UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

BRIEFING ON DIGITAL INSTRUMENTATION AND CONTROL

+ + + + +

THURSDAY,

DECEMBER 17, 2015

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Commission convened in the Commissioners Hearing Room at the Nuclear Regulatory Commission, One White Flint North, 11555 Rockville Pike, at 1:00 p.m., Stephen G. Burns, Chairman, presiding.

COMMISSION MEMBERS:

STEPHEN G. BURNS, Chairman

KRISTINE L. SVINICKI, Commissioner

WILLIAM C. OSTENDORFF, Commissioner

JEFF M. BARAN, Commissioner

ALSO PRESENT:

ANETTE VIETTI-COOK, Secretary of the Commission

MARGARET DOANE, General Counsel

NRC STAFF:

VICTOR McCREE, Executive Director for Operations

JENNIFER UHLE, Director, NRO

JOHN LUBINSKI, Acting Deputy Office Director for Engineering, Office of Nuclear Reactor Regulation (NRR)

JOHN TAPPERT, Director of Division of Engineering, Office of New Reactors (NRO)

RICHARD STATTEL, Senior Electronics Engineer, NRR

DEANNA ZHANG, Senior Electronics Engineer, NRO

EXTERNAL PANEL:

DARREN COFER, Fellow, Rockwell Collins Advanced Technology Center

JOHN CONNELLY, Engineering Manager -- Capital Projects, Exelon Nuclear

ROBERT COWARD, Principal Officer, MPR Associates, Inc.; Digital I&C Working Group, Nuclear Energy Institute

DARYL HARMON, Consulting Engineer, Operating Plant Business, Westinghouse Electric Company

WILLIAM SCHERLIS, Professor, Carnegie Mellon University, and Director of the Institute for Software Research

P R O C E E D I N G S

1:01 p.m.

CHAIRMAN BURNS: Thank you, and I'll invite then our first panel on our meeting on Digital Instrumentation and Control to take their seats at the table.

(Pause.)

CHAIRMAN BURNS: Well good afternoon. I want to welcome our external panelists, the NRC staff and members of the public who are here or may be listening in on today's meeting. The purpose of this afternoon's meeting is to discuss the proposed rulemaking for incorporating by reference the Institute of Electrical and Electronics Engineers Standard 603-2009, the IEEE standard criteria for safety systems for nuclear power generation, which we'll refer to as IEEE 603.

We'll also be discussing other key regulatory and industry activities related to licensing of digital instrumental and control systems. The Commission has a proposed rule before it on IEEE 603, as a voting matter and today's discussions will aid deliberations on that paper.

The paper is numbered SECY 15-0106 and it is publicly available on the NRC's website. Our first panel will include presentations from the following persons: Mr. Robert Coward, Principal Officer, MPR Associates, also representing the Nuclear Energy Institute Digital I&C Executive Working Group; John Connelly, Engineering Manager of Capital Projects for Exelon Nuclear; Daryl Harmon, Consulting Engineer, Operating Plant Business for

Westinghouse Electric Company; Darren Cofer, Fellow with Rockwell Collins Advanced Technology Center, and William Scherlis, Professor at Carnegie-Mellon University and Director of the Institute for Software Research.

After we hear from our external panel, we'll have a five minute break and then hear from the staff. I look forward to presentations and the discussions. I believe Commission Ostendorff wanted to say something, and then I'll turn to the other Commissioners as well.

COMMISSIONER OSTENDORFF: Good afternoon. I don't often do this before a meeting. I'm going to do it today. It is an exception to my normal practice of being silent at this stage. But I think I want to set the stage for this, as far as my own personal views as a Commissioner.

I know in April 2010, when I went to my first commercial nuclear power plant and saw Watts Bar 2 and saw the analog instrumentation and reflected upon my experiences back in the 70's, at reactor prototype at S3G in Ballston Spa I didn't see much different.

In my five and a half years as a Commissioner, I've spent a lot of time looking at instrumentation control, digital I&C. I don't think we are as a nuclear enterprise where we need to be, either at the regulator stage or at the industry stage.

I think there's a lot of opportunity to do better, and that if we're going to continue to operate nuclear power plants in the future, we have to address these issues, some of which will be discussed today.

In September of this year, the Commission received a draft proposed rule on digital I&C from our staff. Along with my Commissioner colleagues, we've spent a lot of time talking about this. We've discussed, debated at a lot of other meetings before today's meeting, and I'll speak for myself.

I quite frankly am unable to come to any conclusion on what to do here, because I feel like we've not looked at the broader picture. We've looked at one piece on IEEE 603-2009. But we've not looked at the broader mosaic, whether it be other proposed rules the staff might be thinking about on common cause failure and dependence, etcetera, or what the impacts this might have for stakeholders represented today on the goal of upgrade the existing nuclear power plants from analog to digital.

So I think this is a really important meeting. I think this is an area of our regulatory work where there's much to be done, and I'm very grateful to all the Commissioners who have been very supportive of us having this session today. Thank you.

CHAIRMAN BURNS: Thank you. Commissioner Svinicki, okay. Well thank you, and with that Mr. Coward, would you please begin the panel presentation.

MR. COWARD: Am I on? I'm on now.

CHAIRMAN BURNS: Yeah, you are.

MR. COWARD: I'm Bob Coward from NPR. I've been asked by NEI to provide what I'll call the industry leadership perspective, and I'm tempted to thank, Commissioner Ostendorff, and pass to the next presenter.

I think that one of the messages that from an industry perspective we want to make sure we'd like to get everybody aligned around is people tend to look at the I&C problem these days. You hear a lot of people talking about the digital I&C problem, and I think we look at it differently.

We look at it as failure to capture opportunity, that when we look at plant safety, plant efficiency, reliability, even something as simple as the ability to maintain the plants, that moving towards digital is a big step in the right direction on all those goals, and something that the industry, all of us together would benefit greatly from.

It also has, from an industry standpoint, and I'm assuming that the staff shares this perspective, we almost see addressing these outstanding questions as a prerequisite as we talk about 60 to 80 that, you know, from a business decision/business investment perspective, there's not a board in this country that's going to approve an application to go to 60 to 80 if it doesn't have some level of confidence that these projects can be done reliably.

So from an industry standpoint, I think you know, we're eager and interested to move to a better place. We were at an NSIAC meeting last year and got into a good discussion among the chief nuclear officers about what's important, what should we be working, and this one quickly rose to the top of the list.

We reached out, a number of us, to talk to people in the industry. There's a lot of industry working groups and some of the staff participates on some of them, as to where things are, and sort of got a

quick landscape view of how things -- where are things at.

Just a couple of key points to give you that perspective. One, cyber. Everybody always tends to start with cyber, because that's a hot one these days. I think from an industry standpoint our perspective is cyber's okay. We'd like for cyber to be in a better place in terms of the value benefit equation of the effort put in, but on the big scale of things, we're willing to put that behind us if we can address some other questions first. We think they're more important.

We see good projects being done across the country. We see some digital I&C going into nuclear power plants, making their plants better, safer, more reliable, primarily in balance of plant secondary system applications, non-safety related applications.

We want to extend that. In terms of challenges, we see some questions about responsibilities not being clear, expectations not being clear, and we'll acknowledge that from an industry perspective, perhaps we've even stubbed our toe a couple of times.

You know, some of the 50.59s that have been done probably had holes in them and one of the things the industry's working on hard right now is to close those holes as well. You roll it all together and the big picture is almost everybody can see the benefits from a digital I&C upgrade enhanced replacement in a nuclear power plant.

The challenge is when you go look at the cost-benefit analysis, the decision-makers. These are not small, trivial projects, and the decision-makers who have the final say, they look at risks, they look at costs, they look at benefits. Even though they see the benefits, the costs and the risks are still outweighing those benefits in many

cases.

That's what we have to knock down, is we have to knock down together that perception. We actually want people desiring and embracing doing these projects, not to be sort of heading down the aisle skittishly or nervously.

In terms of a couple of specific places where we know we need to work, we the industry and we're looking forward to engaging with the staff to work together, 50.59 guidance. Industry's about to submit through NEI some updated guidance on 50.59 specific to digital.

We're looking forward to the staff engaging with questions and dialogue to ensure we're aligned. If you go back I guess six, seven, eight years, I think Commissioner Ostendorff, as you alluded to, there was much more of an interest in digital I&C. There was a big industry-wide effort, as well as engagement with the staff.

I think one of the things we now see in hindsight looking back is there were some things we all thought we agreed to, that perhaps we were saying different things to each other or hearing different things. Because as we've tried to apply or implement the things we agreed to, we're finding that there's different versions of, you know, some interpretable words.

So there are some things like when we say "common cause failure," what does that mean? Okay, let's go resolve that. Let's get everybody on the same page. Just a stable, regulatory structure, and I know you've probably heard about this.

In particular for the operating plants, the way that the licensing gears turn these days really doesn't work well for a utility for a

licensee, from a managed risk cost invested over the time as it affects risk profile. That makes it hard, and we think that -- we think that those gears can be adjusted a little bit, in a manner that still satisfies everybody's needs and becomes much more of an enabler to these projects being done as opposed to a hindrance. That's another area to work together.

Then more in the spirit of an anxiety than a gap or an issue, as we look forward as an industry to closing ITAAC at Vogtle and Summer, there's just anxiety of are we all on the same page as to how we're going to do that. There's questions. A lot of people in the I&C community are nervous that some of the things, you know.

In 2010, we thought we had agreement between industry and the staff on a number of technical topics. We've learned we really didn't.

Today, we think we have agreement on how to do some of these ITAAC inspections, and whether we do or don't is a question we have to go ask, and we'd like to answer that question in advance, not at the last moment.

You put all those things together and the chief nuclear officers, the CEOs asked NEI to put together a working group of industry executives, to help drive this and to help provide the leadership and the coordination of all the various industry groups and company's activities, and to get to a better place.

Ron Jones from SCANA is the leader. He's the chairman of that group. He had a commitment today; that's why I'm here for Ron. I'm on that group with Ron, as well as some other

industry executives, and we're working together as was with others from our companies and industry to try to provide that leadership, that guidance, a framework for engagement that will allow these issues, these gaps to get resolved once and for all.

We think that's doable and that's our goal. We're working on a road map. Let me back up and just say we don't think that the issue is missing guidance or more research or more paper. We think everything's there. We think that from the things that are within our own control on the industry implementation side, and with regard to the extent the industry engages with the staff.

We think it's more about coming together on this six feet of paper, what matters, how to implement it, what's the way to interpret it, because we think most of the research is done. We think that things are out there. We just have to, you know, it's more agreeing on it.

So the purpose of -- the road map we're putting together is to guide, from an industry standpoint, to guide us through that process. It's to paint the big picture, see the broader landscape, see how all these things fit together, see how they prioritize.

One of the things we're looking very hard at is what is the most important critical items that we can prioritize on that are prerequisites for other discussions and other decisions.

We're going to use that road map and it's going to paint the picture for the next several years, of how -- our version of how to get these issues resolved, how to do a handful of pilot projects, and to do that in a collaborative manner which not just answers the questions but

does it in what we'll called a sustained, reliable manner, so that the rest of the industry can then go forward and take advantage of the opportunities.

We're early. We've only really been working this year. The road map isn't quite done. But since I have the floor, there are a couple of asks or suggestions, recommendations that we'd like to make or throw out there.

One I already alluded to, and that's the engagement on the 50.59 guidance. We think that would be good for everybody. We think we have a better set of guidance now. We hope and expect the staff will agree.

The proposed rule on 603, we're all for updating the regulations. We're all for going to later versions of the standards. We think that's a good move in the right direction. We think some of the additional considerations that have been written into the rule actually are harmful.

We'd rather, if it's a choice of that or nothing, we'd prefer nothing. So our recommendation would be to put that on hold. We're looking forward to the staff engaging us on a working group manner, and then finally we're looking forward to the Commissioners being engaged and interested, to help influence and help set the priorities that leads this to resolution.

Because I think, you know, the big question for the last few years has been, you know, people ask can you do these projects reliably, safely, on schedule, on budget without licensing uncertainty. I believe the answer's yes. With confidence, I believe the answer's yes

and we want everyone together to be working towards, you know, how do we do that and demonstrating it and not asking the question of can we. That's where we'd like to get to.

I'm working on the assumption that some of these other presenters will get into a little more detail on some of the things I hit.

CHAIRMAN BURNS: Thank you. Mr. Connelly.

MR. CONNELLY: Good afternoon. First, I'd like to take a moment to thank the Commissioners for providing us an opportunity to present our perspective. There are several critical issues related to the application of digital technology. We greatly appreciate the opportunity to speak to them.

At the risk of stating the obvious, we share a common goal, safe and reliable operations. In our opinion, one of the best ways for us to achieve that common goal is for licensees to upgrade their facilities using the best available technologies. Establishing a clear and unambiguous regulatory framework is a key enabler for that.

Turning our attention to the third slide, I want to spend just a moment on this. Specifically, Exelon's operating experience on digital upgrades. We've been implementing non-safety related digital upgrades for about 20 years, starting with the feedwater systems at Dresden, LaSalle, Quad Cities and Limerick.

That was followed by turbine control system upgrades across most of the Midwest fleet and those continue today across both the Mid-Altantic and Northeast. Our primary focus was to improve system performance through great fault tolerance and elimination of

single point vulnerabilities.

So we looked at those projects and went back and looked historically over our scram data, going all the way back to 1980. The analysis we conducted paints a pretty compelling picture, which is reflected on this slide.

If you look at the feedwater system specifically, we observed a 95 percent reduction in scram rate between the analog systems and the digital systems. Now we did normalize this data so we got it in terms of unit years, so we could compare apples to apples.

We looked similarly at the PWR controls and observed an 83 percent reduction and the BWR turbine controls at 74 percent reduction. So clearly, that's a fairly compelling picture. Digital upgrades significantly reduce initiating events. So there are obvious opportunities there.

Next slide. I included this slide just as another point of data, if you will. This information is widely available on the Internet. You can find it on the FAA website, NTSB, various places. You'll find various iterations of this slide in a number of places.

This is a pictorial representation of hull loss events across the commercial aviation sector. So this wasn't developed for digital technology specifically, but there's an interesting nugget of wisdom that can be discerned from this.

The 747-400 was the first truly digital aircraft, the first glass cockpit aircraft. Now I will tell you that there is some overlap there. These product life cycles tend to be fairly lengthy, so there is going to be some overlap.

But the interesting takeaway from this slide is if you kind of draw a line through just above the 747-400, before that is analog aircraft; below that is digital aircraft. Now obviously this isn't the only factor at play. But there's an interesting takeaway from this. If you look at digital aircraft, while analog aircraft are safe, digital aircraft are safer.

The commercial aviation sector has fully embraced digital technology, and I think there's similar opportunities for us to gain from that experience.

Turning to the next slide, I do want to briefly touch on equipment obsolescence. Considering that a typical domestic plant has been in service roughly 30 years, and also with the full knowledge that and the inescapable reality that all electronic components have a finite life span.

Our exposure to equipment obsolescence is significant. We actively manage these issues. We have strategies in place to mitigate the risk. But the ability to use well-vetted digital solutions would be beneficial to all parties concerned.

The other thing that I'd like the Commission to take away from this discussion is if you think about the nuclear sector, we're a small slice of a very large industrial control sector pie. If you look outside of nuclear, if you look at petrochemical, pharma, the fossil world, digital is the preferred solution.

It is the preferred solution because of its capability, reliability, accuracy and cost effectiveness. So you know, separating ourselves from those product lines and those benefits is probably not in

our best advantage.

Next slide. Cybersecurity. I'm only going to touch on this very briefly. I know it's kind of a significant issue for the industry, but I do want to touch on a couple of things in terms of cybersecurity.

The industry and staff have made substantial progress in resolving implementation issues. There are mechanisms in place, the Cybersecurity Task Force and the interface between NEI and the Commission and the staff. We have made very significant progress.

The point that I would like to make, however, is that Milestone 8, our full compliance deadline for most licensees that's 12/31 of 2017. So effectively we have two years to completely implement the balance of the program. So timely resolution of issues as they emerge is critically important to all parties concerned.

The other point I'd like to make is that cybersecurity and digital I&C really can't be considered in isolation from each other. They're concentric rings around the same center, to a large degree, and there's a need to coordinate both the digital I&C piece of this and the cybersecurity piece of this, and we actually have that through the Digital Working Group.

That's an opportunity. All of those stakeholders are involved in that discussion. So that's an opportunity to get that coordination between the various elements and industry stakeholders.

Next slide. I'm not going to belabor this one in the interest of respecting people's time. I did include this in a presentation, just to kind of lay out the landscape that we're in right now. Most of what you're looking at here in this slide is applicable to safety related

modifications, but there is some applicability to non-safety related applications as well.

This speaks volumes to the need for a clear, unambiguous, graded, stable regulatory framework for both digital I&C and cybersecurity, and frankly we do have models that we can draw from- from other sectors. I guess the key takeaway I'd like to leave the Commissioners with is that while the technology itself can be complex, the framework itself could be simplified and made more streamlined.

Next slide. Unless there are dissenting opinions, IEEE 603-2009, we're going to be talking about that in detail in the next presentation, and we're certainly able to field more questions. The only thing I'd like to say here is that from our perspective, it's kind of like the Hippocratic oath.

The standard in place right now does no harm if we leave it as is. But our concern is- is that it may further muddy the waters and introduce yet another variable, and we'll be talking about that in more detail in just a moment.

So as Bob had alluded to, while I have the floor there's a couple of requests I would like to make. Again, and you'll hear this throughout the presentations and the discussion, a clear, unambiguous, graded and stable regulatory framework for both digital I&C and cybersecurity is critically important to all parties concerned.

Again, we'd ask that we maintain IEEE 603-1991 as the endorsed standard, because it doesn't adversely impact the industry's ability to modernize or introduce yet another variable. The agency and industry should work to develop consensus solutions to key

technical issues and we've alluded to that throughout the previous comments, and we'll be discussing further following presentations.

Specifically, the application of the 50.59 process, the technical reports that are being developed by EPRI and dealing and addressing software common cause failure. The agency and industry should continue efforts to improve NEI-08-09 revision. The currently endorsed version is Revision 6, Revision 7.

We have had discussions with the staff. There are a handful of things that we would like to get clarity around. We have been -- we have had some very productive discussions with the staff and I think we have a success path there.

Similarly, the agency and industry should continue to refine NEI-13-10. For those who are not familiar with 13-10, it introduces a graded approach to cybersecurity. Revision 3 was a watershed event. I would characterize it as a watershed event. We did gain a lot of ground with 13-10.

There are opportunities to improve it in subtle ways by including better worked examples of what good looks like and for potentially get some security programmatic assets out of the direct impact category and into indirect, so we can treat them with a subset of controls. And again, we've had good success working with the staff to get these issues resolved, on the table and resolved.

The last thing I would point out is there are methodologies that we can draw from as we work our way through this road mapping. You know, NAVSEA 08, aerospace, pharmaceutical, petrochemical. There are other standards and models that we can fold

into this process, and I would encourage us all to consider those.

Nuclear tends to be very inwardly focused, but there are other avenues, venues, standards, methodologies that we should consider as part of this process. With that, I'll yield 27 seconds.

CHAIRMAN BURNS: Mr. Harmon, you don't have to use the 27 seconds.

MR. HARMON: I'll start with a fresh ten. Good afternoon and thank you, Commission, for this opportunity to talk you about digital instrumentation controls. I come to you with two hats today.

One is from an vendor's perspective in the nuclear industry. I work for Westinghouse, but also for over 25 years I've been a member of the IEEE Standards Development organization and Nuclear Power Engineering Committee. So I'd like to talk to you a little bit from an IEEE perspective as well.

CHAIRMAN BURNS: Is your mic on?

MR. HARMON: Oops. Okay, thank you. That sounds better. From a Westinghouse perspective, we are heavily invested and believe in digital instrumentation controls. We have an approved common Q platform that we've had before the NRC a couple of times now, and we use it for our digital instrumentation control safety system implementations.

We use that as a key attribute to our new plant designs. So not only for upgrades, but in our new plants, we have 14 AP1000 plants that are being built around the world, ten in China, as you probably know four here in the United States.

We're also using this same technology, the digital instrumentation controls to implement the APR1400 plants in South Korea, Shin-Kori 3 and 4, and at Barakah in the United Arab Emirates. That happens to be the project that I currently work on the APR1400 projects.

If you were to come to either of those two type design's control rooms, you would be much harder pressed to find meters and dials and switches.

There are a few, but primarily you see large screen displays, flat panel displays and the technology behind those out in the plant is all digital safety systems and non-safety systems. So we are implementing our new designs with digital I&C.

We also do upgrades obviously, and as my colleagues have mentioned, we have been involved in reactor protection system, an engineering safety feature actuation system upgrades, post-accident monitoring systems, as well as on the S for safety side, as well as non-safety implementing feedwater control systems, turbine control systems and many other systems that we can upgrade to digital kind of on a piece by piece one at a time perspective.

That's been done both here in the U.S. and at other places around the world. We think there's a big benefit, and in the second slide I talk about some of the benefits. My colleagues have also mentioned these.

Certainly, as John mentioned, there's a decrease in the probability of events and they've seen this particularly with feedwater control systems, turbine control systems, that we don't challenge the

safety systems as much anymore. That's certainly a benefit to a safety aspect of the plants and as well as operations obviously.

A lot of functional improvements. The operators can get the information they need for different plant situations, different plant modes, put together with the controls, the information so that they can use it effectively, and there's a great capability to do that. There's also a capability functionally for redundancy and other functional improvements that allow these plants to be -- to move forward in reliability, as well as the operabilityl.

One aspect that's unique to digital, it allows us to do maintenance, surveillance, etcetera, from a remote location. Some of the intelligent devices, sensors and components can be configured. Troubleshooting can occur, as well as calibration from a remote location. There's no need to go around the plant.

This allows a plant, an existing plant or new plants to focus on some of the more maybe important or higher priority maintenance aspects. I mentioned human-machine interface. There's a great opportunity and we've taken advantage of that to improve the human-machine interface. Let the operators get the information they need for their tasks in the context where they need it.

Then as was mentioned, for obsolescence, we really think that digital instrumentation and controls is a preferred opportunity for us to address obsolescence with a better system what exists today.

So that's the Westinghouse perspective. Let me talk a little bit about IEEE. The IEEE Nuclear Power Engineering Committee, I'll call that NPEC from this point on, is the committee within

the IEEE that is responsible for all the nuclear-related standards.

I am a member of the Nuclear Power Engineering Committee. Also one of the subcomittees that IEEE 603 came from is the Safety-Related Subcommittee. For three years, I was the chairman of that subcommittee back about five years ago, and have worked on that subcommittee for close to 20 years.

In that subcommittee, we have working groups. There is a working group dedicated to maintaining IEEE 603 as well as one of the other standards. An important point here is that the IEEE is adamant about maintaining a diverse constituency in its working groups, as well as NPEC and the subcomittees.

So we want perspectives from vendors, from utilities, from regulators, and we have people from the NRC as well as other regulators on our working groups and on our subcommittees. When an IEEE standard like 603 is revised, it comes to ballot and is put before an industry consensus group in a standards association, which is somewhat independent of the Nuclear Power Engineering Committee itself.

Again in developing the ballot pool, we try to get a consensus that represents a diverse set of individuals, who can then ballot the standard and make comments. The working group then goes through and addresses the comments, to come up with the actual revision to the standard.

The point here is that IEEE 603 really went through an industry consensus, including the perspective of regulators, as it went through its process of being voted on back in 2009. We think that does

represent a good industry consensus.

If we go to the fifth slide, as I mentioned, it was -- we had this broad perspective, and IEEE 603 is actually currently being worked on again. We've learned some things through this rulemaking process and have feedback to IEEE 603.

The working group established a project authorization request, which allows them to modify, to revise the standard. That was approved back in February of 2015 and they're now working on incorporating some of the lessons learned, the information from the rulemaking effort back into IEEE 603.

Particularly the technical, those aspects of rulemaking that focus on technical issues, we're trying to again improve 603. There's another broader standard to IEEE 603, IEEE 7432. That is the standard criteria for programmable digital devices and safety systems of nuclear power generating stations.

It used to be called digital computers, but now we've expanded it to include programmable digital devices, FPGAs for example. That standard has just been balloted and will be issued a revision to that in early 2016.

It contains significantly more criteria for these digital devices, includes criteria for -- to address common cause failure in safety systems with digital devices. So we think that standard now, which the NRC has said they intend to endorse with Reg Guide 1.152, provides a good framework for addressing the digital I&C concerns at a more detailed level in some aspects than IEEE 603.

So some of the concerns in the last slide related to the

IEEE 603 rulemaking. One of them is that the conditions that were aforementioned do add detailed criteria to the proposed rule. It seems different than what's been done with the Code of Federal Regulations previously.

It may not be so appropriate for the Code of Federal Regulations, but more appropriate for a Reg Guide, and that's what we see typically happening with an IEEE standard as the staff goes through and creates a Reg Guide with their regulatory positions related to a standard.

Also one of the issues that we have, especially at Westinghouse where, as I mentioned, we do new plants and digital upgrades, there are different regulations being applied in some instances to new reactors and existing reactors.

That gives us concern in that we have one platform, one set of criteria that we use to design our systems, and we think it's inappropriate to have regulations that are diverse, are different from new reactors and existing reactors.

Then some criteria, special criteria being applied in the data communications that is contradictory to what was in the interim staff guidance.

We have concerns about that related to data communications, and we think that there should be a consistent set of industry standards and rules from the NRC related to the digital I&C and in this case data communications.

So to wrap that up, I think I share a concern with my colleagues that the existing 603 endorsement in the Code of Federal

Regulations does no harm at this point. Some of the conditions being applied may be detrimental to us, and we'd like to maybe work together to move forward in a different approach for the industry. I'll yield like 17 seconds.

CHAIRMAN BURNS: Thank you. Mr. Cofer.

MR. COFER: Thank you. Am I on? How about that? Okay. So I appreciated Commissioner Ostendorff's opening remarks about the S3G in the late 80's. I worked in NAVSEA 08 and did some work on that prototype plant, as well as others before joining the aerospace industry.

So this will be somewhat different, as I'll offer you some perspectives from the aerospace industry. This is -- I've come to appreciate that this is particularly relevant, because NAVSEA 08 since my tenure there has gone, you know, kind of faced the same problem and moved from analog to digital I&C and the way that they did that was to take motivation from the guidelines, the guidance used in the aerospace industry.

So perhaps there's something useful there. So if we could go through the slides here, I'll make reference to several of the points there. It makes sense to talk about our industries, because we do have a lot of similar concerns.

We're safety-critical, we're regulated, we use replication for fault tolerance and more and more we are software intensive, one difference being the nuclear plant is designed to be fail safe. You can shut it down. An airplane has to be fail operational. You can't stop flying.

John alluded to some of the history of digital flight control and fly by wire systems. I won't go into that. There is a long history of this in the aerospace industry, going back into the early Apollo program work and advanced through various NASA programs until the Airbus A320.

I think I have a misprint in the printed materials, but in 1984 Airbus chose to go to an all digital and redundant flight control system. That was a big change for the commercial world at the time, but they did have this 20 years of work to build upon.

The reasons for doing this, of course, were to reduce weight and costs, but also to improve some of the functionality. It improved automation with autopilot systems, advanced functionality like stability augmentation that could be implemented digitally, and then now relying on safety through redundancy.

So no mechanical or physical backups. All of the redundancy is implemented in the digital flight control systems.

Next slide shows our own version of the six feet of paper that regulates systems and software, especially in our industry, starting with CFR Title 14, Part 25 for airworthiness for large commercial aircraft. But there's a, you know, our own chain of documents that goes from the system and safety analysis level all the way down to design assurance for digital hardware and software.

The block in the middle on integrated modularity beyond X is kind of interesting, because that provides guidance for how to host multiple software that has different levels of criticality on the same hardware platform; what you need to do, what are some of the

different acceptable approaches for doing that. So we have guidance for that in our industry.

On the next slide, why does all of this work in our industry? Largely it's because as in the nuclear industry, we're a very conservative industry with a strong safety culture historically.

We've, I don't know exactly how it works in the nuclear industry, but in aerospace there is a consensus-based process between industry and regulators to develop guidance for conforming to the top level regulatory requirements.

But ultimately there is just a ton of testing that is done, and for the safety critical things, what we call Level A, there's complete transparency and visibility into all the code, all the design artifacts.

COTS software and components can be used in aircraft, but at the highest levels of criticality things like, for example we use commercial real-time operating systems in most aircraft today.

We have access to the code. That all can be examined and tested. It's not hidden from us. It's not hidden from the regulators either.

Next slide. But we, as all folks that use software, are facing a challenge. The next slide will just show us. Go ahead and hit next again, that this is a graph of the amount of software in military aircraft, and if you look, finally the last point is the F-35 that we hear so much about in the news.

We have a similar curve commercial aircraft. The amount of software that we're having to grapple with, the complexity of software-based systems is growing dramatically. There's many other

challenges that we're dealing with, as well as the use of software to do safety-critical functions in aircraft continues to grow.

The next slide shows kind of what's going -- what's happened very recently, to try to grapple with some of these things at least at the software component level.

I was involved on the committee that drafted some updated guidance, and you can see some of the things that we dealt with were model-based development, tools, object-oriented software and mathematical analysis techniques called flow methods and how to incorporate guidance for those into our software processes.

So this is the latest and greatest guidance. It's out on the street. Provides instruction on how those kinds of technologies ought to be handled. The one that I work on in particular is this last one, the mathematical analysis techniques.

Next slide, and I'll make a few comments on that, that this is nothing more than saying that for software engineering to be a true engineering discipline, we need to use mathematically-based tools to build and analyze those systems, just like we do for mechanical systems.

We build bridges; we do a finite element analysis. That's the bridge falling down in Minneapolis where I live several years ago, where somebody actually made a mistake in their analysis. So we ought to be able to do the same sorts of things, apply analysis tools to the engineering of safety-critical software systems, and indeed the state of the art allows us to do that now.

The next slide shows kind of at a glance a whole bunch

of things that we have been doing under funding, S&T funding from NASA and DARPA and other government agencies, to develop the tools, not just at the software component level but also at the system architecture level, to allow us to build accurate, generative models for software architectures, and not just test but prove the safety and security properties of those designs.

The DARPA work has primarily been focused on cybersecurity properties; the NASA work has been focused on safety properties. But together we've developed and others that work in the same area that Rockwell does, universities and other aerospace companies, have developed good tools that allow us to reason about large complex systems, to prove isolation between components when it's necessary, to analyze the fault tolerance behaviors, to actually do proofs of correctness of software-based systems.

So let me just conclude with a few lessons learned. Go ahead and go to the next one. So our conclusions are that the model-based development tools are -- have been successfully adopted by the aviation industry and used for all kinds of safety-critical software, and the analysis tools that we have are sufficiently mature and practical for application on real products, real projects and success at the software component level.

So the unit level, if you will, is now being replicated at the system level to manage the complexity of an avionic suite as a whole, and allow us to verify safety properties and to build what are called assurance cases that can be integrated with system architecture models.

Next regarding certification, certification processes change slowly because there's competing concerns of industry and regulators. But in fact, it has been possible for us to develop certification guidance for airborne software that addresses new technologies, such as those that I listed before.

This has been a joint effort between industry and regulators, and we find that case studies where you actually show what these new technologies look like, what evidence they produce, how they satisfy certification objectives are very helpful in helping people make this jump between theory and practice.

Finally, cost matters as always. Most defects in our experience occur early in the design process, indeed at the requirements stage of a system and defects are much more expensive to correct later in the process.

So it makes sense just from a cost standpoint for us to focus our efforts on analysis at the earliest stages of development, analyzing requirements and design specifications to prove them correct before we go and -- any defects turn into implementation defects that have to be corrected at a much greater cost later on in the process or, in the worse case, after delivery of a system.

Many studies have shown a good return on investment for using these kinds of analysis techniques early in the life cycle of a system. Thank you very much.

CHAIRMAN BURNS: Thank you. Professor Scherlis.

PROFESSOR SCHERLIS: Thanks. I thank the

Commission for the invitation to speak today. Regarding my background, I've spent most of my career, about three decades, working on the technical aspects of software assurance, but I also have some government experience.

Darren Cofer mentioned DARPA projects. I was -- I spent seven years at DARPA as an IPA followed by an SES appointment, and then returned to Carnegie-Mellon. This was 22 years ago, but I felt I should mention that.

My remark today focuses on prospects for software assurance, including security considerations. The theme of my remark is evidence, specifically the role of structured technical evidence to support human assurance judgments.

Next slide, please. The role of evidence was identified as early as 1968, in the first NATO workshop on software. This was the workshop where the phrase "software engineering" was coined. The aim of any testing scheme is to ensure that the customer gets substantially the software that he ordered. This was the old days, and it must provide the customer with convincing evidence that this is so.

We all know that the current generation of evaluation standards in many areas do not follow this advice so closely. The standards tend to focus on aspects of process, on system design, on test and evaluation practices. A little bit less focused on the operational artifacts themselves.

There are good reasons. I shouldn't say good; I should say there are understandable, historical reasons for this lack of

focus. My belief and the premise of my talk is that we are now at a point where we can take this advice from almost 50 years ago more seriously.

I say now because on the one hand the development of modeling analysis, as in fact Darren Cofer just described, has moved to a point. But in addition, the development of tools and data management techniques has also advanced dramatically. The development of digital systems is now data-intensive.

We have the potential, I would say more than before to get from trust to verify, where we can have a meaningful impact on our ability to develop and assure safety-critical systems that are also highly capable. There are things that can be done soon. The DO-178 family of standards is good evidence of that.

My remark is really how can we get to very high levels of capability for digital I&C and do that in a cost effective way. What's the mechanism to do that? As the speakers, everybody has noted, there's great opportunity for digital I&C.

So of course complicating this is the use of COTS components, commercial off the shelf. Also the rich supply chains that are now increasingly evident for digital systems; common cause failures, how do we define and assess diversity and security in the presence of increasingly sophisticated adversaries. Supply chain is important, especially when we have the diversity of suppliers.

Next slide, please. So I want to point out some of the software challenges we face. These apply in the general context, but also significantly for safety-critical systems. Some are less important

because we accept certain a priori constraints for safety critical. But we should recognize that we are doing that.

A general point about software. I would say for an extremely wide range of systems, software is the most significant building material of our age. Functionality is moving from physical and analog to digital for very good reasons.

But software is also the material of cybersecurity, the offensive and defensive weaponry are constructed from it, as are the assets we're trying to protect. The limits of software capability. Again as Darren Cofer has noted, derive from mathematical and not physical features.

There's a kind of unboundedness, such that as we aspire to greater levels of capability, we're very often able to get there. This up and to the right concept, which looks a lot like Moore's law but is a very different phenomenon, is going to continue through our lifetimes.

This is due to powerful languages, models, analysis, tools. But it's also due to our ability to assemble systems from components. This is why supply chain is a very important issue. Think about, for example, your mobile device. There are thousands of suppliers that contribute just to what's on one person's mobile device.

But our ability, I should say, also to do the modeling analysis to assure systems is also proceeding at a very rapid pace. It's just these two things are moving together. So there are very few categories of systems that are sort of genuinely not buggy.

Aerospace, particularly flight controls, is an exception to that because of the success of those standards. But we hold back

on functionality and capability in that context in order to meet those criteria, because software's abstract evaluation is a very different kind of proposition.

So I want to mention two other ideas on that first list on that slide. One is common cause failures. Of course we want to go after both sides of the risk product, reduce consequences through better modeling and analysis, but also likelihood through diversity and defense in depth.

The second point is continuous cyber attack. We have to recognize that, you know, we kind of focus on the network. That's where the adrenalin is flowing. It's like fire engines at the fire, fighting the fire. But really it's the fire codes; it's how we build things. It's the supply chain and insiders in fact as well that we have to focus in.

Regarding evaluation, on the slide I inventory some of the challenges of current practices. A lot of the standards help with quality, but they do not deliver quality, and you can read the list. You know, informal documents, a lot of reverse engineering, designs that are difficult to evaluate and heuristic practices.

But I want to move to the bottom of that slide, the business structures. There are many structures we've become -- to which we've become habituated in the mainstream practice. We cannot successfully evaluate a black box executable, you know, and get any kind of an assurance judgment. We need the transparency.

So if we're going to make use of COTS for safety critical, we have to gain that transparency. Again, this was discussed. And even when we have just the source code, really we're not able to

draw conclusions with confidence.

So let's go to the next slide, please. This just mentions some points of experience, related research projects, kind of analogous to Darren Cofer's slide. My point here is that the research focus is in a sense to push that tradeoff curve out, to get more safety and security with acceptable cost, but also gaining increasing capability. So this is kind of the long perspective.

So now let's move to the next chart. This is my last chart and my main point. Software development technology and infrastructure have evolved, I would say, to a point where we can do things in a different way.

There's a timeliness argument that I'm going to make. There are a lot of ideas that have been around for a while, but because of the evolution of the technology, including models, analyses, the treatment of data from development practices, we are able to take these ideas seriously.

The idea is to contemplate the creation of what we could call chains of evidence to support assurance claims. What I mean is an explicit linkage of dependencies that connect the models and the analyses and all the various -- the test cases and all the various other artifacts related to a system.

This linkage, even back to requirements and the safety and hazard analyses, can help us make that assurance judgment much more efficiently.

So as we build the systems, as we advance this development of evidence to the earliest stages of development, we

create an opportunity to make the evaluation process much more efficient, and therefore to enable upgrade and evolution, recertification also to be efficient.

Really what is contributing in a great way to this is the increasingly expressive models and evaluation methods, analysis methods that focus on software artifacts. Code obviously. The Google repository has a billion lines of code in it, tens of thousands of transactions a day. Virtually every transaction is recorded back through the fullness of time.

This is standard practice for the smallest through the largest software development teams. That's code configuration. The opportunity is to link in the models and the analyses that many of us are involved with, that pervade the DO-178 community, and to link those in with hazard and safety models and analytics, and create those dependency linkages and rationale structures.

In the past, many of these models and data were lost. They were in people's heads. They were on white boards. We pay a high price in reverse engineering to recover this. The big change is now we can express these efficiently and we can do analyses on that basis. Thank you.

CHAIRMAN BURNS: Well thank you all for your presentations. I'll start off with a few questions. I guess in terms I'll put first to 60 percent of the panel I guess, Mr. Coward, Mr. Connelly, Mr. Harmon, I'm trying -- in trying to understand some of the industry concerns, the nuclear industry concerns with where we are or where we might be going with digital requirements, but also it strikes me the

concern is not only the potential for a particular rule that we have before us, but it's also a question about disconnects, if you will, between where the existing framework is.

For example, and Mr. Coward you talked about the 50.59 process, where is that -- how has that divergence come up, because I think you said, talked about in 2010 we thought we were sort of at the same wave length, but that's sort of grown apart.

Where are the biggest push points or pressure points in this needing to gain a sort of more common perspective?

MR. COWARD: Well I guess what I'm going to do is I'm going to defer to the guy who is nominally responsible for these, to give a better -- I could comment, but I'll let John give a few specific examples.

CHAIRMAN BURNS: Okay.

MR. CONNELLY: And feel free to jump in any time you'd like.

MR. COWARD: I will.

MR. CONNELLY: Common cause failure. That's current, you know, what we're currently working through right now for the NEI-101 task force.

You know, trying to understand or getting a common sense of understanding in terms of what are the initiators for common cause failure; what are the appropriate mechanisms for mitigating common cause failure? How do those translate into the designs that we're implementing?

Trying to get a common frame of reference, if you will,

for you know, what is the right way to deal with software or all forms of -- including software, all forms of common cause failure.

MR. COWARD: And I think a lot of it, Commissioner, Chairman, is there's different ways to look at this. Part of the challenge is we're talking about the application of -- by our standards new technology into these plants, right?

The rest of the world chuckles at us when we say that, but we're talking about the application of new technology and there's always going to be lessons learned and things that come up, where you -- from doing this one, the next one you're smarter and then you're smarter, then you're smarter.

I think one of the things that's happened is especially when you look at people considering safety-related projects, as well as some of the bigger non-safety related, all of us together haven't been as good as we could have been, at really, truly understanding those lessons, and quite frankly getting the kind of stream of projects that allows all of us to have some momentum as we're going forward.

You know, one of the ones we point to a lot is a plant that decided to do elements of digital upgrade in their feedwater system. That's not just the software, but some of the components, and through the process someone said hey, we can make this even better and not just control this glass, but we can control this glass and we can control this book.

That was a great idea, and they probably did a good project. But what they missed was they took a glass, a book and whatever my other prop was, the other glass that previously were three

independent, separate devices and connected them together in a way that even though it was a non-safety related project, and the --

I'll call the posture of the people doing it was to think this is just a balance of point, secondary system, non-safety related project to replace analog controls with digital, they created new potential failure modes that could affect multiple components at one time, and actually introduced some pretty good 50.59 questions, all right.

But because we didn't have all of us together, because we haven't had the stream of those projects going to learn together, and to share the lessons and to feed that back collectively together, it was a one-off, as opposed to occurring in a way that we all can embrace it.

So there's a lot of factors going on here, if that makes any sense.

CHAIRMAN BURNS: The part of it that's curious to me is whether -- and you touched on it -- the artifact in terms of the development over the years. I'll give you a personal example.

A representative, a company that also builds nuclear plants or designs nuclear power plants, but also does refrigerators, and it's not Westinghouse --

(Laughter.)

CHAIRMAN BURNS: -- basically told us when we were having some issues, they said, well, you don't have a refrigerator. You have a digital device. And it's very true. And he says, the problem was the software, it needed a software upgrade whereas you don't have -- and I'm wondering is our -- is the lexicon we use in terms of

regulation which was developed in -- I won't call it a pre-digital age, but in an age where it's more analog than it is digital?

There's something of how we talk about safety-related, important to safety, other things like that, doesn't quite fit.

MR. COWARD: I'm not sure if this is going to specifically answer your question, but I will tell you I do believe that the way we talk is a consideration. Because there are -- I like to use the phrase we've ended up using some interpretable words and some interpretable phrases.

And instead of having -- over the years there's been a number of instances where instead of having crisp, clear, rigorous three-way communication to confirm that what I just said to you, that you have the same exact meaning, understanding of it as me?

I say it, you nod your head and say, yeah, I agree with that. And we walk out of the room. We're convinced we just agreed, and the reality is we're like this (indicating).

And there's a cumulative set of a number of those over the last number of years, the last several years in particular where in the end, you know, people are excited about doing these projects. I mean, these are great, valuable, important projects that go to the basic infrastructure of our industry, our assets and the ability to continue to generate the important power we need and for this industry to be successful and to do it together.

So, people get excited and there's a tendency to just go. And it isn't, you know, and it isn't until they realize somewhere downstream that, oh, that touch point we thought we had at the

beginning, we didn't.

And I think -- I'm not sure if it was Darren or Bill, but one of them pointed out when you find those conflicts at the back end, they're a whole lot more disruptive, costly and distracting than they were up front.

And what's been happening -- again, I'll go back to my perspective more as the industry leader than the I&C guy trying to implement one of these projects. If I'm making a decision to do this, it's an expensive project, it's a potentially disruptive project, but very beneficial, you know.

When I see the collateral damage that a lot of these projects occur, when I see that, you know, at the, you know, four-lap race and on the third lap all of a sudden you have to add three more laps and the cost goes up and the schedule goes out and the next thing you know we're going back and forth to Rockville left and right, you know, just, you know, I'm not getting, you know, as long as my guys can keep buying stuff on eBay and Craigslist, I'm going to keep doing it.

And what I know is I know that we've just about exhausted that. And I know that, you know, my -- I apologize I got to four, you know, personally speaking one of the things I worry about a lot is the future of this industry is the people. All right. We need great, young, strong, technical people coming into this industry.

You bring the young people into these plants and they just look at you like what planet are you from? All right. You know, it doesn't excite them and they don't even know how to work with the stuff. The number of people left who can even work with these

systems is going down.

And I think you put all these things together, you throw them into one salad bowl, the kinds of thinkings or the kinds of attitudes that result all in good conscience, all with good intentions, we've been working in a way together where everybody is trying to do this and we're stubbing our toe enough.

And the executives who are watching us see the blood on the floor and they say, I want you to stop bleeding on the floor. And the best way to stop you from bleeding on the floor is to tell you to stop running.

And we need to collectively demonstrate to those decision-makers, all of us together, and I'm sure we can, that we can jog around this room without stubbing our toe and bleeding on the floor, and we can make these assets more valuable and improve safety and improve reliability. I'll stop.

CHAIRMAN BURNS: And sort of in that context, I'm going to turn to Professor Scherlis and Mr. Cofer, you talk a bit in the context of the airline industry and some of the transition there, but the evidence chain, you talk about evidence chains.

I mean, one of the difficulties I think for the regulatory -- a regulatory framework, and it's whether it's us, pharma, airlines, et cetera, is regulators to some extent are reactive. They are pro -- and they are proactive, but oftentimes reactive.

So, we're creating frameworks and certainties about a certain -- in some aspects, but what I'm hearing is that you in terms of the development and innovation that's going on and the rapidity with

which it occurs, there is somehow the balancing of understood criteria and flexibility for innovation that is good. The good type, if you will.

And I'm trying -- anything else you would like to add in terms of how do you do -- how do you achieve that kind of balance? How is it you are, in effect, allowed that innovation or in terms of doing that kind of testing, that kind of evidence chain building, if you will.

If I've made myself clear or coherent or -- I know it's --

DR. SCHERLIS: No, I think I understand your question, and there is a kind of a dilemma. On the one hand we want to avoid framework of standards that is over-prescriptive with respect to either the process that's followed or the structure of designs. But on the other hand, and, in fact, this goes back to Robert's remark, the earlier we engage with certain issues, the better.

And there's data, for example, from NASA some years ago with respect to software defects that shows that the difference -- if you find the defect shortly after it is injected, all right, the difference between that and finding the defect later in the life cycle is orders of magnitude of cost.

And when we talk about commercial software, it goes beyond that. Because once it's deployed, the cost of update is very high just to test. More than 200. And there's several studies that were done that kind of reinforce those numbers.

So, on the one hand we want to avoid over-prescription. But on the other hand, we want to make sure that in a development process the modeling and analysis and evaluation is done as early as possible.

And so, one of the reasons why the idea of evidence is appealing, is that we -- you could say it -- levy on the developer a requirement to produce the evidence along with the artifacts that will actually be executing in situ, but that evidence makes the evaluation job straightforward.

So, in a sense, we say to the developer within a very broad framework of criteria, here's a body of evidence and the argumentation to support it. And then you can come to an evaluation judgment confidently and quickly.

And the advantage of that is as systems evolve, the incremental cost to update the system, for example, for changing infrastructure or changing functionality enhancement, whatever it is, that cost goes down, but we still have to live with that dilemma of how much prescription.

And I don't think that there's a necessary tradeoff. I think we can be creative about what's the nature of the framework. This has been done, for example, with respect to security practices.

There's a security development life cycle developed by two Microsoft people more than a decade ago. It's called the SDL. Very widely adopted and it's really a framework of what practices to engage in at what stage of an engineering activity, but it's not prescriptive with how we actually conduct the engineering activity or how we design the systems that are being engineered.

DR. COFER: This tension that you mention between innovation and regulation, it was very much in play when we were doing our update to the DO-178 documents. The previous version of that,

version B, was published in something like 1992.

So, I mean, between then and when we did the next update starting in 2006, there's a lot of changes in the software industry that had to be addressed.

And in that committee involving both industry and regulators from Europe and the United States, FAA and EASA, the folks that have to receive this evidence from applicants and industry are asking how can I possibly review this material, because I haven't been trained to do this. How am I going to get my head around that?

So, one of our jobs in updating these guidance documents was to try to reach a common language for all of the different objectives that needed to be satisfied so that both the regulator and the applicant could point to the same piece of paper and say, okay, I understand that for this new technology, new-ish technology, this is what the evidence in satisfying this objective might look like.

And so, again, not being prescriptive, but trying to say this is -- this is what you should expect to see from an applicant if they are using this kind of tool, this kind of technology to claim that they're satisfying this objective. So, that's one thing we've done.

Indeed I think there is going to have to be some amount of education on the part of the regulators to come up to speed on some of these new technologies. And, again, these pilot studies, case studies that I've mentioned are also helpful.

CHAIRMAN BURNS: Okay. Thank you. Thanks very much. I appreciate the indulgence of my colleagues. Commissioner Svinicki.

COMMISSIONER SVINICKI: Thank you, Mr. Chairman. And thank you to all the witnesses for their presentations today. I find this conversation very valuable.

I think it's interesting to reflect on some of the history. I joined this commission in a time in which it had been meeting as frequently as every six months on this topic of digital instrumentation and control. And it's interesting to look at commission expectation, if you will, and direction to the NRC staff from 2007.

This commission said the staff should proceed with the timely implementation of NRC's digital instrumentation and control project plan and the issuance of interim guidance recognizing that the staff will continue to work with the stakeholders to refine the guidance, to address the existing issues within each of the six working groups, and to risk inform the regulatory framework for digital I&C.

I'm sure as they issued that direction they felt they had it all tied up in ribbons and bows. As we wind down to year 2015 and, you know, get close to within 18 months of when -- the ten-year anniversary of that direction to the NRC staff, it's interesting to go back even further to a policy paper written to the Commission in the year 1993.

So, let's go back 22 years and the staff was talking about an issue we just talked about today. I'm sure it felt just as contemporary. Defense against common mode failures in digital I&C.

In 1993 the staff wrote recently, so you have to remember again this was 22 years ago, increased attention has been given to detailed assessments of the integrity of software applied to

safety-critical functions. These assessments have covered a broad range of applications including computer-based medical treatment facilities, computer-based fly-by-wire aircraft control systems and nuclear power plant protection systems.

The staff found a consensus among computer science and software engineering experts that such safety-critical applications should be backed up by some system not based on software.

The experts base this opinion on the facts that the quantitative estimate for the reliability of I&C systems based on high-integrity software cannot yet easily be determined.

And Professor Scherlis is laughing at this, because it seems in your field 22 years ago it's ancient history.

But, you know, as I sit here today and we have representatives who have spoken to aviation, there's been mention of pharma and pharmaceuticals and the medical community, I sit here as a part of the nation's nuclear regulator saying, well, in '93 the staff assessed that all these sectors were in the boat together.

It's my observation that these other sectors, medical technology, we may not be in that profession, but we're pretty much all patients. I'm looking at the age demographic in the room. We're all patients now. So, I find -- I don't find a lot of analog anything in a doctor's office or a hospital setting. So, they passed us by.

And as one of millions of Americans who will next week get on an airplane to spend holidays with family and friends and loved ones, the quality of my colleagues' work at the FAA matters a whole lot to me as I enter that small metal tube and get flung through the

atmosphere.

So, I'm assuming that the quality -- nuclear is special, we say that around here a lot, but it isn't so special that it can just lay itself aside from solving the problem of 1993's paragraph.

So, my one question to anyone, any soul brave enough to answer this question is, you are the doctor and we are the nation's nuclear safety and security regulator. I bring you in. Diagnose for me why the others, you know, moved past this issue and we have not. And then prescribe the cure for me on that.

And I know for those of you in nuclear business, this is touchier for you to be honest about this one, but I'm wondering -- and please opine whether is it fundamentally a mindset and a paradigm shift? Because I do agree and have had plain talk with the NRC staff that if you view digital's introduction as introducing only vulnerability and no benefit, your inclination as a safety regulator will be to write the most prescriptive regulation.

And I would, you know, postulate to you that in the paper that Commissioner Ostendorff and others have talked about on IEEE 603-2009, the conditions in there represent the instinct of safety professionals to say I prohibit whole sets of types of systems architecture, I prohibit in its entirety two-way communications between certain types of systems.

That is my inclination if all I care about is safety and not generating megawatt hours or anything else. So, but these other groups conquered that instinct somehow.

These other regulators conquered it. What did they

do?

MR. COWARD: Can I comment on that and tell you why?

COMMISSIONER SVINICKI: Yes.

MR. COWARD: At NPR, about seven, you know, I think most people know NPR was founded by the three chief guys working with Rickover. So, we've always been primarily a nuclear energy company. We remain a nuclear energy company. About 70 percent of our business is nuclear.

About 20 percent of our business is for the medical device community, the medical -- doing medical product development. Some other time I can tell you how we ended up there.

But as president of NPR, I have oversight of that as well and I tend to go to some of their industry meetings and meet with other executives. And I tell the story all the time about how if you look at that industry, heavily regulated, heavy quality programs, they put stuff in people, all right.

And you go to their meetings and all you feel in the room is a spirit, you feel it, of the innovation, the moving forward perspective. They have figured out within the context of a heavily regulated industry with rigorous and onerous quality programs, they have figured out together how to move forward.

We're doing at NPR right now, we are designing for a customer an artificial pancreas. One of the first, all right. It's software-controlled, all right.

There are times when it seems like the expectations

and the rigor and the requirements and the burden, it's more of a feel than it is the paper, the feel for how to do some non-safety-related MSR controls in a nuclear power plant -- I'm not putting down an MSR, but the non-safety-related MSR controls in a nuclear power plant feel like they carry a heavier burden than doing the software which is going to control this artificial pancreas that if it goes bad for five minutes, it will kill somebody.

And I think that my comment to your question is, and it's a place where all of us can work together on the vendor side, the licensee side, the regulator side, the opportunity we all have in front of us is to revisit and work on our culture and to not let the pursuit of perfection prevent us from making progress.

Because I personally believe we've wondered into a place where the pursuit of the perfect digital I&C platform and system in a nuclear power plant has led us to leave the existing systems in the plant and actually increase the risk right now.

I believe numerous -- I'm not saying unacceptable risk, but I think the overall risk right now is actually higher than it would be if we replaced the systems.

And I think we have to overcome together, the leaders of the industry, that cultural barrier that says we have -- we're nuclear, it has to be perfect.

And I'm not saying accept less than perfect, but what I'm saying is we have to convince ourselves and those around us that it is okay to move forward if it's going to make us better.

COMMISSIONER SVINICKI: Thank you. Would

anyone else like to comment? Particularly those of you from maybe more outside the nuclear industry.

DR. SCHERLIS: So, let me try this. And I think Darren may have more authoritative comment on the first part of my remark, which is maybe partnering with other safety-critical industries would be helpful. Aerospace embedded medical devices and NASA, for example, which has similar issues more focused on reliability.

The practices that are emerging in those industries, the kinds of models, the kinds of analyses, the technical means, the tooling, all that's to advantage. And as part of that, promote innovation.

That could mean partnering, for example, with some of the NITRD agencies. NITRD is the Networking and Information Technology Research and Development Coordination Activity out of the National Science and Technology Council, which involves about a dozen agencies who are all involved in investing in technical innovation related to IT and networking.

Partnering with them as a kind of a receptor of their technologies to do pilot projects could be very helpful and at least getting an understanding of what's possible and where things might go.

But on the other hand, I think it's important to kind of stare down some of the existing industry norms in a COTS world, which are really adverse.

If you look at a license for a typical COTS product, it really has two provisions. One is it does what it does, and it doesn't do what it doesn't do.

COMMISSIONER SVINICKI: And it doesn't start on

fire like those hoverboards.

DR. SCHERLIS: Right. It's as is. It's as is. The license actually has those two words in it, "as is." And the second is don't look, which is to say you may not do penetration testing or any kind of activity that may look like reverse engineering.

This is the norm for many licenses in the world of COTS. And that's a challenge if we want to embed those things, because then we have to make special relationships with those vendors.

And so, we've become habituated in a sense to accepting the presence of a large number of defects, but that's not a universal fact. There are many systems where we really achieve an extremely high level of quality and we're able to assess that pretty well.

And so, I think the idea on the one hand partnering, and the other hand sort of actively engaging with the innovative community as a client. People get excited by the applications and the challenges and create a kind of innovation culture.

That doesn't mean that those innovations are going to kind of transition right into the current set of systems, but at least we get a sense of, okay, as we look towards the horizon, what's the right vector for us to be on and how can an understanding of that vector and participation in that process help guide rulemaking in a way that will make more opportunities available to the industry so that the kinds of things that are happening with medical devices that Robert just described are possible for digital I&C.

COMMISSIONER SVINICKI: Well, I'm over my time.

So, I'll leave it to my colleagues to pick up on the thread of that if they're interested. Thank you.

CHAIRMAN BURNS: Thank you. Commissioner Ostendorff.

COMMISSIONER OSTENDORFF: Thank you, Chairman. Thank you all for your presentations. They were very enlightening and extremely helpful for us.

About a year and a half ago I went to visit a nuclear power plant in Region II. I'm not going to mention the plant, but basically the chief nuclear officer for this fleet told me that because of regulatory uncertainty he was directing his staff not to proceed to go from analog to digital automatic voltage regulator for emergency diesel generator.

A few months ago I was visiting a plant in Region I and I was dismayed when the -- it's an operating plant and the plant manager told me that, yes, I asked him to show me signs of where you're upgrading your instrumentation. And he said, well, Commissioner, we're upgrading this. I've directed my engineering staff to go reverse engineer this existing analog component to build a new analog component. That was not an encouraging message.

Earlier this year in March 2015 during our annual Regulatory Information Conference, I sat on the industry and staff group along with John Thorp over there. John was in there from NRR.

There was about 50 or 60 people in this room. Steve Arndt was in there from NRC staff and there was others I'm not able to put my eyes on. And our staff, I think, was pleading for industry to

submit some more pilots, examples, upgrade requests to the NRC to give us some more run time to demonstrate success.

And it was not a warm and touchy-feely atmosphere on that topic. And a lot of hesitancy to do that because of prior experiences.

And I appreciate, Robert, your comment that, you know, you think some of the misinterpretation and some of the staff versus industry assigning different meanings to the same phrase, et cetera, not assigning blame to anybody, any organization, that's not constructive.

I support your comment that, you know, I think I support it where our staff has been. Send us something to do. Send us something to look at here.

And John Lubinski there who we'll hear in the next panel, is nodding his head. But I worry that without a commitment to some contextual example, you know, these kinds of components that have some nuclear industry applicability that there's an interest and incentive to move forward on that creates a lot of interest, I don't see us getting any -- making much progress. So, how can industry and/or staff work together?

And I'll also note the -- you got a roadmap, NRC's got a roadmap, they're not the same roadmap. There needs to be some convergence there to work towards some common outcomes that industry and staff can agree to. So, I'm going to stop there and let you guys comment.

MR. COWARD: Yeah, I think just a quick comment.

I think we have talked a couple times with your staff. And I think even if we don't end up with one roadmap, I think the vision is to end up with collaborative roadmaps that will feed off of each other and work together.

And I think the challenge to us, and this is the challenge to the NEI working group, the challenge to your staff from the chief nuclear officer meetings I've been in, I think there is a long list of people eager to submit the second application.

COMMISSIONER OSTENDORFF: Okay.

MR. COWARD: You know, they're waiting for someone to pay to learn the lessons. And what we have to figure out together is how can we give someone the comfort that it's not going to be as bad as he thinks and it's worth the investment and that everyone will be responsive together and get it through in a way that it's successful for that plant and the others that will fall in right behind it. And that's part of the theme of our roadmap.

COMMISSIONER OSTENDORFF: Well, I sincerely believe NRC staff wants to receive these applications. I know they do. And so, they're anxious and eager to work on it. They seem to be given an opportunity.

Did you want to say anything, John?

MR. CONNELLY: I did. So, we have had discussions about the roadmaps, both the NEI roadmap and the NRC roadmap, and they're not inconsistent with each other. I mean, there are large degrees of continuity between them and obviously we'll have to -- there will have to do some adjustment or refinement there.

You kind of alluded to it earlier that -- I can give a representative example. So, when faced with -- in the Westinghouse world, the pending obsolescence of solid state protection system circuit cards, okay, there's kind of a fork in the road there.

We could go down the path of a full-blown digital upgrade similar to what Oconee did, or we could go with fit, form and function upgraded cards by the OEM.

They were -- the initial system or the original construction system was highly reliable, has proven for decades its high reliability, but the newer circuit cards were even better and addressed obsolescence issues.

So, to my knowledge every licensee in the United States elected the path of in-kind upgrades versus a large-scale modernization project just because there is very -- it's a very low-risk profile.

I think what you're alluding to is, you know, we'd like to see more of Oconee-like projects. But until we have some run time with the processes and people can feel more comfortable about the risk profile that attaches to that, it's not likely that licensees will be, you know, that we will be submitting projects like that to the staff. It's just -- it's a -- we're a naturally risk-adverse industry and rightly so.

COMMISSIONER OSTENDORFF: Okay. I'm just going to make a comment with you, John. Your Slide 2 that shows the historical performance for digital feedwater turbine controls, that was extremely helpful.

And I'll tell you I was talking to a couple of the

commissioners here in advance of this meeting and I don't think I've ever seen that kind of an articulation of a safety benefit. And I think it's very helpful for us to be able to see, because it helps put it in the broader context.

And I think Commissioner Svinicki hit this point earlier about how do we look at the overall safety benefit, not just is this independence attribute or this common cause failure attribute met in a more compliance method, but what are the benefits of this. And so, thank you for bringing this to the table.

MR. CONNELLY: You're welcome.

COMMISSIONER OSTENDORFF: Daryl, I thank you for you presenting dual-hatted Westinghouse and IEEE. And I've got about eight questions for you all. I don't have time to deal with all of these, but let me just ask you a couple of them.

MR. HARMON: Okay.

COMMISSIONER OSTENDORFF: When is the next update due for IEEE 603?

MR. HARMON: I think the -- as I mentioned, the working group currently has a PAR. They started work on it this year. The -- I think the expectation is that it could be issued in early -- or sometime in 2018. So, that would be the next issuing of the standard.

COMMISSIONER OSTENDORFF: On your Westinghouse hat --

MR. HARMON: Okay.

COMMISSIONER OSTENDORFF: -- you obviously do a lot of business overseas.

MR. HARMON: I do mostly overseas.

COMMISSIONER OSTENDORFF: Yeah. So, how would you characterize the high level of the different regulatory requirements for digital I&C for existing nuclear power plants or new plants between what you're seeing overseas and what the NRC is being requiring?

MR. HARMON: The two -- the experience that I have overseas is primarily in South Korea and now in the United Arab Emirates. Would say KINS in South Korea quite closely follows what the NRC does, how they use IEEE standards.

South Korean regulations are also based on IEEE standards and I would say they relatively closely follow what the NRC does.

In the UAE it's a little unique because FANR is a new regulatory organization. My experience so far with them is that they have regulators from many diverse backgrounds. It's like the, somewhat, the United Nations in FANR.

So, they have some different perspectives. Some certainly U.S.-based and it's still IEEE-based primarily, but there's other perspectives that are brought to the table. So, I would say they may be a little more diverse in terms of their regulatory perspectives.

We're a little bit, you know, we're still early in the UAE nuclear industry. So, may be a little hard to tell.

COMMISSIONER OSTENDORFF: Okay.

MR. HARMON: Does that help?

COMMISSIONER OSTENDORFF: It does. Thank

you. Last question for our two final witnesses here. The general context, you know, from your experience in your respective communities and I think really adds a lot of value for us to hear how others look at these issues. So, thank you for doing that.

Testing and evidence, how should we as a regulatory body use the existing digital instrumentation control experience, some of which was highlighted on John's slide for feedwater and turbine control, how should we use that as evidence to look at things such as common cause failure or software failure modes?

Run time, you know, years of experience, reliability-type studies.

DR. COFER: Yeah. So, this is -- it's somewhat of a religious debate in how you assess the reliability of --

COMMISSIONER OSTENDORFF: That's why I asked the question.

DR. COFER: -- software. And in terms of my denomination in that particular argument, I don't believe in treating software probabilistically, because it's not. It's pure design. It doesn't behave probabilistically.

That doesn't mean to the -- it's affected by its underlying hardware, its inputs which are probabilistic. And so, we have -- we can -- if we can, you know, make that distinction between software, which is pure design just analogous to a mechanical design, and then the underlying physical process is that influence, then that gives us a basis for having a proper science of reliability.

That being said, there's different approaches to how

you deal with software common cause failures.

In our industry, we have typically relied on diversity so that it -- but it varies a lot depending on the regulatory organization, even which FAA office is doing the certification, the OEM, the airframer, the manufacturer of the equipment. Everybody has different ways of doing things to try to show that they're safe, but ultimately they have to perform a safety analysis as you would in your industry to demonstrate the required reliability.

But it is very common to if you have two cross-checking channels, to require different microprocessors so that the executable then is different and you have some assurance hopefully that will fail in different ways.

That said, there are also studies that show that if you build things from the same set of requirements, you can end up with the same errors being programmed in. So, it's not a magic silver bullet in any sense.

And there's also others that have shown that you would be better off focusing all your attention to develop one piece of software, one common piece of software for redundant channels that you put all of your effort in and you have the highest level of assurance in rather than splitting that effort into multiple development efforts and possibly having errors in those redundant channels.

I don't think there is a conclusive answer to that yet. Personally I think because of the tools and methods that we have available to us now, I would lean towards trying to make sure that the software is -- you focus all your attention on the one software, getting

the software right and then probably having some degree of architectural dissimilarity where you might have a separate sensor, a separate backup to try to cross-check it.

I'm not sure if that answered your question, but --

COMMISSIONER OSTENDORFF: I appreciate that. Dr. Scherlis, do you want to add anything there?

DR. SCHERLIS: I agree with what Darren has said. There's a danger in applying probabilistic models and doing Bayesian arithmetic on software components, but the environment in which the software operates does have physical characteristics.

And so, the software is responding to the models -- the software has got to be designed, rather, to respond to the way we understand the models, the environment and, in fact, software is discontinuous.

There's a famous old story, an old, old NASA story in a Fortran program, a period which was supposed to be a comma. And on those old line printer outputs, it's kind of hard to tell the difference and that fundamentally changed everything about how that code operated.

So, recognizing that and building the models and then building the software to respond to those models, that's Point 1.

Second is with respect to diversity it is a hard problem. I agree with what Darren said. You can look at lots of different dimensions of diversity, the algorithms, the choice of language, the choice of infrastructure and tooling, the hardware, the people who do the development.

But if they're building to the same spec, and this is an old result, then we don't get as much variance as we're looking for. And so, really play to both sides of the risk product, really work hard to get the instance correct.

And that may mean pushing simplicity into the design in order to get that and getting enough evidence and doing the mathematical reasoning. That's kind of where we are, as I understand, with flight controls to a great extent. But if we do go diverse, let's do that kind of multi-factorial analysis of all the dimensions. Make sure we understand how to get as much dimensionality as we can and then try to define measures within those dimensions.

There's no -- I don' think there's a simple answer to this question of CCF, but I -- it's not an impossible problem either.

COMMISSIONER OSTENDORFF: Thank you. Thank you all.

CHAIRMAN BURNS: Thank you, Commissioner. Commissioner Baran.

COMMISSIONER BARAN: Thanks. I want to start off by thanking Dr. Cofer and Dr. Scherlis for being here. It's really helpful to get a broader perspective.

You know, there are some issues we have here that are really truly exclusive to the nuclear sector, but digital instrumentation control really isn't one of those issues. And it's something that other industries where safety is critical have grappled with. So, it's very helpful to get that perspective.

Let me turn to this side of the table though for a minute

and ask -- I want to focus a little bit on IEEE 603, the standard and the conditions that the staff has added to the original standard and get a better understanding of the views and concerns about those.

So, as Mr. Harmon pointed out, this was an industry consensus standard, the core standard was. I want to just make sure we're all kind of on the same page in terms of understanding how much of the concern you all have expressed about where that proposal is now is related to the conditions.

I guess another way of putting that is does everyone -- does NEI, does Exelon, does Westinghouse, would you all support incorporating by reference the standard if their conditions weren't fair?

MR. COWARD: I believe the answer is yes.

COMMISSIONER BARAN: You would support incorporating it without the conditions.

MR. HARMON: I would agree with that, too. What's been expressed to me is most of the concern is with the conditions and going beyond what the standard imposes or has for criteria.

MR. CONNELLY: As would we. The only concern that I would express is that, you know, because there is this large sea of standards, that introducing yet another change into that environment may ultimately be counterproductive, you know.

We're probably better served to iron out these major issues, you know, the application of 50.59 dealing with common cause failure and so forth, get those issues ironed out before we introduce yet another variable into it.

COMMISSIONER BARAN: Well, let me follow up on

that aspect of it, because I was interested in that point when you made it originally in terms of, you know, trying to get our arms around a lot of issues here. Can't we just hold this constant while we work on these other things?

And I'd like to get your thoughts on this, which is, you know, we've talked a lot about innovation, how much things have changed, and those standards are from 1991. The standard is 25 years old.

Isn't it outdated? Don't we need to update the standard? Can we really -- can we really afford to hold this variable constant and have it use a standard that's 25 years old?

MR. HARMON: Well, from the IEEE's perspective, we did approve a standard back in 2009. And again we're working on it now. Certainly a 25-year-old standard with the way technology has improved could have some question.

Although it is a fairly high-level standard in terms of safety system criteria, it would seem the 2009 standard may be better suited and there's still improvements.

Some of the things we've learned from the rulemaking activity that are now being factored back into IEEE 603 that will be the next standard, but it would seem that one might want to move forward.

I'm not as familiar with the 50.59 aspects and other possible influences or things that will happen to the overall regulation that --

COMMISSIONER BARAN: Well, let me ask about this: In terms of the conditions that the staff have added to this and are

proposing, proposing to propose, my understanding is that several of those conditions are currently in existing guidance that we have.

So, these aren't, for the most part, new expectations. Some of this is moving things from current regulatory guidance into regulation.

First of all, do you think that's an accurate characterization? And if so, what's the concern about, you know, kind of the same expectations being shifted from guidance to the regulation?

MR. COWARD: Let me start and then you please fix me. I think the spirit of your comment or question is on track. I think part of it is what is the right place for the existing guidance to land and what is the right forum to put it in, what is the right kind of document, what is the right use?

And the potential to set what a number of people in the industry think would be sort of some bad precedent, that they just don' think it belongs where they're trying to put it, you know, that's a big part of it.

And I think the other big part of it is the, you know, all of us in nuclear tend to be fairly clear, logical thinkers with a heavy technical bend. And the idea of ending up with what are essentially different criteria for Byron or the plant that might get built at Turkey Point, just doesn't seem to make sense to us.

COMMISSIONER BARAN: Well, let me follow up on that just for a second, because this is one of the points that was made, which is there's a concern about having a different set of requirements for existing plants and new plants.

But in our regulatory framework we have several areas where there are requirements that differ for new versus existing plants, probabilistic risk assessment, severe accidents, management guidelines and other things where it's not the same.

Are they really similarly situated in this case? Is there really a problem with having different requirements for existing plants and new plants that you factor in kind of the ability, and maybe this is an oversimplification of, you know, designing around some of these problems for a new plant.

MR. COWARD: And I think that our perspective would be along the lines of we agree there's numerous areas where you're going to have different requirements and different processes. This isn't one of them.

COMMISSIONER BARAN: Okay.

MR. COWARD: This is sort of core, underlying, basic design philosophy that we would expect to be the same everywhere.

COMMISSIONER BARAN: Going back to kind of the conditions and whether it's more appropriate to have some of these concepts in regulation, some of the concepts in regulatory guidance, I get the sense, and we'll have a staff on the next panel, we can explore this, that part of this is a disagreement about, well, how do you have greater clarity in the requirements and greater regulatory certainty.

And you read the staff paper and their view is, well, you wanted greater clarity. Here it is. We're putting conditions in the regulation. What can be clearer than that?

But I take it that your view is, well, having that kind of

level of detail in the regulations isn't -- doesn't result in regulatory stability or certainty. It's something that would be an obstacle to improving the -- improving the licensing for digital upgrades.

Can you talk a little bit about that? Why is there this disconnect about the level of specificity that should be in the regulation versus in the guidance? And why is additional specificity in the regulation?

If it's performance-based at least, why is that an obstacle to progress in this area? That's a lot all in one question, but, you know, it's kind of a general theme, I think, here.

MR. HARMON: I think one of the things that at least we see is that the Code of Federal Regulations is typically technology neutral. It doesn't specify implementations.

Some of the conditions I think such as hard wiring certain signals, the one-way communication as opposed to defining criteria for data communications and when you could have bidirectional communications as previously specified, I think those are the things that kind of react to and believe that those may limit us and make it more difficult to implement some of the solutions we're trying to implement.

COMMISSIONER BARAN: So, from your point of view, and we'll get the staff's view on this, too, some of these conditions aren't really performance-based, they are prescriptive from your point of view and it's going to limit particular technologies.

MR. HARMON: Yes.

COMMISSION BARAN: Okay. I think I'll stop here.

This is helpful. I've gained a better sense of the views and the concerns about this and it's good for kind of starting discussion with the staff on the next panel. Thanks so much. Appreciate it.

CHAIRMAN BURNS: Okay. Thank you, Commissioner. I want to thank again the panel for their presentations this afternoon. It's been very rich discussion. And with that, we're going to take a break.

Let's reconvene at five to 3:00 and we'll hear from the staff panel at that time. Thank you.

(Whereupon, the above-entitled matter went off the record at 2:48 p.m. and resumed at 2:57 p.m.)

CHAIRMAN BURNS: We'll come back to order.

I would ask folks in the audience, I feel like I'm at the theater, but to silence your cell phones and electronic devices, particularly appropriate since we're talking about digital things today. But, I've heard a couple of them, ring-a-ding-dings today, so if you would do that, I would appreciate it.

We'll proceed with the second half of the meeting, the presentation of the staff who will provide background on NRC Digital Instrumentation and Control Activities including recent lessons learned and we'll discuss the proposed rule that's in front of the Commission and incorporate by reference the IEEE 603-2009 Standard and other issues that may be relevant to this topic.

So, I'll call on the Executive Director for Operations, Vic McCree to begin.

MR. MCCREE: Good afternoon, Mr. Chairman,

Commissioners.

We're here this afternoon to discuss our efforts to continue to improve the licensing of digital instrumentation and control systems for commercial nuclear power plants in the United States.

We'll discuss the proposed rule currently before the Commission to incorporate by reference the IEEE Standard the 603-2009 into the NRC's regulations.

We'll also provide the Commission with a summary of other key activities that we are pursuing.

The NRC is a learning organization and we're focusing on addressing emergent challenges in the area of instrumentation and control technology.

We're committed to ensuring safety while achieving a stable, consistent and predictable regulatory framework consistent with our principles of good regulation for use of digital instrumentation and control systems.

With me at the table today are John Lubinski, Acting Deputy Office Director for Engineering, Office of Nuclear Reactor Regulation, to his right, Richard Stattel, Senior Electrical Engineer also from NRR, to our left, John Tappert, the Director of the Division of Engineering, Office of New Reactors and Deanna Zhang, Senior Electronics Engineer, also from the Office of New Reactors.

Next slide, please?

I'd like to note that our presentation today has a deeper level of detail than our normal presentation at Commission meetings, but it's in an attempt to be responsive to the questions that I know that

you're interested in hearing us respond to.

We will begin our presentation with a short discussion of the unique issues associated with Digital I&C and a brief history of recent efforts.

We'll also discuss lessons learned from other industries from licensing experience in the United States and regulators from other countries.

We'll discuss the efforts of the NRC Digital Instrumentation and Control Steering Committee and the industry's Digital Instrumentation and Control Working Group that developed interim guidance for the implementation of digital systems in the late 2000s.

We'll also discuss our continuing efforts to use the interim guidance to improve the licensing of digital systems.

We will then discuss in some detail the proposed rulemaking that's currently before the Commission.

And, we will conclude our presentation with a discussion of other key efforts that we're engaged in to continue to improve to improve the licensing of digital system.

Digital technology provides significant advantage over earlier analog or relay-based systems as mentioned during the industry panel.

However, with these advantages have come new challenges. We recognize that added functional capability of these systems as well as new design development and testing methods have outpaced our regulatory guidance.

The use of IEEE 603-2009 is just one aspect of addressing the potential challenges with digital instrumentation and control systems. We recommended in our SECY 15-0106 Commission approval to publish for comment a proposed rule that incorporates the standard.

We're also developing an action plan to support the continued improvements and plan to work with key external stakeholders on these activities.

The priorities in the action plan include improving the licensing processes based on lessons learned from past and current reviews and working with industry to address concerns with licensee implementation of plant digital modifications using the 10 CFR 50.59 process.

The significant challenged addressed in the action plan is the use of identical software across redundant safety channels that could potentially defeat this redundancy and lead to common cause failure.

As Commissioner Svinicki noted earlier in a 1993 Staff Requirements Memo, the NRC position on software common cause failure was established and it is today still the Agency's policy in this challenging area.

However, we do believe it prudent to take a fresh look at the NRC position on needed diversity to address the potential for common cause failure. And, we plan to coordinate our efforts in this area with our external stakeholders.

I will now turn it over to John Tappert to discuss our

experience with digital system review and efforts to improve the regulatory process.

John?

MR. TAPPERT: Thank you, Dick.

Next slide, please?

To begin with, digital technology is unique from analog technology. Specifically, digital systems involve the execution of application software and instruction are logic to perform system functions.

The flexibility of digital technology offers many benefits to address some of the reliability and maintenance issues with analog technology.

Although digital technology offers benefits, the unique hazards associated with the use of digital technology should be considered.

Examples of such hazards include difficulty in achieving deterministic behavior, inability to fully test the system, difficulty in achieving communications and dependence and potential for latent errors in software that could result in software common cause failures.

To utilize this technology, the applicant must demonstrate that these systems will operate reliably to ensure the safety of the plant under normal and accident conditions.

This includes ensuring that systems provide a sufficient level of diversity and defense-in-depth, commensurate with the potential consequences of failure.

Next slide, please?

Digital systems were initially deployed in the nuclear industry in the 1980s. In response to our early experience, in the late 1990s, we issued licensing guidance documents and staff review guidance covering some of the unique aspects of digital system development processes including software development and consideration of diversity and defense-in-depth.

Though this new guidance provided additional clarification of our expectations for licensees to adhere to our rigorous digital development process, the industry sought a more predictable and effective regulatory approach.

We have looked towards other industries for lessons learned from their experiences with implementation of digital technologies, for example, the military and commercial aviation and the process industries.

And, we've evaluated that experience to provide additional insights to our guidance.

Next slide, please?

In 2007, at the industry's request for additional clarification, the NRC formed the Digital I&C Steering Committee. And during the 2007 to 2011 time frame, the NRC with participation from stakeholders developed seven Interim Staff Guidance documents, or ISGs, for the evaluation of proposed Digital I&C systems.

We intend to incorporate the content of the ISGs into the NRC Standard Review plan during the next update.

We used some of the interim guidance in our

evaluation of the Oconee reactor protection system upgrade and for a number of Design Certification Application reviews such as the AP1000 and US APWR.

Based on lessons learned and the Oconee project, we issued ISG 6 regarding the licensing process and used this updated guidance in the performance of the Diablo Canyon process protection system digital upgrade review.

Next slide, please?

It is likely that more digital safety system upgrades will be needed in the coming years to address operational and obsolescence issues.

We have identified that NRC policies and processes can be improved to decrease uncertainty and the cost of licensing digital technologies.

In order to improve the Digital I&C licensing process, we are working on the lessons learned from the Diablo Canyon ISG 6 pilot review.

Some concepts within ISG 6 that have worked well include pre-application meanings, early submittal of certain design documents to support acceptance reviews and guidance on documentation submittal.

One concept that has been less successful is the use of a graded or tiered approach to determine the level of NRC review needed. Since this concept is based solely on the pre-approval status of the I&C platform.

We believe additional system aspects should be

considered for this determination including scope and type of modification being performed.

And, currently, we are focusing on future process improvements to enhance the current digital licensing processes as described in ISG 6.

Next slide, please?

With regards to new reactors, the new reactors, the new reactor I&C designs use highly integrated Digital I&C systems which may include features such as control of safety-related equipment for non-safety I&C system, bidirectional communication between safety and non-safety systems and a high number of interdivisional data communication links.

We have used the current Digital I&C Interim Staff Guidance to review new reactor designs. In several instances, new reactor applicants were challenged in providing sufficient design information, analysis to support the safety demonstration for these integrated systems.

In addition, the applicants did not initially provide sufficient analysis to demonstrate that hazards associated with I&C interactions with plant systems were fully analyzed.

Further, some designs differed significantly from Interim Staff Guidance. And, as a result, these reviews continued much longer and required significantly more resources than originally planned.

To address these issues, some applicants were able to successfully demonstrate safety by modifying the design and

addressing NRC requirements at a higher level of the I&C design such as implementing physically limited one-way data communications. And, this approach was found to greatly simplify the safety case.

Next slide, please?

The current NRC regulation, 10 CFR 50.55(a) incorporates by reference IEEE Standard 603-1991. We believe it is appropriate to update the regulation to incorporate the most recent 2009 version in order to capture criteria specific to address digital technology.

We believe that this proposed rule will make Digital I&C system licensing more efficient and effective.

We have also gained some additional lessons learned from recent licensing experiences. For example, the industry developed NEI 01-01, Guideline on Licensing Digital Upgrades, to provide guidance for performing the 10 CFR 50.59 evaluation for digital upgrades.

And the NRC endorsed NEI 01-01 through a regulatory issued summary.

Based on recent experience, we have identified some weaknesses and ambiguity in this guidance, particularly in the area of addressing the potential of software common cause failures.

These weaknesses in the current guidance have contributed to several licensees improperly performing 50.59 analyses.

In addition, the diversity and defense-in-depth criteria provided in the Staff Requirements Memorandum to SECY 93-087 need to be reevaluated to determine whether it should be updated to

reflect advances in digital technology.

We have also sought to stay abreast of Digital I&C developments in the United States and the international nuclear industry as well as other industries where digital technology is used in safety applications. And, this has included our work with the multinational design evaluation program and various research efforts.

An example of this is the documentation of technical approaches used in other industries to determine what is the appropriate level of diversity needed to mitigate software common cause failure.

And, this assessment can be found in NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems.

And, we will discuss the topic of software common cause failure in more detail later in the presentation.

And now, Rich will now provide a discussion of the proposed IEEE 603-2009 rulemaking.

Thank you.

Next slide, please?

MR. STATTEL: Thank you, John.

The Standard IEEE 603 is titled Standard Criteria for Safety Systems in Nuclear Power Generating Stations.

It's a performance-based standard for the design and development of safety-related instrument and control systems.

It is intended to be a technology neutral and its criteria are used by the NRC to determine regulatory conformance for all I&C

safety systems. This standard is incorporated by reference into NRC's regulation 10 CFR 50.55(a).

When performing I&C safety evaluations, we use IEEE 603 as the principle regulatory basis document. The criteria of this standard are considered as required means of meeting the general design criteria associated with I&C systems.

The 1991 version of IEEE 603 includes a safety system criteria for several topical areas.

Next slide, please?

An NRC working group was formed to evaluate and compare the new version, 2009 version of the standard with the 1991 and 1998 versions of that standard.

This slide summarizes the changes that the working group identified. The new standard addresses potential safety issues that might arise from incorporating advanced technologies and safety systems.

It provides added guidance to address electromagnetic compatibility issues. It adds new criteria to address the potential for common cause failures. It adds clarification for the requirements for equipment not credited to perform safety functions, but connected to safety systems. And, it adds a specific requirement for electrical isolation and digital communication independence between safety and non-safety systems.

Additionally, the standard contained updates to references and eliminates references that were no longer in effect.

Next slide?

The backfit analysis performed determined that the application of the standard was not mandatory for current license holders. Instead, new criteria as proposed will be applied to new applications and selectively to license amendments.

The previous date base applicability criteria were left in place to maintain existing design basis for those currently licensed plants.

A new set of criteria was included in the proposed rule to define applicability for the new standard.

The conditions for determination of applicability are functionality, technology, independent strategy and diversity strategy.

The proposed rule includes guidance for determining the applicability and tables which provide examples of different types of I&C design changes, some of which would require compliance with the new proposed criteria and some others that would not.

Next, I'll discuss each of the conditions for the use of IEEE 603 being proposed. Many of these conditions have been a part of our regulatory guidance for some time, as was mentioned earlier.

We felt that it would be beneficial to provide more specific regulatory basis for those requirements to ensure these important aspects would be addressed.

We expect applicants to provide documentation to demonstrate compliance with these conditions when performing Digital I&C system upgrades.

The standard already contains clauses to address integrity and independence. But, the interpretation of these clauses

has not always been consistent between the applicants and the NRC staff.

The added conditions in the proposed rule are intended to reduce regulatory uncertainty that concerns applicants by elaborating these criteria.

Next slide?

The first condition I'll discuss regards system integrity. This new clause would require, in order to assure the integrity and reliable operation of safety systems, safety functions shall be designed to operate in a predictable and repeatable manner.

The existing integrity criteria in the standard refers to IEEE 7432 which I would characterize that as a companion standard to IEEE 603. But, that standard is not incorporated so it doesn't really have the weight of regulation.

We felt that the additional regulatory basis would ensure conformance with those criteria.

Next slide? Oh, I'm sorry, I've got another paragraph here.

Okay, predictable and repeatable operation of the system requires that the results of translating input signals to output signals are determined through known relationships among controlled system states and required responses to those states.

It also requires that a given set of input signal produces the same output signals for the full range of applicable conditions to defined in the design basis.

All signal processing between sensor, data input and

safety control device actuation must be accomplished in a manner that is neither redundant, portions of the safety system, nor other external inputs can affect the system's ability to perform its safety functions.

Next slide?

In the next set of slides, I'll be discussing a proposed criteria for maintaining communication independence.

The figure shown here shows a reactor protection system architecture. It illustrates three different types of communication interfaces which can exist in these designs.

When I refer to communications between safety divisions, I'm referring to the interfaces shown here in the blue and red lines which connect different components of a safety-related system to support safety functions.

This includes interfaces between divisional safety processors shown as the blue horizontal lines as well as the red line interfaces to the coincidence voting processors.

When I refer to communications between safety systems and non-safety-related systems, I'm referring to the interfaces shown here in the green lines which connect safety system components with external non-safety-related systems such as plant computer systems or maintenance work stations.

Next slide, please?

So, for independence, this condition adds several new requirements to the existing independence criteria of IEEE 603.

Protection systems and safety systems must implement provisions for protection against identified hazards.

Next slide?

Subparagraph A of the independence clause would clarify that signal processing portions of the safety system shall provide the capability to ensure that degradation or failures of signals exchanged among redundant safety divisions or between safety systems and other systems do not propagate in a manner which results in impairment of the safety functions.

For example, safety function processors should not directly exchange information with other processors outside of the division.

Separate communication processes, instead, should be used to ensure the data is received, formatted correctly and is properly addressed to the intended destination.

Subparagraph B would clarify that safety systems shall be designed with provisions for detecting and mitigating the effects of signal faults or failures received from outside the safety division.

Redundant divisions of safety systems should have the capability of tolerating such faults or failures originating from outside that division in a manner that, again, does not degrade the ability of the system to perform safety functions.

Next slide?

Subparagraph C would clarify the requirements for communications in currently operating nuclear power plant designs.

Specifically, it would clarify that communications or signals received by a safety system from outside the division or system should be limited to those that support the accomplishment of a safety

function or otherwise benefit safety.

In the proposed rule, safety benefit is defined as justification for adding safety system functionality that is not necessarily required for accomplishment of the safety function, but that contributes to safety.

Examples would include increasing safe system availability or increasing the safety of a mechanical, nuclear or electrical system design.

Next slide?

Subparagraph D contains new independence criteria being proposed for new reactors. This clause would clarify requirements for communication in new reactor designs.

The first part of this ensures that data communication from safety systems to non-safety systems is in one direction while the system is in operation and is accomplished through hardware means.

The second provision ensures that transfer of signals between redundant portions of safety systems is only permitted when signals transferred is required for the performance of safety-related functions.

Next slide?

The third criteria ensures that for functions that require safety systems to receive signals from non-safety systems to ensure diversity and defense-in-depth were support automatic anticipatory reactor trip functions.

The signal transfer method is restricted to means that do not use data communications.

And, finally, the fourth criteria requires that new reactor applicants who propose alternatives to these previous conditions would identify direct and indirect pathways to safety systems from other systems.

This additional requirement facilitates the identification of interdependencies and failure modes in alternative designs.

These proposed independence criteria would improve evaluation processes for new reactor I&C designs by allowing new reactor applicants to demonstrate communications independence at hardware architectural design level.

Establishing communication at the hardware architectural level would also minimize the potential for propagation of design errors.

We recognize that there are certain cases where a safety division would need to receive signals from outside the division.

For example, voter processors need signals from other systems in order to accomplish the coincidence voting functions.

A safety system may also need signals from the non-safety to support diversity functions.

Next slide?

We believe the proposed rule will have a positive -- the positive impacts on operating plants performing digital safety system upgrades that are shown here on this slide.

Applicants will be able to design their digital safety systems to the new improved standard without having to rely on alternatives clause for approval.

It's more efficient to perform our evaluations without having to evoke alternative standards clause. This supports a more consistent evaluation with the greater degree of predictability.

The NRC already evaluates hazards associated with digital systems per our existing regulatory guidance. And IEEE 603 includes a clause which addresses the need for hazard analysis.

We believe that adding this as a regulatory requirement would reinforce the importance of this activity.

Go to the next slide, please.

The benefits of the rule on operating reactors will also apply for new reactors. In addition, for new reactors, we believe the licensing process will be more effective because the proposed independence criteria would allow new reactors to demonstrate communication independence with a higher level of design information at the architectural level.

As such, applicants would not need to provide detailed design implementation information.

The proposed independence condition incorporate lessons learned from new reactor licensing reviews. These criteria restrict the implementation of communications for safety systems to limit failure modes and unexpected behaviors associated with communications while preserving some of the benefits of digital technology and allowing functionality that improves reliability and availability.

Next slide?

In reviewing IEEE 603-2009 Standard and developing

the proposed rule, we engaged with the industry stakeholders in various forms. Some of the key interactions are listed on this slide.

First, we were actively involved with the NPEC working group throughout the development of IEEE 603. The NPEC working group, as mentioned before, consists of members from the industry as well as NRC staff with all having expertise in the I&C development area.

NRC working group members have discussed and presented plans for incorporating the 2009 rule into our requirements including the additional conditions.

In 2014, we gave two presentations to the ACRS on the draft proposed rule language as it existed at that time. The draft rule was made publically available to support these meetings and highlighted NRC's plans to provide these additional conditions.

As documented in letters to the staff, the ACRS has generally agreed with the proposed rule and has provided several recommendations to add conditions to clarify the use of the standard.

We accepted some but not all of these conditions in our response to the ACRS.

More recently, we conducted a public meeting webinar in August of this year to solicit feedback on the draft rule language. We described our intent to provide the proposed rule to the Commission with recommendation to publish it for stakeholder comment, including specific questions on the key issues in the proposed rulemaking.

As noted in the meeting summary, we received a diversity of comments such as the suggestion to include a provision

which would allow new reactor applicants to provide a greater level of design detail without having to invoke the alternatives clause.

The industry also expressed interest in having an opportunity to participate in workshops.

This concludes my discussion of the proposed rule. I'm now going to turn over the presentation to John Lubinski who will discuss key initiatives related to instrumentation and control.

MR. LUBINSKI: Thank you, Rich.

Rich discussed our evaluation of IEEE 603-2009, the proposed rule and our external stakeholder interactions thus far. I'd like to highlight a few of the benefits of the proposed rule first.

We believe it is appropriate to update the regulations to incorporate the most recent version of IEEE 603 in order to capture criteria specific to digital technology.

We believe the 2009 version provides a safety improvement over the '91 version of the standard. This includes addressing potential safety issues that might arise from incorporating components that use advanced technologies and safety systems, additional guidance to address electromagnetic capability compatibility issues and better classification for equipment not credited to perform a safety function but is connected to safety-related equipment.

In most cases, the conditions included in the proposed rule and the regulatory guidance that we have used for some time into the rule.

We believe it would be beneficial to provide more specific regulatory basis for those requirements in order to ensure

these important aspects would be addressed during licensing.

Specifically, the added condition on applicability will provide more specific criteria on what plant modifications will require updating of the licensing basis.

Additionally, the added condition on system integrity will ensure better consistency and demonstration of this property for digital system and improve regulatory predictability.

We also believe that there will be added regulatory certainty provided by the proposed restriction associated with data communication in the independent section of the rule.

We recommend the Commission approve publication of the proposed rule to incorporate by reference the 2009 version for public comment. We believe it is important to obtain formal external stakeholder feedback on the use and incorporation of the standard.

Next slide, please?

We believe the use of the IEEE standard is only one of the actions needed to address Digital I&C upgrades. We are developing a Digital I&C action plan to review all aspects of our current licensing processes.

The plan's objective is to identity where improvements can be made and the effectiveness and efficiency of our regulatory processes for Digital I&C licensing and upgrades.

To make most effective use of our resources as well as the industry's resources, the issues will be prioritized based on our belief as to which topics, if resolved quickly, could realize the greatest impact.

Where appropriate, the plan identifies specific links to research activities that need to be addressed to support improved technical and regulatory basis for policy or process improvements.

We plan to work with external stakeholders to integrate our Digital I&C action plan with the NEI roadmap. And, we currently have a public meeting planned in January to discuss both our action plan as well as the roadmap.

In addition, as we develop our roadmap, we will continue to revise it periodically based on lessons learned as we implement the actions.

Next slide, please?

The current draft of the Digital I&C action plan includes ten activities related to Digital I&C. One we've already discussed was the use of the IEEE Standard 603.

Next, the Deanna Zhang and I will discuss in more detail four activities which are listed on this slide.

These activities have near term milestones or may require Commission engagement which is why we're discussing them in more detail today.

The first is revising guidance for 50.59 evaluations for Digital I&C modifications.

The second is reevaluating the current process for addressing potential for software common cause failure of digital systems. It is likely we will engage the Commission regarding this activity.

And, the third is identifying the most effective process

for staff to perform its evaluation of proposed license amendments and new applications related to Digital I&C.

And the fourth is evaluating the process and timing for evaluating applicants compliance with cybersecurity requirements. We plan to provide a vote paper to the Commission on this topic.

I will note that while we have not seen the roadmap that NEI has developed nor have they seen our complete Digital I&C action plan, we have coordinated on the major topics and would note that the first two topics, 50.59 evaluations as well as common cause failure are top priorities in both plans and we think that the plans will align on our prioritizations.

Next slide, please?

During component design basis inspections, NRC inspectors have identified noncompliances with 50.59 reviews performed by licensees for digital systems. This is one of the reasons that we are reexamining our 50.59 guidance.

Current industry guidance for evaluating Digital I&C modifications against 50.59 is included in NEI Guidance NEI 01-01. This guidance was originally endorsed by the NRC through a regulatory issue summary.

However, over time, the NRC and industry have found that additional clarity and specificity is needed for this guidance.

We understand that NEI has a working group dedicated to enhancing this guidance. We understand our current plans are to propose its revised guidances and new Appendix D to the implementing guidance which is NEI 96-07.

We plan to meet with NEI on January 13th to discuss the revised guidance. We plan to evaluate the new appendix and, if appropriate, we would rescind our current endorsement of NEI 01-01 and, instead, endorse the new guidance in Appendix D of NEI 96-07.

Any new NRC guidance which endorses guidance development by the industry would become available in the first quarter of 2017.

Additionally, two weeks ago on December 2nd, we met with NEI and EPRI to learn about EPRI's new good practices design document which is being developed in parallel to the new NEI guidance.

The EPRI guidance will not be submitted for NRC endorsement. However, EPRI has solicited our technical comments on the document and we will work with them to provide those comments.

I would now like to turn to Deanna Zhang to discuss the remaining items in the Digital I&C action plan.

MS. ZHANG: Thank you, John.

Digital technology has the potential to introduce software common cause failures and unwanted system interactions due to undetected systematic faults.

The Commission's SRM to SECY-93-087 defines specific criteria for addressing software common cause failures. These criteria are specified the performance of a diverse and defense-in-depth analysis and provisions of a diverse means of accomplishing the safety function.

We implemented this direction in Branch Technical Position 7-19 titled, Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation Control Systems in Chapter 7 of the Standard Review Plan.

This Branch Technical Position provides guidance on diverse means that could be used to mitigate software common cause failures including adoption of internal diversity with the safety system or use of manual operator actions.

In addition, this Branch Technical Position allows a 100 percent testing of simple systems to address the potential for software common cause failure.

This guidance was based on Interim Staff Guidance developed at the request of industry to consider testing as means to address software common cause failures. Also, guidance for performing the diversity and defense-in-depth analysis of reactor protection systems is provided in NUREG/CR-6303 as endorsed by the Standard Review Plan.

This guidance constitutes the implementation of the current NRC policy on software common cause failure.

Next slide?

The current policy and guidance for addressing the potential for software common cause failures have been challenging for some licensees.

For example, the current guidance is a consequence-based approach for addressing software common cause failures and does not directly relate to safety significance. Thus, the

same rigor for treatment of software common cause failures applied to all safety systems without consideration to the significance of the safety function performed by each particular system of the overall plant safety.

In addition, even though we have effectively licensed digital systems using this process we believe the assumptions in SECY-93-087 should be reevaluated in light of significant technological advancements.

Specifically, over the past 20 years, digital technology and the tools for designing it have changed significantly including advancements in both the use of digital use of field programmable data rates and complex programmable logic devices.

The time that the 1993 SRM was issued, few standards and no regulatory guidance documents existed for implementing digital technology in nuclear power plants.

Since 1993, there have been significant improvements in the methods used to design and implement digital systems. There have also been advances in the tools needed to analyze and test these digital systems.

This has led to improved quality and reliability of these systems and improved industry standards as well.

Some of these changes have also been reflecting our updates to Branch Technical Position 7-19. But, the basic NRC policy has not been updated.

Based on evolution and technology and our lessons learned from digital upgrades, we are evaluating the existing policy on software common cause failure and looking at options to update it.

This evaluation will also assess potential ways to achieve a graded approach based on safety significance.

We intend to prepare a report and a SECY paper outlining the technical basis for either modifying the existing software common cause failure policy or for establishing a new rule to appropriately apply diversity and defense-in-depth for Digital I&C safety systems. Our goal is to have a draft SECY paper by the third quarter of 2016.

In parallel with this effort, we will maintain appropriate interfaces with industry stakeholders to identify what activities, if any, can be performed to facilitate addressing this particular issue.

Next slide, please?

As previously highlighted, ISG-06 introduced new concepts to the licensing process. After the pilot program with Diablo Canyon to upgrade the plant protection system, where plant has the processes described in ISG-06.

For example, the level of technical detail and the need for acceptance test reports in the license applications for digital upgrades will be reviewed.

In addition, we are considering options to support industry's request to reduce early regulatory uncertainty prior to submittal of the factory acceptance test results.

We continue to enhance the guidance for licensing processes for new and operating reactors including improvements to ISG-06 and the issuance of design specific review standards.

In particular, to provide additional guidance on

addressing safety hazards associated with highly integrated I&C systems.

We intend to pilot the use of the design review -- design specific review standard for the NuScale Small Modular Reactor which is anticipated to be submitted in the last quarter of 2016.

We also plan to incorporate our lessons learned from ISG-06 into a Branch Technical Position. A draft of this Branch Technical Position is projected to be ready in the third quarter of 2016.

We're considering the lessons learned, industry feedback, new concepts for licensing processes along with research activities to support licensing, to develop stable, consistent and predictable licensing guidance.

Next slide, please?

Finally, we are evaluating the possibility of enhancing the regulatory framework to consider cybersecurity at the design phase. The current cybersecurity regulatory framework is programmatic in nature.

As such, we currently do not perform cybersecurity design reviews during licensing. We believe that considering cybersecurity early in the system design process will help avoid designs that may be difficult or impossible to adequately protect after implementation. The ACRS has made similar recommendations.

As such, we are developing a SECY paper that considers options for performing licensing reviews of cybersecurity design information and plan to provide that SECY paper for Commission consideration by the second quarter of 2016.

Next slide, please?

Besides the IEEE 603 proposed rule and the four issues that were discussed in the previous slides, there are five additional topics that the Digital I&C action plan addresses.

This includes evaluating new methods for assessing highly integrated systems that focuses on hazards and safety design principles.

Improving the regulatory infrastructure to achieve more efficient and effective licensing reviews, developing guidance for evaluating proposed alternatives to NRC requirements and guidance, improving regulatory consistency between licensing and inspection activities and enhancing Digital I&C topical report evaluation and update process.

In support of developing new methods for assessing highly integrated systems, we're engaged in research activities that, in the intermediate term, we hope will yield efficiencies and effectiveness improvements to Digital I&C licensing reviews.

This includes evaluating techniques for hazard analysis and structure safety arguments, many of which of these techniques you've heard from the other panelists that are being used for other industries.

This concludes our discussion of our near term Digital I&C initiatives. I will now turn it back to Vic for closing remarks.

MR. MCCREE: Thank you, Deanna.

In summary, we recommend a Commission approval to publish the proposed rule. And doing so will enable us to obtain

formal external stakeholder feedback on the potential use and incorporation of IEEE 603-2009.

If approved by the Commission, we will also hold a public workshop during the comment period to seek and understand stakeholder input.

As John noted, we will continue to identify and address the other key regulatory initiatives through the development and implementation of the Digital Instrumentation and Control action plan.

The actions over the next several months include work on the 10 CFR 50.59 guidance and evaluating the NRC's processes for evaluating software common cause failure.

We believe it's important to coordinate with external stakeholders and we will continue to coordinate with the industry's Digital Instrumentation and Control Working Group as well.

This concludes our presentation and we'd be happy to address your questions.

Thank you.

CHAIRMAN BURNS: Thank you all for your presentations.

As we hear the discussion, you know, it's a rich field of issues and, you know, actions, potential actions because we're talking not only about a proposed rule on IEEE standards but we're also, particularly, I think Deanna's presentation focused on and some of the others, there is a lot of other stuff going on here.

So, I'm going to try to touch a few of these things. I mean, I think the simple, you know, the question that's sort of posed by

the first panel I think, you know, strikes a number of us.

Let's assume there was a consensus just decided to go ahead with approval as we often do with industry standards under 50.55(a) and approve IEEE 603-2009 and that's it. What are we missing doing that? What is the critical -- convince me what the critical additions in this rulemaking which are different than a lot of, you know, industry standards incorporation by reference I've seen before, what's the critical?

MR. LUBINSKI: I think if we were to look at that, there's many options on how you would address the issue. We chose one option which we thought was the best of incorporating these requirements as conditions in the rule.

We could continue to keep them in a guidance and work with the industry as this being companion guidance to the rule if we were to go forward with just an incorporation of the standard with no conditions and address any concerns that the industry has with those conditions through the development of the guidance.

We have been effective at using that. We have performed reviews already using the alternative clause under 50.55(a) to approve applications that have met the 2009 standards and many of those have met the conditions, the additional conditions already. So we can continue to do that.

What do you lose? I think you lose a little bit of the transparency and clarity of what the requirements are. And, if there's a concern or a difference among us and the licensee on where we're going, then you may get into a little bit of a debate about whether or not

the requirement is necessary and if it's in guidance.

And then, finally, in the past, sometimes we've been criticized for including information which we treat as a regulation, if you will, and put it in guidance and, therefore, regulate through guidance.

So, that would be the other criticism we may be open to if we do that.

CHAIRMAN BURNS: Okay. One of the things, and again, and focusing on the last presentation, you talked about the potential for new licensing processes, new -- other new things is my one concern I would have. What would be the impact of some of those on the adoption of a rule with these added conditions, if any?

MR. LUBINSKI: I'll let John refer to the new reactor licensing first.

MR. TAPPERT: Okay. So, Deanna was talking about our design specific review standard which is probably our biggest initiative right now to try to streamline and focus the I&C reviews.

That's in place for the NuScale application which we're expecting to receive the end of the next calendar year.

So, that's baked in so that's almost irrespective of what the 603 rulemaking does.

CHAIRMAN BURNS: Okay. One of the other questions, I'm going to turn away from IEEE 603, I think.

But, go to the issue that both panels discussed with respect to 50.59 and that over some period here, sort of understandings have diverged with respect to the requirement in 50.59 because is an important control point from the standpoint it allows what we think are

safety acceptable changes in operation and in our license so we don't have to review everything.

Where would you say, in terms of coming to a greater consensus about where that guidance should be, what are the primary gaps or primary push points?

MR. LUBINSKI: In answering that question, let me say I think there's two aspects with the 50.59 guidance.

One is the clarity of the application of that guidance. So, we may be aligned with the industry that there were certain 50.59 reviews that were performed inadequately and the industry may agree with that in hindsight.

There may be other areas where the industry would disagree with our interpretation of 50.59 and its application with respect to whether it is coming up with a, you know, a new scenario that was not previously analyzed by the licensee or come up with a different outcome. So, there may be differences.

We have yet to see the guidance that NEI has developed, so it's too soon to answer what that question would be. And, that's the importance to our January meeting with NEI on that new guidance to see how much of this is clarity and specificity of the guidance and understanding current 50.59 and where are there differences between our interpretation.

I will say one of the big -- because it is a link to common cause failure because that's another aspect that feeds into 50.59 which is why I believe both us and the industry have put both of those items as our high priority items to look at.

CHAIRMAN BURNS: Okay. One of the -- you know, we obviously in the first panel we had a couple additional experts outside of our industry. And, I know during the discussion maybe one of the Johns, I think you mentioned, in terms of our, you know, participation in multinational design evaluation program and I know from, you know, past experience, Digital I&C has been an issue, you know, one of the subcommittee type issues on MDEP for a long time.

What do we -- any comments you want to make from what you heard on the first panel about the -- what we might learn from aviation? And, is that, in terms of approaches that we've seen through MDEP, you know, that the French have done or others, and I know, you know, again, this is from sort of being, you know, the amateur reader, if you will, on some of this that there are some differences.

But, any insights we have from MDEP or our interaction on aviation industries or others?

MR. STATTEL: I'd like to make an observation with regard to that because I think a lot of the misunderstandings we've had in 50.59 have actually resulted from some of the things that we're hearing from the other industries.

So, for example, the challenges that we've all faced involve and the way we respond to those involve not just looking at the end result or the testing but also focusing on processes, the development processes and different aspects of these systems.

And, that's why you see these big maps and these complex maps of the different facets of I&C that we all look at. And, I think that tends to create some misperception so, like one of the

statements I've seen in some of these 50.59s that were deemed unacceptable was that, well, we used a really good development process so, therefore, we didn't have to do complete testing. Right?

So, in our interpretation, we wanted basically to address multiple facets of the design and their interpretation was more, well, since I have a good process, then I can basically de-emphasize the end testing results or I don't have to concern myself with the common cause failure aspects because it's -- I've reduced the likelihood of that.

CHAIRMAN BURNS: Okay.

MS. ZHANG: I'd like just to add from the MDEP perspective.

So, I chaired the Digital I&C Working Group and it's a number of regulators we have and we all have a number of concerns with respect to software common cause failure.

We developed a common position for this. And, what we have come to alignment is that, yes, it is a multifaceted issue. There are many ways to address it, but we definitely have to address it. It's not something we can ignore.

And, what we have to come to agreement on is that there are -- you should do analysis. You should consider different coping measures. But, the acceptance may be different, the acceptance criteria for applying it may be different.

CHAIRMAN BURNS: And, how so? How are the acceptance criteria different? What drives that?

MS. ZHANG: So, for example, in the French

regulators, they look at a lot more in terms of the software. So, they get the actual software code. They evaluate it, they analyze it for the potential software defects that may be in there.

So, there's a lot more emphasis on testing, analysis and development than what we would typically look at in our licensing reviews.

CHAIRMAN BURNS: Okay, all right.

MR. TAPPERT: And, I'd just like to add, you talked about other industries, one of the items in the action plan is dealing with highly integrated systems. And, that's more of an intermediate term thing where we're going to be looking at different opportunities and different paradigms to look at greater reliance of hazard analysis and structured safety arguments to kind of think about different ways of evaluating these systems.

So, that's why we can kind of import some of that knowledge.

CHAIRMAN BURNS: Okay, thanks.

All right, thanks very much.

Commissioner Svinicki?

COMMISSIONER SVINICKI: Well, I want to thank the staff for the presentations today. But, beyond that, I'd like to thank Richard, John Lubinski and Deanna for, I think at this point, we may be up to close to four hours worth of separate briefing time that I've had an opportunity to talk about the specific IEEE 603-2009, that SECY paper.

That's been very helpful in terms of building a foundation to consider the staff's recommendation that's in front of me.

Something that's not been mentioned because today's meeting, the topic, when the topic of that paper comes up, the staff has presented on, appropriately so, the staff's recommended position.

There are multiple nonconcurrences to that staff recommendation, however, all of which I've reviewed, all of which I found very thoughtful and I do thank the nonconcurring individuals. I don't know if any of them are attending here today.

In all cases, those were very thoughtful nonconcurrences and, for me, in terms of my review of the matter, many of them were quite compelling.

A number of them originate with NRC reviewers who have, frankly, decades worth of experience on this topic as safety reviewers here at the Nuclear Regulatory Commission. So, the level of experience they have in the operating reactor field carries a lot of weight with me.

So, again, I think as we discuss this today, we have discussed the staff's recommendation which was the ultimate decision adjudicated by the staff as they reviewed the nonconcurrences.

However, there is other body in the decision record for the Commission's consideration which I think is important. And, but for its existence, it might be a little more straightforward. But, you know, candidly put, our experts are not of one mind on the additional conditions, principally, a lot of the nonconcurrence has to do with the addition conditions beyond incorporation by reference, there's not unanimous support for those.

So, that will be a factor in my deliberations on the

underlying matter.

I think that, at some point, it is difficult as an organization, we do need to find, maybe it will be through the additional work that we continue to engage with external stakeholders.

At some point, if we could bring this diversity of position into greater alignment, I think it would strengthen us as a professional organization and the experts for the nation on this topic that we have to be able to auger some competence in our decision making.

So, again, I'm fully supportive of the nonconcurrence and differing views process. I just think that we've got a lot of moving parts here and if there's a fundamental philosophical divide or divergence that's occurring, my general instinct maybe just even as a human being, is that sometimes you want to mend that first and then you want to continue to the detailed technical work.

So, I think if you can't get the ideology in alignment, I think we might then -- I might -- my successor in, you know, 2027 won't read an SRM from 2017 and say, gosh, ten years ago it was so quaint that Commission thought that these things were near resolution.

But, I think it is something for the senior leadership team here. I know alignment is tough. I know the EDO and his direct reports do a lot of alignment meetings. That's part of being a technical community, a community of professionals and experts is that we need to go through that process.

And so, I think it's healthy. I'm not in any way suggesting that this is deeply irregular, but I do think, you know, before we dot every I and cross ever T, we may want to get to the root cause.

That's kind of popular in this business. We might want to get to the root causes of some of that divergence.

So, I only had one specific question and it had to do, as the Chairman mentioned, there's other things beyond that SECY paper which Deanna covered.

Deanna, you talked about work on highly integrated systems. Do we have a good definition for a nonpractitioner in this field of what differentiates an integrated system from a highly integrated system?

MS. ZHANG: I think it's just an upper, but if we look at a lot of the shared resources that are going between the different systems between levels of independent systems.

Prior to, you know, use of digital systems and even throughout the upgrades, it's always been a little bit more piecemeal. You get one system that performs one function. Now you have a system that could perform multiple functions.

And, that's where the integration comes from is how much functionality are you putting into one resource or how many different systems share the same resource in performing different functions?

COMMISSIONER SVINICKI: Okay, thank you. That's helpful and I look forward to learning more about work as the staff moves forward on advancing its work products in that area.

I guess I'll just close maybe with a little bit of a pep talk to say that the first panel talked about other industries. I made a comment there that other sectors may be some how overtook us and

surpassed us on conquering this issue.

You know, I want to say that I come at this sincerely with just so much respect for all the differing views that exist on this, the recommendation and the other views.

People have -- our experts have come at this with a lot of conviction. But, at my level, you know, some of this bubbles up to fundamental determinations of how safe is safe enough? What is risk tolerance? What risks can be tolerated? What level of risk can be tolerated or levels of uncertainty?

And, that is a threshold judgment at every level of senior leadership. We've got to make tougher and tougher decisions about that. The Commission being the ultimate expression, we often have to make the ultimate judgment call on how safe is safe enough.

But, I will say this to you, none of your peers over at FAA or anywhere else are better at this than us, so we absolutely will resolve this. I know we will conquer it. It is not, as the first panel said, a question if we can resolve these issues, we will because there is no future for nuclear technology, either for the stuff that's operating now or future stuff if as the nuclear safety regulator for the American public, if we can't solve this, there's no future. I know we can solve it. I know we're going to.

So, you know, continue, please, no matter the outcome of the Commission's decision on the 603 paper, please continue to work on this with the kind of commitment that you have.

Thank you, Mr. Chairman.

CHAIRMAN BURNS: Thank you.

Commissioner Ostendorff?

COMMISSIONER OSTENDORFF: Thank you all for your presentations.

I want to start out, and I'll let anybody answer this who wants to. With the first panel, we clearly heard from industry that, with respect to this piece that deals with IEEE 603-2009 that there is not agreement that we should add these additional requirements above and beyond the industry standards.

I just want to provide an opportunity to anybody that wants to speak to address that issue.

MR. LUBINSKI: I'll start at a high level and maybe ask others to talk detail.

I think what I also heard from the industry this morning as well as hearing in other communications with the industry was, one was a prioritization of resources when they were saying that the IEEE 603-2009, they were looking at what's the resources to continue through the rulemaking, go through the comment period, what the concern would be there and trying to address those additional conditions through that process.

And, I hear that they're looking from a prioritization standpoint and saying things like 50.59 and common cause failure are more important and should be addressed first and then we can look at the conditions.

I think from the standpoint of the additional conditions, what I also heard this morning was a concern of making them regulatory requirements versus the actual technical nature of those

requirements and Rich can maybe expand on some of the technical nature of some of those aspects.

I think we have been effective across the board as a regulator and an industry in addressing issues associated with those additional conditions through current licensing reviews that have been performed whether they're in the operating reactor or in the new reactor area.

So, the conditions have been in guidance, not as conditions, of course, but have been in guidance to address things like the hazard analysis, the independence and the communications. So, we have been able to address those on a case by case basis.

But, I think from the standpoint of understanding more of the specific concerns from the industry on those specific items, no, we don't have a clear handle on that.

Rich, did you want add?

MR. STATTEL: I'll expand a little bit upon that.

The working group did spend a lot of time discussing this. And, virtually every one of the conditions that you see in the proposed rule was originally proposed as guidance, that inclusion into the reg guide that accompanies this rule.

There wasn't unanimous agreement, there still isn't among the working group members.

The real thing is, at a glance, you might think that taking exactly the same verbiage out of a consensus guide that everyone agrees to and moving that language into a rule, well, why would that be a problem?

But it's really a context issue and by putting it in the rule and changing the context of that language, you really make that the only acceptable way, you know, by definition, by putting it in the regulation and it makes it a whole lot more difficult for designers to innovate and to realize some of the safety benefits that could otherwise be realized.

So, it really does change the context. In some cases, like the hazard analysis requirements, I like to call it a strong guidance because, you know, every safety evaluation I've ever done on a digital system, we require them to identify hazards and we require the applicant to address all of the hazards they identify.

So, making that a regulation, it's, you know, it kind of emphasizes the importance of it, but I really can't see applicants proposing alternatives to that, like I'm not going to address the hazard that I identified.

So, those are not so much controversial. But other ones, the independence requirements in particular are viewed as being a lot more difficult and problematic.

Those requirements in particular, those are where we basically divided the rule into new and operating reactor criteria and, what really drove that was the processes. We really have -- we really face very different problems when we're reviewing a design certification versus an amendment, a license amendment.

So, one of the big differences I'll point out, there's a lot of subtleties to this, but one of the big differences is, with an operating plant, it's operating. It has a licensing basis. We have something to

compare the new system to. And it's therefore, there is a basis for putting forth your safety conclusions. Right? You're at least as safe or you're improving safety on that system.

With the new reactors, you don't have that baseline, so that makes it a lot more difficult for them. And, honestly, you know, we're all engineers here and we do kind of think a lot alike.

However, you know, we're really faced with very different problems and I think, you know, if we reverse positions and, you know, I was working on the new reactor side, I would have a lot of the same concerns they have.

So, it's really the process that drove those differences in the proposed criteria.

COMMISSIONER OSTENDORFF: Okay. John? Or Deanna, yes?

MR. TAPPERT: I just wanted to chime in.

So, the way I think about it, and I think John talked about this earlier, is there's a lot ways to skin a regulatory cat. And, I think what the proposal before the Commission is really the staff's best proposal to go forward.

But, we recognize that there are, you know, good arguments on different approaches as well. And, that's why in addition to the proposed rule before you, we've also proposed an approach where we wanted to have an extended public comment period. We wanted to have public workshops in order to get more stakeholder input.

We've actually put a number of -- or

suggested -- recommended putting a number of questions in the proposed Federal Register Notice to kind of elicit some of this feedback on, you know, are these too prescriptive? Are there better ways of doing this? Are there unintended consequences?

So, I think what we have is our best thinking, but we recognize that we need other input as well.

COMMISSIONER OSTENDORFF: Thanks. Deanna?

MS. ZHANG: Yes, and I would like to just add on a little bit to what Rich was saying which is, you know, we heard from the previous panelists, you know, evidence. And that's something that we definitely had an issue with with a lot of the new reactor applicants is that they did not provide evidence that the design was safe in terms of communications independence.

And with that, you know, are there other means to achieve the same result as limiting the architecture? Yes, there are other means. And, that's why we do have an alternative process which we have successfully used before.

But, when we looked at our previous lessons learned from the recent design certification applications, because of the lack of evidence and because not all the hazards were correctly identified, we had a lot of issues approving and reviewing those designs.

COMMISSIONER OSTENDORFF: I'll just make a comment, I'm not going to ask a question of this, but in my vote on the Commission involvement or decisions rulemaking, I did use cite -- a paragraph using this SECY paper as an example. And, it's quite

frankly, not a positive example.

Where it took 18 months in concurrence to come to the Commission and there is different -- I respect the fact everybody's engineers and always trying to do things the right thing, but both Rich and Deanna have hit upon there's different ways of looking at this in the organization.

So, I just would ask you to look at my vote on that because I think it's highlighting the lack of agility in decision making here which I'm going to make a comment on as I close.

I start out by saying I'm struggling with this one. At the conclusion of today's meeting, I'm still struggling.

I've heard Deanna talk about well, we need to go back maybe and look at SECY-93-087. We've had -- the SECY paper talks about these other future rulemakings. They are not well defined.

John, I appreciate the comment on public, you know, comment and so forth. My personal view as a Commissioner, I don't vote on something that I'm not comfortable putting out there that I would say this proposed rule can be a final.

So, I'm very leery to vote on something to say throw it over the transom let public comment on. Is it premature? You know, with all these other moving parts, I can't, you know, we spend a lot of time, as Commissioner Svinicki noted, we've had a lot of different briefings before today from the staff on this exact topic.

How should I look at our ability as a Commission to make a decision on this given all these other moving parts?

MR. LUBINSKI: Yes, if I could. I'm going to refer a

little bit to John Tappert's comment a minute ago.

In addressing the issue with respect to the IEEE 603 Standard, there are many options and the way to handling it is was stated, as Commissioner Svinicki said, there were diverse opinions from staff. And, you could probably go about three or four different options on how to move forward with respect to the standard.

We chose what we believed was the best option in moving forward and provided that to the Commission.

COMMISSIONER OSTENDORFF: I just want to make sure I'm clear on the record.

I do not fault the recommendation that came to the Commission. My real concern is these other ancillary efforts that are not real clear what they might mean going forward.

MR. LUBINSKI: Understood, I appreciate that.

And, the reason I brought that up too, my comment is that we think that the public comment period that we would have if this proposed rule is approved is important.

We also believe that in going forward, if we had no comments on the proposed rule and it went final, we believe it would be an effective way to regulate.

With respect to the other issues, we did take those into consideration and looking at continuing with this rulemaking.

In fact, common cause failure was one of the issues that we considered putting into this rulemaking and making part of this rulemaking at that time.

One of the reasons we pulled it out of the rule and are

looking at it as potentially, and that's what's referenced in the rule is the diversity and defense-in-depth rulemaking that's being handled under separate, is we did believe that more work was needed on that. We believed better regulatory basis was needed.

We also believed in going forward that more stakeholder interaction was needed, external stakeholder interaction. We do plan to do that in the coming year to work with the industry to get their issues.

We're currently calling it a rulemaking process. Whether it turns into a rule or not is going to be a question. It could be that we believe that the current policy or say policy position, if you will, on the SRM from 1993 is adequate and we continue to stick to it. It could be a modification and guidance but we won't know until we do more evaluation. But, we felt that was necessary.

In answering your question why are we comfortable going forward with 603 with these other issues there? We're not seeing that we need to change 50.59 and we don't see a big connection to 603 with that.

For common cause failure, that is one piece of what's being evaluated and if it turns into guidance, why should we hold up this rulemaking When it could just be a change in guidance and moving forward?

We would have certainty in the industry from the standpoint as a question you asked the industry earlier about additional applications coming in. We know that's the goal with the industry. In their roadmap, we understand that they've put target dates for the next,

I'll say, major application to come in and feel that if they can't get to the point of doing that, then that's not success on the roadmap.

We believe having some certainty with respect to how you handle 603 will help with the certainty in that application coming in. We believe handling these other issues in parallel, we have looked at the what can be done in parallel and what can be done in series and that's the reason the action plan was put together and we do believe that 603 can and should move forward while we're handling those issues in parallel.

COMMISSIONER OSTENDORFF: Okay, thank you.

CHAIRMAN BURNS: Thank you, Commissioner.

Commissioner Baran?

COMMISSIONER BARAN: Thanks.

John, let me just pick up right where Commissioner Ostendorff left off on this question of diversity and defense-in-depth and how to approach this.

And so, the ultimate recommendation from the staff was don't address that in this IEEE 603 rulemaking. Let's do what's likely going to be a separate rulemaking to address diversity and defense-in-depth.

And, I guess my first question on this is, what happens, you know, what happens if we don't include -- we don't address diversity and defense-in-depth in this rulemaking but then we end up not proceeding with a separate rulemaking on those topics? Where are we going to be at that point if we don't do it here and then, for whatever reason, ultimately, we don't do it separately?

MR. LUBINSKI: Okay, I will say from the first point is the IEEE 603 rulemaking is an incorporation by reference rulemaking into 50.55(a).

There is a link with common cause failure, diversity and defense-in-depth but it's not an industry standard, if you will, that's been put together that would be incorporated into 50.55(a). And, there have been questions whether that is the appropriate place for it or does it go in another section of the regulation if it becomes a rule.

From the standpoint of not addressing it, I would say that I believe the issue will be addressed. Whether it's addressed as a rulemaking or not is a separate question and I think that's where you're coming from.

If we were to move forward and look, there are a number of outcomes and I don't know what they're going to be. The outcome could be that our addressing of common cause failure is adequate the way it is, that the SRM that was issued in '93 is adequate and maybe there's only tweaking of the current guidance which incorporates that.

All the way to the other end, it says we believe the only way to have certainty is to put it into the rule.

We've discussed today some of the conditions that we would include and how important are they to be conditions in the rule for 603 versus being handled through a guidance.

So, I think if I were to listen to your question of the worst case scenario if rulemaking was turned off in that area, what would happen? I believe there would be some type of enhancement

and guidance that would address this issue and we would go through the process of interacting with external stakeholders on that guidance to assure that it addresses the issues in an adequate manner.

COMMISSIONER BARAN: In that eventuality, we would continue to regulate based on this 1993 SRM. We wouldn't have anything in regulations, we'd have regulatory requirements based on an SRM.

MR. LUBINSKI: I would say that if we were doing something different in a guidance that contradicted the SRM in any way, we would not necessarily have to go through a rulemaking, but we would come back to the Commission with a statement of direction from the Commission in 1993 was this in an SRM and get Commission approval to change what was in that SRM. We would reference that SRM, talk about the merits of why we would change that and, if we were not doing rulemaking, we would say we plan to address this through staff guidance but request Commission endorsement of that new, if you will, standard or policy.

COMMISSIONER BARAN: I guess it just strikes me that there's some awkwardness in proceeding that way, right? I mean normally we have regulatory requirements that are actually enshrined in regulation versus in just a Staff Requirements Memorandum.

And so, if it's a very significant issue from the staff point of view, the idea that we'd address it but we'd never address it in actual regulation strikes me as problematic.

MR. LUBINSKI: Right, it's not addressed in a regulation at this point, but what we did is put it into durable guidance, if

you will, from the standpoint of our standard review plans, our ISGs as well as Branch Technical Position.

Branch Technical Position 719, thank you, I'm getting help from the back, thanks. It is listed in that Branch Technical Position which we use.

So, from a durable guidance standpoint, it is durable guidance.

COMMISSIONER BARAN: Jennifer, did you want to --

MS. UHLE: Yes, this is Jennifer Uhle, I'm the Director of the Office of New Reactors.

And, I think in part, the Commissioner's question is also asking what are -- where are the regulatory requirements for anything associated with Digital I&C?

And so, I&C has been certainly a requirement since the inception of nuclear power. And it specified in the general design criteria 21, 22, 23. There's elements in Appendix B, so that's Appendix B to Part 50.

And then, of course, there's IEEE 603 which is endorsed by reference under 50.55(a).

So, there is no one clear Digital I&C rule. That's not how it has been put together and it gets confusing because then it's a patchwork and we can talk about this element of IEEE 603 here. But then there's other issues about common cause failure and the reliability of the system that is discussed in the general design criteria and then the supporting guidance.

So, I don't know if that helps at all. The SRM to SECY-93-087 provides direction to the staff on how to implement those regulatory requirements that are in the GDC and that was previously in 50.55(a).

COMMISSIONER BARAN: But, is there a downside, and this is a question for everyone who wants to answer it. Is there a downside to seeking stakeholder feedback on a potential, you know, provision on diversity and defense-in-depth through this proposed rule, getting that feedback?

Now, originally, once upon a time, in the staff process developing this, there was a provision on this. It was taken out in response to a nonconcurrence. Is there an advantage, given that we don't know what the Commission may or may not approve in the future on a separate rulemaking, we don't know even if there would be a separate rulemaking, is there an advantage of to getting public comment on that question now in this proposed rule? Is there any downside to doing that?

MR. LUBINSKI: We've already in our current package in response to many of the nonconcurrences and differences of opinion we've had included additional questions in the current rulemaking package of which this is one of those questions how we should address diversity and defense-in-depth common cause failure.

It's a specific question, one of many that are listed in the Statements of Consideration seeking feedback.

We have also, if we were to move forward, issue the proposed rule and have the workshops John talked about, that would

be one of the main topics of discussion along with the other questions that are listed in the rule today.

COMMISSIONER BARAN: Okay. Well, and then taking a step back on the -- and obviously, I think it's fair to say there are a wide range of views about how to proceed with this rulemaking, and we've talked a lot about the question of what goes in a regulation and what goes in guidance.

And, from your point of view, and this is a question really for either John or the other John, you know, how much of the disagreement about this just boils down to whether we're going to take some of these requirements and put them into a regulation versus keep them in guidance where they are now?

Is that really what the disagreement's about, whether -- not what the requirement or expectation would be, but rather does it reside in their regulation or does it reside in the guidance?

MR. LUBINSKI: I would say probably that's the majority of it, but that's not all of it. There are some disagreements and I think for the -- where there are technical disagreements even internally, and I know there are externally as well, but even internally where you may have disagreements on the technical requirements, there's a concern that if you do put it into the rule that makes it that much more difficult for the people with the diverse view to have their concerns addressed.

When they're in guidance documents, they feel that maybe there's a bit more leeway when they're going through a review process that it's only guidance and, therefore, they don't have to treat it

as a regulation when they're implementing it through a licensing process.

COMMISSIONER BARAN: Did you want to add anything on that, John?

MR. TAPPERT: I would just step it back to your previous question about the common cause failure and the desire to get stakeholder feedback in the context of the rulemaking.

So, John referred to the Federal Register Notice, proposed Federal Register Notice which had question in it.

We also have in the action plan a separate track to look at that one issue. And, as part of that, there will be public engagement and feedback. So, even absent the rule, there'll be activities to engage on that topic.

COMMISSIONER BARAN: And one of the issues or questions that came up on the first panel was, well, are these conditions that the staff has added to the core standard, are they performance-based technology neutral or are they technology specific? Does someone want to respond on that?

Is this a situation where we're potentially being overly prescriptive in the regulation and allowing only one way to do something or are these performance-based standards that are technology neutral?

MR. STATTEL: I would just like to point out, I know the perception might be that we're diametrically opposed on these matters. But, in actuality, we're a lot closer than you might think.

So, for example, if a design met all of the conditional

requirements that are being proposed here, no one at this table would disagree that that's a safe system, that that's an acceptable system.

Where the disagreement is, is that's the only way to achieve a safe system. So, in a lot of cases, you know, just the same conditions under a regulatory guidance perspective, you know, that would alleviate the difference of opinion. Right?

But, you know, When you start putting those prescriptive type requirements into the regulation, that's, you know, you're really boxing the designs in and that's where it becomes problematic.

COMMISSIONER BARAN: And, John and John, I mean are you share that view? Are these prescriptive requirements that are represented by these conditions that allow for only one way to do it?

MR. TAPPERT: And, I think at least some of that is being directed at some of the communications requirements for the new reactors communications provisions.

So, and I can't argue that those are anything but very prescriptive. I mean they are. And, the reason they are that way in the proposal is based on our experience in trying to review these design certifications.

And, it's been a very problematic area and our view is that to get better regulatory surety and have a better path to success on these things, it's appropriate to be that prescriptive, understanding in general that's not how we want to do business. But, in this particular instance, we think that the evidence supports that proposal.

MR. LUBINSKI: And, I would agree with John from the standpoint of that being prescriptive and I would not argue at all.

There are others that may be technology neutral and more performance-based such as the performance of a hazard analysis. There's not -- it's not prescriptive in how it's done, what the results need to be, but it's that the hazard analysis is performed.

And, I'd say that's more of a level of detail of information that's provided to the NRC for review versus a prescriptive design standard in this.

COMMISSIONER BARAN: Is the one way communication, is that the only example of a condition that's prescriptive from your point of view?

MR. STATTEL: No, there are three criteria in the new reactors clause. One is that communications for a diverse control, so basically a non-safety signal to actuate a safety injection pump, for example. That would have to be transmitted via a non-digital means. So, basically, it would have to be a discrete analog signal essentially.

And, of course, the one way communications to non-safety-related systems, that's the other example.

MS. ZHANG: So, specific to new reactors, that's the answer is the prescriptiveness comes for the new reactor independence clauses. But, in terms of, you know, are there better ways of doing it? And this is where we are looking at the highly integrated systems, new methodologies for assessing it as part of our Digital I&C action plan.

And, we have active research in this area where we're

working with the Carnegie Mellon Institute to look at modeling techniques to bottle some of the design certification applications to have come in.

And, based on the results of those studies, we may find that there are better ways to do it.

COMMISSIONER BARAN: Okay, thank you.

CHAIRMAN BURNS: Thank you.

Anything else from my colleagues?

Well, again, I appreciate the presentations from the staff today as well as from our first panel. It's been a good discussion of the issues related to the use of digital technology in the nuclear industry and our associated regulatory activities.

Obviously, an area of high interest and today's discussion I think are important input to the Commission's consideration of various matters including the particular paper in front of us.

Again, thank you. And, with that, we'll adjourn.

(Whereupon, the above-entitled matter went off the record at 4:23 p.m.)