in the fire protection area with spurious actuations and looking at various cables. If we go to digital systems, I assume we'd be using different type of cabling. Have we looked yet at the behavior and performance of that cabling when it comes to fire related issues?

In particular, if you have issues, I don't know if you have the same kind of issues with spurious actuation and those kind of things. I don't know if that's an issue we've looked at yet.

MR. CROTEAU: I can speak a little to that. In Research, we recently had an opportunity to witness some Naval reactor testing. We're still working on results of that. I think it may have been just last week, but basically the fiber-optic cable, the cable itself is much less susceptible to fire damage and things. We're just the early phases of putting that together and taking a look at that.

COMMISSIONER JACZKO: Thank you.

MR. REYES: I think that if you look at the new designs, there's several design features that I think are going to make this issue not irrelevant but less relevant; physical separation, less number of active components that need to be repositioned to deal with an emergency, and then the fact that with copper

wires you can have electrical connections with fiber-optic cables, a little different scenario.

I think when you're finished with those three different design features, we're going to be in a much better space. I don't want to write it off.

COMMISSIONER JACZKO: I'm glad to hear that you're taking a look at it. And that it will be perhaps an area of enhanced safety.

Mark, I guess a question I have for you is maybe you can talk a little bit more – well, two questions. One, this idea of interaction between safety and non-safety systems is not something we do right now. Why is that something that would potentially become an issue with digital systems? Couldn't you just separate those systems in the same way that we do?

MR. CUNNINGHAM: It runs counter to the concept of a highly integrated control room is what it amounts to. From a design standpoint, from an operations standpoint, there are a lot of advantages to having all of this brought together. That's the basic thing. That is the technology that is emerging. We're in the context of trying to find acceptable ways to keep the right things separate, if you will.

COMMISSIONER JACZKO: Okay. The next question, and I appreciate that answer, really has to do with this issue of PRA. I've heard a lot about risk informing all of these things. I could've sworn we heard from ACRS that I&C components were inherently design flaws and that's not something we generally model in PRA space.

What does it mean to be talking about risk informing in this area and how exactly do design flaws in the software and the digital I&C, how does that contribute from a risk stand point? What is exactly the nature of this work going forward? Which everybody seems to agree is long-term work and I'm not sure is the most important priority right now.

MR. CUNNINGHAM: Part of it is are there new risk analysis techniques that could be used to capture more subtle type of failures that might occur in a software system or a multi-channel software system. That's a very daunting adventure, if you will, as to whether you could ever get to the point of modeling these types of things.

To the extent that some of these things, as they were saying earlier, you see software problems coming up in different ways and they manifest themselves as failures that you should be able to model in the PRA. You'll never get to the point to be able to model every type of failure.

COMMISSIONER JACZKO: In that sense, what you're modeling is the effect of the failure, but you can't necessarily model from the standpoint of probability or the frequency of this occurrence. At some point, you have to overlay into that and make an assumption about a particular software failure. What is the impact then in terms –

MR. CUNNINGHAM: In a lot of aspects of PRA what you're doing is not capturing the fundamental physics, if you will; it's the effect that it's having downstream. You end up lumping some of these together and estimating a failure

rate for a type of effect, if you will.

COMMISSIONER JACZKO: Just one follow up on that. Are the issues – certainly from the common cause failure, the issues there is if you've got a design basis accident is your reactor protection system or whatever digital system going to work properly to deal with that?

Is there kind of the opposite effect, which is that you can have a failure – are we looking at the aspect of having a failure in the digital I&C system that actually creates an accident scenario that you would do something from a reactor standpoint that would put you in a bad situation or is that not so much the issue?

MR. CUNNINGHAM: In risk analysis space beyond design basis event space, that would be fair game. You expect a new system can cause new problems, if you will. That would be fair to include in the risk analysis down the road a ways.

MR. GROBE: On a very low level, we just had an operating experience similar to that. It wasn't a design basis event at Honeywell. There was an inherent design flaw that was not disclosed until they had a failure of an inverter, an uninterruptible power supply. When they reestablished power, the system rebooted and unknown to the operators at that time, when the system reboots, it automatically goes to cold conditions so it repositioned a whole bunch of valves and the plant was hot. So there were various tanks that over pressurized and they had a small release of HF.

Those are the kind – the EPRI fellow talked about not design errors, but

unintended consequences of design that you didn't anticipate the full ramifications of that design until you have a certain scenario, sequence of events that enlivens that aspect of the design and it comes out differently. It resulted at Honeywell the operators having to go around and manually reposition a bunch of valves in the plant.

COMMISSIONER JACZKO: I guess that perhaps to some extent helps me better understand the statements that are throughout all the staff material about common cause failures not being design basis events. I guess from what I understand now, it would mean now that in the sense of the common cause failures will not be analyzed as leading to an accident situation. I guess, do we have a good technical basis for why that shouldn't be considered a design basis event?

MR. GROBE: It was a policy decision made by the Commission in the early '90s. I wasn't part of that decision making process, so I'm not sure what all of the considerations of the Commission were at that time. Our requirements clearly lay out the expectations for protection against single failures. This could be construed as a single failure, but the Commission decided that it was not. It was beyond design basis.

Although it is beyond design basis, the Commission directed that it is something that has to be accounted for in the design and the National Academy reaffirmed that in the late 90's that that was the proper approach to reactor designed digital control systems common cause failures.

COMMISSIONER JACZKO: Thank you, I appreciate that.

CHAIRMAN KLEIN: A question, Mark. When I go into existing reactor control rooms, you see a lot of stuff. You see gauges and dials all over the place. If you look at the designs for the new ones, it's much smaller. So the question is, if there is an event that one has to address, how do you prioritize the information that comes up on the screen?

MR. CUNNINGHAM: Again, that's kind of inherent in what lies behind those screens. There are some of the issues that they're dealing with on protocols and things like that. How do you ensure that the operator is getting the right priority of information? How are you ensuring that the components are getting the right type of information?

MR. REYES: You consider it much easier with analog system because what you're looking for; the rods are in the core, the turbine is tripped, and you're managing your water observing level pressure and temperature. That's basically it.

If everything is working in the integrated control room you can just hit it and it will give you your emergency operating and normal procedure basically mimic it and you can quickly say rods are in, turbine is tripped, water level pressure and temperature – boom, boom, boom. We're there. Now let's check the rest.

My view is it's much, much easier. Right now you have to run all over the place. Are the rods in? Is the turbine tripped? And you actually have to run half a mile all over the control room to get you where you want to be. This will give you a

much better way to manage the scenario; knowing where your parameters are and giving you the priority for the symptoms that you need to resolve in emergency procedures. It is, unless you have a common cause failure, it is much better for managing an event.

CHAIRMAN KLEIN: It will be interesting to watch when you get to simulators. As you simulate it, does it really work that way?

MR. GROBE: I was just going to mention that. We had the opportunity to watch a steam generator tube rupture on the AP1000 simulator. The simulator is not complete, but it's complete enough that they can run various scenarios and it was fascinating. The running around the control room is not just checking gauges, but it's going back and reading your procedure.

All of that's in the computer and it automatically sets you up with all the data that you need to walk through the procedure very rapidly. As a matter of fact, the computer can do the procedure itself. It becomes a very interesting man/machine interface, human/machine interface issue. That's one of the problem statements in the human factors area is what are called soft controls.

CHAIRMAN KLEIN: Well, Bill, I'll ask you the question I asked Amir. What are the two issues that you want the Commission to do to have success on digital I&C?

MR. REYES: Money and more money. That's what he tells me all the time.

MR. BORCHARDT: Well, I want to think continued interest and the

other one really is budget. It's the money. It's a difficult area to hire new talent into. They're not easy issues. They take time to resolve. It's something we are going to have to be working on for several years. That's really it.

CHAIRMAN KLEIN: Time and money, right? Commissioner McGaffigan?

COMMISSIONER McGAFFIGAN: Can I ask on this Duke/Oconee application. How long was that in with us and we were working on it before they figured they'd better withdraw it and start over? You said it wasn't our finest hour, but how long were we working on an application that we had accepted?

MR. GROBE: I don't have the exact dates. We can get that for you.

COMMISSIONER McGAFFIGAN: Was it months? Years?

MR. GROBE: It was not months.

MR. REYES: We can give you details.

MR. KEMPER: Hi. I'm Bill Kemper, the Branch Chief of Instrumentation and Control at NRR. We reviewed that application for about a year before it finally became apparent to all of us that due to quality considerations of the application, it was just not ready to move forward. The licensee decided at that time to withdraw it.

COMMISSIONER McGAFFIGAN: So it was about one year from the time we accepted it for review to the time that everybody mutually decided they best withdraw it?

MR. KEMPER: Yes, sir. That's correct.

MR. REYES: The issues that led to that –

MR. MARINOS: I am Evangelos Marinos. I am the Branch Chief for Projects and Oconee is under my authority to review and issue the license amendment. We did receive the license amendment in 2003.

COMMISSIONER McGAFFIGAN: 2003? And it's only recently –

MR. MARINOS: This amendment was withdrawn over a year ago because of controversy about requirements of the staff.

COMMISSIONER McGAFFIGAN: It was before us about three years. Okay. I understand Mr. Grobe's comment. Again, I'm not going to probe further. I'm just not an expert in this area. I sound like a broken record, but I do think being from Missouri in this area is a good thing.

CHAIRMAN KLEIN: Thanks. Thank you all for the staff's response. I think you can tell from the question that this is an area of interest to us. So we will have more hearings.

We still want to have a more robust National program that deals with digital I&C and I think the Commission will keep pushing that because it is very important, not only for the NRC, but for the Nation as a whole. If we can combine assets so that not everyone has to pay – I mean everyone pays – as opposed to just the NRC and the nuclear industry, I think we will be better served as we move toward the advancing digital I&C, including human interface.

So this is an area I think is very important for us and the Commission will continue its interest. Thank you for your presentations.