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

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

2 1:01 p.m.

3 CHAIRMAN BURNS: Thank you, and I'll invite then

4 our first panel on our meeting on Digital Instrumentation and Control to

5 take their seats at the table.

6 (Pause.)

7 CHAIRMAN BURNS: Well good afternoon. I want to

8 welcome our external panelists, the NRC staff and members of the

9 public who are here or may be listening in on today's meeting. The

10 purpose of this afternoon's meeting is to discuss the proposed

11 rulemaking for incorporating by reference the Institute of Electrical and

12 Electronics Engineers Standard 603-2009, the IEEE standard criteria

13 for safety systems for nuclear power generation, which we'll refer to as

14 IEEE 603.

15 We'll also be discussing other key regulatory and

16 industry activities related to licensing of digital instrumental and control

17 systems. The Commission has a proposed rule before it on IEEE 603,

18 as a voting matter and today's discussions will aid deliberations on that

19 paper.

20 The paper is numbered SECY 15-0106 and it is

21 publicly available on the NRC's website. Our first panel will include

22 presentations from the following persons: Mr. Robert Coward,

23 Principal Officer, MPR Associates, also representing the Nuclear

24 Energy Institute Digital I&C Executive Working Group; John Connelly,

25 Engineering Manager of Capital Projects for Exelon Nuclear; Daryl

26 Harmon, Consulting Engineer, Operating Plant Business for

1   Westinghouse Electric Company; Darren Cofer, Fellow with Rockwell

2   Collins Advanced Technology

3   Center, and William Scherlis, Professor at Carnegie-Mellon University

4   and Director of the Institute for Software Research.

5   After we hear from our external panel, we'll have a five

6   minute break and then hear from the staff.   I look forward to

7   presentations and the discussions.   I believe Commission Ostendorff

8   wanted to say something, and then I'll turn to the other Commissioners

9   as well.

10   COMMISSIONER OSTENDORFF: Good afternoon.

11   I don't often do this before a meeting.   I'm going to do it today.   It is an

12   exception to my normal practice of being silent at this stage.   But I think

13   I want to set the stage for this, as far as my own personal views as a

14   Commissioner.

15   I know in April 2010, when I went to my first commercial

16   nuclear power plant and saw Watts Bar 2 and saw the analog

17   instrumentation and reflected upon my experiences back in the 70's, at

18   reactor prototype at S3G in Ballston Spa I didn't see much different.

19   In my five and a half years as a Commissioner, I've

20   spent a lot of time looking at instrumentation control, digital I&C.   I don't

21   think we are as a nuclear enterprise where we need to be, either at the

22   regulator stage or at the industry stage.

23   I think there's a lot of opportunity to do better, and that

24   if we're going to continue to operate nuclear power plants in the future,

25   we have to address these issues, some of which will be discussed

26   today.

1   In September of this year, the Commission received a

2   draft proposed rule on digital I&C from our staff.   Along with my

3   Commissioner colleagues, we've spent a lot of time talking about this.

4   We've discussed, debated at a lot of other meetings before today's

5   meeting, and I'll speak for myself.

6   I quite frankly am unable to come to any conclusion on

7   what to do here, because I feel like we've not looked at the broader

8   picture.   We've looked at one piece on IEEE 603-2009.   But we've not

9   looked at the broader mosaic, whether it be other proposed rules the

10   staff   might   be   thinking   about   on   common   cause   failure   and

11   dependence,   etcetera,   or   what   the   impacts   this   might   have   for

12   stakeholders represented today on the goal of upgrade the existing

13   nuclear power plants from analog to digital.

14   So I think this is a really important meeting.   I think this

15   is an area of our regulatory work where there's much to be done, and

16   I'm   very   grateful   to   all   the   Commissioners   who   have   been   very

17   supportive of us having this session today.   Thank you.

18   CHAIRMAN   BURNS: Thank   you.   Commissioner

19   Svinicki, okay.   Well thank you, and with that Mr. Coward, would you

20   please begin the panel presentation.

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

22   CHAIRMAN BURNS: Yeah, you are.

23   MR. COWARD: I'm Bob Coward from NPR.   I've

24   been asked by NEI to provide what I'll call the industry leadership

25   perspective, and I'm tempted to thank, Commissioner Ostendorff, and

26   pass to the next presenter.

1   I think that one of the messages that from an industry

2   perspective we want to make sure we'd like to get everybody aligned

3   around is people tend to look at the I&C problem these days.   You hear

4   a lot of people talking about the digital I&C problem, and I think we look

5   at it differently.

6   We look at it as failure to capture opportunity, that

7   when we look at plant safety, plant efficiency, reliability, even

8   something as simple as the ability to maintain the plants, that moving

9   towards digital is a big step in the right direction on all those goals, and

10   something that the industry, all of us together would benefit greatly

11   from.

12   It also has, from an industry standpoint, and I'm

13   assuming that the staff shares this perspective, we almost see

14   addressing these outstanding questions as a prerequisite as we talk

15   about 60 to 80 that, you know, from a business decision/business

16   investment perspective, there's not a board in this country that's going

17   to approve an application to go to 60 to 80 if it doesn't have some level

18   of confidence that these projects can be done reliably.

19   So from an industry standpoint, I think you know, we're

20   eager and interested to move to a better place.   We were at an NSIAC

21   meeting last year and got into a good discussion among the chief

22   nuclear officers about what's important, what should we be working,

23   and this one quickly rose to the top of the list.

24   We reached out, a number of us, to talk to people in the

25   industry.   There's a lot of industry working groups and some of the staff

26   participates on some of them, as to where things are, and sort of got a

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

2   Just a couple of key points to give you that perspective.

3   One, cyber. Everybody always tends to start with cyber, because

4   that's a hot one these days. I think from an industry standpoint our

5   perspective is cyber's okay. We'd like for cyber to be in a better place

6   in terms of the value benefit equation of the effort put in, but on the big

7   scale of things, we're willing to put that behind us if we can address

8   some other questions first. We think they're more important.

9   We see good projects being done across the country.

10   We see some digital I&C going into nuclear power plants, making their

11   plants better, safer, more reliable, primarily in balance of plant

12   secondary system applications, non-safety related applications.

13   We want to extend that. In terms of challenges, we

14   see some questions about responsibilities not being clear, expectations

15   not being clear, and we'll acknowledge that from an industry

16   perspective, perhaps we've even stubbed our toe a couple of times.

17   You know, some of the 50.59s that have been done

18   probably had holes in them and one of the things the industry's working

19   on hard right now is to close those holes as well. You roll it all together

20   and the big picture is almost everybody can see the benefits from a

21   digital I&C upgrade enhanced replacement in a nuclear power plant.

22   The challenge is when you go look at the cost-benefit

23   analysis, the decision-makers. These are not small, trivial projects,

24   and the decision-makers who have the final say, they look at risks, they

25   look at costs, they look at benefits. Even though they see the benefits,

26   the costs and the risks are still outweighing those benefits in many

1   cases.

2   That's what we have to knock down, is we have to

3   knock down together that perception.   We actually want people

4   desiring and embracing doing these projects, not to be sort of heading

5   down the aisle skittishly or nervously.

6   In terms of a couple of specific places where we know

7   we need to work, we the industry and we're looking forward to engaging

8   with the staff to work together, 50.59 guidance.   Industry's about to

9   submit through NEI some updated guidance on 50.59 specific to digital.

10   We're looking forward to the staff engaging with

11   questions and dialogue to ensure we're aligned.   If you go back I guess

12   six, seven, eight years, I think Commissioner Ostendorff, as you alluded

13   to, there was much more of an interest in digital I&C.   There was a big

14   industry-wide effort, as well as engagement with the staff.

15   I think one of the things we now see in hindsight

16   looking back is there were some things we all thought we agreed to,

17   that perhaps we were saying different things to each other or hearing

18   different things.   Because as we've tried to apply or implement the

19   things we agreed to, we're finding that there's different versions of, you

20   know, some interpretable words.

21   So there are some things like when we say "common

22   cause failure," what does that mean?   Okay, let's go resolve that.

23   Let's get everybody on the same page.   Just a stable, regulatory

24   structure, and I know you've probably heard about this.

25   In particular for the operating plants, the way that the

26   licensing gears turn these days really doesn't work well for a utility for a

1   licensee, from a managed risk cost invested over the time as it affects

2   risk profile.   That makes it hard, and we think that -- we think that those

3   gears can be adjusted a little bit, in a manner that still satisfies

4   everybody's needs and becomes much more of an enabler to these

5   projects being done as opposed to a hindrance.   That's another area to

6   work together.

7   Then more in the spirit of an anxiety than a gap or an

8   issue, as we look forward as an industry to closing ITAAC at Vogtle and

9   Summer, there's just anxiety of are we all on the same page as to how

10   we're going to do that.   There's questions.   A lot of people in the I&C

11   community are nervous that some of the things, you know.

12   In 2010, we thought we had agreement between

13   industry and the staff on a number of technical topics.   We've learned

14   we really didn't.

15   Today, we think we have agreement on how to do

16   some of these ITAAC inspections, and whether we do or don't is a

17   question we have to go ask, and we'd like to answer that question in

18   advance, not at the last moment.

19   You put all those things together and the chief nuclear

20   officers, the CEOs asked NEI to put together a working group of

21   industry executives, to help drive this and to help provide the leadership

22   and the coordination of all the various industry groups and company's

23   activities, and to get to a better place.

24   Ron Jones from SCANA is the leader.   He's the

25   chairman of that group.   He had a commitment today; that's why I'm

26   here for Ron.   I'm on that group with Ron, as well as some other

1   industry executives, and we're working together as was with others

2   from our companies and industry to try to provide that leadership, that

3   guidance, a framework for engagement that will allow these issues,

4   these gaps to get resolved once and for all.

5   We think that's doable and that's our goal.   We're

6   working on a road map.   Let me back up and just say we don't think

7   that the issue is missing guidance or more research or more paper.

8   We think everything's there.   We think that from the things that are

9   within our own control on the industry implementation side, and with

10   regard to the extent the industry engages with the staff.

11   We think it's more about coming together on this six

12   feet of paper, what matters, how to implement it, what's the way to

13   interpret it, because we think most of the research is done.   We think

14   that things are out there.   We just have to, you know, it's more agreeing

15   on it.

16   So the purpose of -- the road map we're putting

17   together is to guide, from an industry standpoint, to guide us through

18   that process.   It's to paint the big picture, see the broader landscape,

19   see how all these things fit together, see how they prioritize.

20   One of the things we're looking very hard at is what is

21   the most important critical items that we can prioritize on that are

22   prerequisites for other discussions and other decisions.

23   We're going to use that road map and it's going to paint

24   the picture for the next several years, of how -- our version of how to get

25   these issues resolved, how to do a handful of pilot projects, and to do

26   that in a collaborative manner which not just answers the questions but

1   does it in what we'll called a sustained, reliable manner, so that the rest

2   of the industry can then go forward and take advantage of the

3   opportunities.

4   We're early.   We've only really been working this year.

5   The road map isn't quite done.   But since I have the floor, there are a

6   couple of asks or suggestions, recommendations that we'd like to make

7   or throw out there.

8   One I already alluded to, and that's the engagement on

9   the 50.59 guidance.   We think that would be good for everybody.   We

10   think we have a better set of guidance now.   We hope and expect the

11   staff will agree.

12   The proposed rule on 603, we're all for updating the

13   regulations.   We're all for going to later versions of the standards.   We

14   think that's a good move in the right direction.   We think some of the

15   additional considerations that have been written into the rule actually

16   are harmful.

17   We'd rather, if it's a choice of that or nothing, we'd

18   prefer nothing.   So our recommendation would be to put that on hold.

19   We're looking forward to the staff engaging us on a working group

20   manner, and then finally we're looking forward to the Commissioners

21   being engaged and interested, to help influence and help set the

22   priorities that leads this to resolution.

23   Because I think, you know, the big question for the last

24   few years has been, you know, people ask can you do these projects

25   reliably, safely, on schedule, on budget without licensing uncertainty.   I

26   believe the answer's yes.   With confidence, I believe the answer's yes

1   and we want everyone together to be working towards, you know, how

2   do we do that and demonstrating it and not asking the question of can

3   we.   That's where we'd like to get to.

4   I'm working on the assumption that some of these

5   other presenters will get into a little more detail on some of the things I

6   hit.

7   CHAIRMAN BURNS: Thank you. Mr. Connelly.

8   MR. CONNELLY: Good afternoon. First, I'd like to

9   take a moment to thank the Commissioners for providing us an

10   opportunity to present our perspective. There are several critical

11   issues related to the application of digital technology. We greatly

12   appreciate the opportunity to speak to them.

13   At the risk of stating the obvious, we share a common

14   goal, safe and reliable operations. In our opinion, one of the best ways

15   for us to achieve that common goal is for licensees to upgrade their

16   facilities using the best available technologies. Establishing a clear

17   and unambiguous regulatory framework is a key enabler for that.

18   Turning our attention to the third slide, I want to spend

19   just a moment on this. Specifically, Exelon's operating experience on

20   digital upgrades. We've been implementing non-safety related digital

21   upgrades for about 20 years, starting with the feedwater systems at

22   Dresden, LaSalle, Quad Cities and Limerick.

23   That was followed by turbine control system upgrades

24   across most of the Midwest fleet and those continue today across both

25   the Mid-Altantic and Northeast. Our primary focus was to improve

26   system performance through great fault tolerance and elimination of

1   single point vulnerabilities.

2   So we looked at those projects and went back and

3   looked historically over our scram data, going all the way back to 1980.

4   The analysis we conducted paints a pretty compelling picture, which is

5   reflected on this slide.

6   If you look at the feedwater system specifically, we

7   observed a 95 percent reduction in scram rate between the analog

8   systems and the digital systems. Now we did normalize this data so

9   we got it in terms of unit years, so we could compare apples to apples.

10   We looked similarly at the PWR controls and observed

11   an 83 percent reduction and the BWR turbine controls at 74 percent

12   reduction. So clearly, that's a fairly compelling picture. Digital

13   upgrades significantly reduce initiating events. So there are obvious

14   opportunities there.

15   Next slide. I included this slide just as another point of

16   data, if you will. This information is widely available on the Internet.

17   You can find it on the FAA website, NTSB, various places. You'll find

18   various iterations of this slide in a number of places.

19   This is a pictorial representation of hull loss events

20   across the commercial aviation sector. So this wasn't developed for

21   digital technology specifically, but there's an interesting nugget of

22   wisdom that can be discerned from this.

23   The 747-400 was the first truly digital aircraft, the first

24   glass cockpit aircraft. Now I will tell you that there is some overlap

25   there. These product life cycles tend to be fairly lengthy, so there is

26   going to be some overlap.

1   But the interesting takeaway from this slide is if you

2   kind of draw a line through just above the 747-400, before that is analog

3   aircraft; below that is digital aircraft.   Now obviously this isn't the only

4   factor at play.   But there's an interesting takeaway from this.   If you

5   look at digital aircraft, while analog aircraft are safe, digital aircraft are

6   safer.

7   The commercial aviation sector has fully embraced

8   digital technology, and I think there's similar opportunities for us to gain

9   from that experience.

10   Turning to the next slide, I do want to briefly touch on

11 equipment obsolescence.   Considering that a typical domestic plant

12 has been in service roughly 30 years, and also with the full knowledge

13 that and the inescapable reality that all electronic components have a

14 finite life span.

15   Our   exposure   to   equipment   obsolescence   is

16 significant.   We actively manage these issues.   We have strategies in

17 place to mitigate the risk.   But the ability to use well-vetted digital

18 solutions would be beneficial to all parties concerned.

19   The other thing that I'd like the Commission to take

20 away from this discussion is if you think about the nuclear sector, we're

21 a small slice of a very large industrial control sector pie.   If you look

22 outside of nuclear, if you look at petrochemical, pharma, the fossil

23 world, digital is the preferred solution.

24   It is the preferred solution because of its capability,

25 reliability, accuracy and cost effectiveness.   So you know, separating

26 ourselves from those product lines and those benefits is probably not in

1   our best advantage.

2   Next slide.   Cybersecurity.   I'm only going to touch on

3   this very briefly.   I know it's kind of a significant issue for the industry,

4   but I do want to touch on a couple of things in terms of cybersecurity.

5   The industry and staff have made substantial progress

6   in resolving implementation issues.   There are mechanisms in place,

7   the Cybersecurity Task Force and the interface between NEI and the

8   Commission and the staff.   We have made very significant progress.

9   The point that I would like to make, however, is that

10   Milestone 8, our full compliance deadline for most licensees that's

11   12/31 of 2017.   So effectively we have two years to completely

12   implement the balance of the program.   So timely resolution of issues

13   as they emerge is critically important to all parties concerned.

14   The other point I'd like to make is that cybersecurity

15   and digital I&C really can't be considered in isolation from each other.

16   They're concentric rings around the same center, to a large degree, and

17   there's a need to coordinate both the digital I&C piece of this and the

18   cybersecurity piece of this, and we actually have that through the Digital

19   Working Group.

20   That's an opportunity.   All of those stakeholders are

21   involved in that discussion.   So that's an opportunity to get that

22   coordination between the various elements and industry stakeholders.

23   Next slide.   I'm not going to belabor this one in the

24   interest of respecting people's time.   I did include this in a presentation,

25   just to kind of lay out the landscape that we're in right now.   Most of

26   what you're looking at here in this slide is applicable to safety related

1   modifications, but there is some applicability to non-safety related

2   applications as well.

3   This speaks volumes to the need for a clear,

4   unambiguous, graded, stable regulatory framework for both digital I&C

5   and cybersecurity, and frankly we do have models that we can draw

6   from- from other sectors.   I guess the key takeaway I'd like to leave the

7   Commissioners with is that while the technology itself can be complex,

8   the framework itself could be simplified and made more streamlined.

9   Next slide.   Unless there are dissenting opinions,

10   IEEE 603-2009, we're going to be talking about that in detail in the next

11   presentation, and we're certainly able to field more questions.   The

12   only thing I'd like to say here is that from our perspective, it's kind of like

13   the Hippocratic oath.

14   The standard in place right now does no harm if we

15   leave it as is.   But our concern is- is that it may further muddy the

16   waters and introduce yet another variable, and we'll be talking about

17   that in more detail in just a moment.

18   So as Bob had alluded to, while I have the floor there's

19   a couple of requests I would like to make.   Again, and you'll hear this

20   throughout the presentations and the discussion, a clear,

21   unambiguous, graded and stable regulatory framework for both digital

22   I&C and cybersecurity is critically important to all parties concerned.

23   Again, we'd ask that we maintain IEEE 603-1991 as

24   the endorsed standard, because it doesn't adversely impact the

25   industry's ability to modernize or introduce yet another variable.   The

26   agency and industry should work to develop consensus solutions to key

1   technical issues and we've alluded to that throughout the previous

2   comments, and we'll be discussing further following presentations.

3   Specifically, the application of the 50.59 process, the

4   technical reports that are being developed by EPRI and dealing and

5   addressing software common cause failure.   The agency and industry

6   should continue efforts to improve NEI-08-09 revision.   The currently

7   endorsed version is Revision 6, Revision 7.

8   We have had discussions with the staff.   There are a

9   handful of things that we would like to get clarity around.   We have

10   been -- we have had some very productive discussions with the staff

11   and I think we have a success path there.

12   Similarly, the agency and industry should continue to

13   refine NEI-13-10.   For those who are not familiar with 13-10, it

14   introduces a graded approach to cybersecurity.   Revision 3 was a

15   watershed event.   I would characterize it as a watershed event.   We

16   did gain a lot of ground with 13-10.

17   There are opportunities to improve it in subtle ways by

18   including better worked examples of what good looks like and for

19   potentially get some security programmatic assets out of the direct

20   impact category and into indirect, so we can treat them with a subset of

21   controls.   And again, we've had good success working with the staff to

22   get these issues resolved, on the table and resolved.

23   The   last   thing   I   would   point   out   is   there   are

24   methodologies that we can draw from as we work our way through this

25   road mapping.   You know, NAVSEA 08, aerospace, pharmaceutical,

26   petrochemical.   There are other standards and models that we can fold

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

2   Nuclear tends to be very inwardly focused, but there

3   are other avenues, venues, standards, methodologies that we should

4   consider as part of this process.   With that, I'll yield 27 seconds.

5   CHAIRMAN BURNS: Mr. Harmon, you don't have to

6   use the 27 seconds.

7   MR. HARMON: I'll start with a fresh ten.   Good

8   afternoon and thank you, Commission, for this opportunity to talk you

9   about digital instrumentation controls.   I come to you with two hats

10   today.

11   One is from an vendor's perspective in the nuclear

12   industry.   I work for Westinghouse, but also for over 25 years I've been

13   a member of the IEEE Standards Development organization and

14   Nuclear Power Engineering Committee.   So I'd like to talk to you a

15   little bit from an IEEE perspective as well.

16   CHAIRMAN BURNS: Is your mic on?

17   MR. HARMON: Oops.   Okay, thank you.   That

18   sounds better.   From a Westinghouse perspective, we are heavily

19   invested and believe in digital instrumentation controls.   We have an

20   approved common Q platform that we've had before the NRC a couple

21   of times now, and we use it for our digital instrumentation control safety

22   system implementations.

23   We use that as a key attribute to our new plant designs.

24   So not only for upgrades, but in our new plants, we have 14 AP1000

25   plants that are being built around the world, ten in China, as you

26   probably know four here in the United States.

1   We're also using this same technology, the digital

2   instrumentation controls to implement the APR1400 plants in South

3   Korea, Shin-Kori 3 and 4, and at Barakah in the United Arab Emirates.

4   That happens to be the project that I currently work on the APR1400

5   projects.

6   If you were to come to either of those two type design's

7   control rooms, you would be much harder pressed to find meters and

8   dials and switches.

9   There are a few, but primarily you see large screen

10 displays, flat panel displays and the technology behind those out in the

11 plant is all digital safety systems and non-safety systems.   So we are

12 implementing our new designs with digital I&C.

13   We also do upgrades obviously, and as my colleagues

14 have mentioned, we have been involved in reactor protection system,

15 an   engineering   safety   feature   actuation   system   upgrades,

16 post-accident monitoring systems, as well as on the S for safety side,

17 as well as non-safety implementing feedwater control systems, turbine

18 control systems and many other systems that we can upgrade to digital

19 kind of on a piece by piece one at a time perspective.

20   That's been done both here in the U.S. and at other

21 places around the world.   We think there's a big benefit, and in the

22 second slide I talk about some of the benefits.   My colleagues have

23 also mentioned these.

24   Certainly, as John mentioned, there's a decrease in the

25 probability of events and they've seen this particularly with feedwater

26 control systems, turbine control systems, that we don't challenge the

1   safety systems as much anymore. That's certainly a benefit to a safety

2   aspect of the plants and as well as operations obviously.

3   A lot of functional improvements. The operators can

4   get the information they need for different plant situations, different

5   plant modes, put together with the controls, the information so that they

6   can use it effectively, and there's a great capability to do that. There's

7   also a capability functionally for redundancy and other functional

8   improvements that allow these plants to be -- to move forward in

9   reliability, as well as the operabilityl.

10   One aspect that's unique to digital, it allows us to do

11   maintenance, surveillance, etcetera, from a remote location. Some of

12   the intelligent devices, sensors and components can be configured.

13   Troubleshooting can occur, as well as calibration from a remote

14   location. There's no need to go around the plant.

15   This allows a plant, an existing plant or new plants to

16   focus on some of the more maybe important or higher priority

17   maintenance aspects. I mentioned human-machine interface.

18   There's a great opportunity and we've taken advantage of that to

19   improve the human-machine interface. Let the operators get the

20   information they need for their tasks in the context where they need it.

21   Then as was mentioned, for obsolescence, we really

22   think that digital instrumentation and controls is a preferred opportunity

23   for us to address obsolescence with a better system what exists today.

24   So that's the Westinghouse perspective. Let me talk

25   a little bit about IEEE. The IEEE Nuclear Power Engineering

26   Committee, I'll call that NPEC from this point on, is the committee within

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

2   I am a member of the Nuclear Power Engineering

3   Committee.   Also one of the subcomittees that IEEE 603 came from is

4   the Safety-Related Subcommittee.   For three years, I was the

5   chairman of that subcommittee back about five years ago, and have

6   worked on that subcommittee for close to 20 years.

7   In that subcommittee, we have working groups.

8   There is a working group dedicated to maintaining IEEE 603 as well as

9   one of the other standards.   An important point here is that the IEEE is

10   adamant about maintaining a diverse constituency in its working

11   groups, as well as NPEC and the subcomittees.

12   So we want perspectives from vendors, from utilities,

13   from regulators, and we have people from the NRC as well as other

14   regulators on our working groups and on our subcommittees.   When

15   an IEEE standard like 603 is revised, it comes to ballot and is put before

16   an industry consensus group in a standards association, which is

17   somewhat independent of the Nuclear Power Engineering Committee

18   itself.

19   Again in developing the ballot pool, we try to get a

20   consensus that represents a diverse set of individuals, who can then

21   ballot the standard and make comments.   The working group then

22   goes through and addresses the comments, to come up with the actual

23   revision to the standard.

24   The point here is that IEEE 603 really went through an

25   industry consensus, including the perspective of regulators, as it went

26   through its process of being voted on back in 2009.   We think that does

1   represent a good industry consensus.

2   If we go to the fifth slide, as I mentioned, it was -- we

3   had this broad perspective, and IEEE 603 is actually currently being

4   worked on again.   We've learned some things through this rulemaking

5   process and have feedback to IEEE 603.

6   The working group established a project authorization

7   request, which allows them to modify, to revise the standard.   That was

8   approved back in February of 2015 and they're now working on

9   incorporating some of the lessons learned, the information from the

10   rulemaking effort back into IEEE 603.

11   Particularly the technical, those aspects of rulemaking

12   that focus on technical issues, we're trying to again improve 603.

13   There's another broader standard to IEEE 603, IEEE 7432.   That is the

14   standard criteria for programmable digital devices and safety systems

15   of nuclear power generating stations.

16   It used to be called digital computers, but now we've

17   expanded it to include programmable digital devices, FPGAs for

18   example.   That standard has just been balloted and will be issued a

19   revision to that in early 2016.

20   It contains significantly more criteria for these digital

21   devices, includes criteria for -- to address common cause failure in

22   safety systems with digital devices.   So we think that standard now,

23   which the NRC has said they intend to endorse with Reg Guide 1.152,

24   provides a good framework for addressing the digital I&C concerns at a

25   more detailed level in some aspects than IEEE 603.

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

1   IEEE 603 rulemaking. One of them is that the conditions that were

2   aforementioned do add detailed criteria to the proposed rule.   It seems

3   different than what's been done with the Code of Federal Regulations

4   previously.

5   It may not be so appropriate for the Code of Federal

6   Regulations, but more appropriate for a Reg Guide, and that's what we

7   see typically happening with an IEEE standard as the staff goes

8   through and creates a Reg Guide with their regulatory positions related

9   to a standard.

10   Also one of the issues that we have, especially at

11   Westinghouse where, as I mentioned, we do new plants and digital

12   upgrades, there are different regulations being applied in some

13   instances to new reactors and existing reactors.

14   That gives us concern in that we have one platform,

15   one set of criteria that we use to design our systems, and we think it's

16   inappropriate to have regulations that are diverse, are different from

17   new reactors and existing reactors.

18   Then some criteria, special criteria being applied in the

19   data communications that is contradictory to what was in the interim

20   staff guidance.

21   We   have   concerns   about   that   related   to   data

22   communications, and we think that there should be a consistent set of

23   industry standards and rules from the NRC related to the digital I&C and

24   in this case data communications.

25   So to wrap that up, I think I share a concern with my

26   colleagues that the existing 603 endorsement in the Code of Federal

1   Regulations does no harm at this point.   Some of the conditions being

2   applied may be detrimental to us, and we'd like to maybe work together

3   to move forward in a different approach for the industry. I'll yield like 17

4   seconds.

5   CHAIRMAN BURNS: Thank you.   Mr. Cofer.

6   MR. COFER: Thank you.   Am I on?   How about

7   that?   Okay.   So I appreciated Commissioner Ostendorff's opening

8   remarks about the S3G in the late 80's.   I worked in NAVSEA 08 and

9   did some work on that prototype plant, as well as others before joining

10   the aerospace industry.

11   So this will be somewhat different, as I'll offer you some

12   perspectives from the aerospace industry.   This is -- I've come to

13   appreciate that this is particularly relevant, because NAVSEA 08 since

14   my tenure there has gone, you know, kind of faced the same problem

15   and moved from analog to digital I&C and the way that they did that was

16   to take motivation from the guidelines, the guidance used in the

17   aerospace industry.

18   So perhaps there's something useful there.   So if we

19   could go through the slides here, I'll make reference to several of the

20   points there.   It makes sense to talk about our industries, because we

21   do have a lot of similar concerns.

22   We're safety-critical, we're regulated, we use

23   replication for fault tolerance and more and more we are software

24   intensive, one difference being the nuclear plant is designed to be fail

25   safe.   You can shut it down.   An airplane has to be fail operational.

26   You can't stop flying.

1   John alluded to some of the history of digital flight

2   control and fly by wire systems.   I won't go into that.   There is a long

3   history of this in the aerospace industry, going back into the early Apollo

4   program work and advanced through various NASA programs until the

5   Airbus A320.

6   I think I have a misprint in the printed materials, but in

7   1984 Airbus chose to go to an all digital and redundant flight control

8   system.   That was a big change for the commercial world at the time,

9   but they did have this 20 years of work to build upon.

10   The reasons for doing this, of course, were to reduce

11   weight and costs, but also to improve some of the functionality.   It

12   improved automation with autopilot systems, advanced functionality

13   like stability augmentation that could be implemented digitally, and then

14   now relying on safety through redundancy.

15   So no mechanical or physical backups.   All of the

16   redundancy is implemented in the digital flight control systems.

17   Next slide shows our own version of the six feet of

18   paper that regulates systems and software, especially in our industry,

19   starting with CFR Title 14, Part 25 for airworthiness for large

20   commercial aircraft.   But there's a, you know, our own chain of

21   documents that goes from the system and safety analysis level all the

22   way down to design assurance for digital hardware and software.

23   The block in the middle on integrated modularity

24   beyond X is kind of interesting, because that provides guidance for how

25   to host multiple software that has different levels of criticality on the

26   same hardware platform; what you need to do, what are some of the

1 different acceptable approaches for doing that. So we have guidance

2 for that in our industry.

3   On the next slide, why does all of this work in our

4 industry? Largely it's because as in the nuclear industry, we're a very

5 conservative industry with a strong safety culture historically.

6   We've, I don't know exactly how it works in the nuclear

7 industry, but in aerospace there is a consensus-based process

8 between industry and regulators to develop guidance for conforming to

9 the top level regulatory requirements.

10   But ultimately there is just a ton of testing that is done,

11 and for the safety critical things, what we call Level A, there's complete

12 transparency and visibility into all the code, all the design artifacts.

13   COTS software and components can be used in

14 aircraft, but at the highest levels of criticality things like, for example we

15 use commercial real-time operating systems in most aircraft today.

16   We have access to the code. That all can be

17 examined and tested. It's not hidden from us. It's not hidden from the

18 regulators either.

19   Next slide. But we, as all folks that use software, are

20 facing a challenge. The next slide will just show us. Go ahead and hit

21 next again, that this is a graph of the amount of software in military

22 aircraft, and if you look, finally the last point is the F-35 that we hear so

23 much about in the news.

24   We have a similar curve commercial aircraft. The

25 amount of software that we're having to grapple with, the complexity of

26 software-based systems is growing dramatically. There's many other

1   challenges that we're dealing with, as well as the use of software to do

2   safety-critical functions in aircraft continues to grow.

3   The next slide shows kind of what's going -- what's

4   happened very recently, to try to grapple with some of these things at

5   least at the software component level.

6   I was involved on the committee that drafted some

7   updated guidance, and you can see some of the things that we dealt

8   with were model-based development, tools, object-oriented software

9   and mathematical analysis techniques called flow methods and how to

10   incorporate guidance for those into our software processes.

11   So this is the latest and greatest guidance.   It's out on

12   the street.   Provides instruction on how those kinds of technologies

13   ought to be handled.   The one that I work on in particular is this last

14   one, the mathematical analysis techniques.

15   Next slide, and I'll make a few comments on that, that

16   this is nothing more than saying that for software engineering to be a

17   true engineering discipline, we need to use mathematically-based tools

18   to build and analyze those systems, just like we do for mechanical

19   systems.

20   We build bridges; we do a finite element analysis.

21   That's the bridge falling down in Minneapolis where I live several years

22   ago, where somebody actually made a mistake in their analysis.   So

23   we ought to be able to do the same sorts of things, apply analysis tools

24   to the engineering of safety-critical software systems, and indeed the

25   state of the art allows us to do that now.

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

1   of things that we have been doing under funding, S&T funding from

2   NASA and DARPA and other government agencies, to develop the

3   tools, not just at the software component level but also at the system

4   architecture level, to allow us to build accurate, generative models for

5   software architectures, and not just test but prove the safety and

6   security properties of those designs.

7   The DARPA work has primarily been focused on

8   cybersecurity properties; the NASA work has been focused on safety

9   properties. But together we've developed and others that work in the

10   same area that Rockwell does, universities and other aerospace

11   companies, have developed good tools that allow us to reason about

12   large complex systems, to prove isolation between components when

13   it's necessary, to analyze the fault tolerance behaviors, to actually do

14   proofs of correctness of software-based systems.

15   So let me just conclude with a few lessons learned.

16   Go ahead and go to the next one. So our conclusions are that the

17   model-based development tools are -- have been successfully adopted

18   by the aviation industry and used for all kinds of safety-critical software,

19   and the analysis tools that we have are sufficiently mature and practical

20   for application on real products, real projects and success at the

21   software component level.

22   So the unit level, if you will, is now being replicated at

23   the system level to manage the complexity of an avionic suite as a

24   whole, and allow us to verify safety properties and to build what are

25   called assurance cases that can be integrated with system architecture

26   models.

1   Next regarding certification, certification processes

2   change slowly because there's competing concerns of industry and

3   regulators.   But in fact, it has been possible for us to develop

4   certification guidance for airborne software that addresses new

5   technologies, such as those that I listed before.

6   This has been a joint effort between industry and

7   regulators, and we find that case studies where you actually show what

8   these new technologies look like, what evidence they produce, how

9   they satisfy certification objectives are very helpful in helping people

10   make this jump between theory and practice.

11   Finally, cost matters as always.   Most defects in our

12   experience occur early in the design process, indeed at the

13   requirements stage of a system and defects are much more expensive

14   to correct later in the process.

15   So it makes sense just from a cost standpoint for us to

16   focus our efforts on analysis at the earliest stages of development,

17   analyzing requirements and design specifications to prove them correct

18   before we go and -- any defects turn into implementation defects that

19   have to be corrected at a much greater cost later on in the process or, in

20   the worse case, after delivery of a system.

21   Many studies have shown a good return on investment

22   for using these kinds of analysis techniques early in the life cycle of a

23   system.   Thank you very much.

24   CHAIRMAN   BURNS: Thank   you.   Professor

25   Scherlis.

26   PROFESSOR   SCHERLIS: Thanks.   I thank the

1   Commission for the invitation to speak today.   Regarding my

2   background, I've spent most of my career, about three decades,

3   working on the technical aspects of software assurance, but I also have

4   some government experience.

5   Darren Cofer mentioned DARPA projects. I was -- I

6   spent seven years at DARPA as an IPA followed by an SES

7   appointment, and then returned to Carnegie-Mellon. This was 22

8   years ago, but I felt I should mention that.

9   My remark today focuses on prospects for software

10   assurance, including security considerations. The theme of my

11   remark is evidence, specifically the role of structured technical

12   evidence to support human assurance judgments.

13   Next slide, please. The role of evidence was

14   identified as early as 1968, in the first NATO workshop on software.

15   This was the workshop where the phrase "software engineering" was

16   coined. The aim of any testing scheme is to ensure that the customer

17   gets substantially the software that he ordered. This was the old days,

18   and it must provide the customer with convincing evidence that this is

19   so.

20   We all know that the current generation of evaluation

21   standards in many areas do not follow this advice so closely. The

22   standards tend to focus on aspects of process, on system design, on

23   test and evaluation practices. A little bit less focused on the

24   operational artifacts themselves.

25   There are good reasons. I shouldn't say good; I

26   should say there are understandable, historical reasons for this lack of

1   focus.   My belief and the premise of my talk is that we are now at a

2   point where we can take this advice from almost 50 years ago more

3   seriously.

4   I say now because on the one hand the development

5   of modeling analysis, as in fact Darren Cofer just described, has moved

6   to a point.   But in addition, the development of tools and data

7   management techniques has also advanced dramatically.   The

8   development of digital systems is now data-intensive.

9   We have the potential, I would say more than before to

10 get from trust to verify, where we can have a meaningful impact on our

11 ability to develop and assure safety-critical systems that are also highly

12 capable.   There are things that can be done soon.   The DO-178 family

13 of standards is good evidence of that.

14   My remark is really how can we get to very high levels

15 of capability for digital I&C and do that in a cost effective way.   What's

16 the mechanism to do that?   As the speakers, everybody has noted,

17 there's great opportunity for digital I&C.

18   So of course complicating this is the use of COTS

19 components, commercial off the shelf.   Also the rich supply chains that

20 are now increasingly evident for digital systems; common cause

21 failures, how do we define and assess diversity and security in the

22 presence of increasingly sophisticated adversaries.   Supply chain is

23 important, especially when we have the diversity of suppliers.

24   Next slide, please.   So I want to point out some of the

25 software challenges we face.   These apply in the general context, but

26 also significantly for safety-critical systems.   Some are less important

1   because we accept certain a priori constraints for safety critical.   But

2   we should recognize that we are doing that.

3   A general point about software.   I would say for an

4   extremely wide range of systems, software is the most significant

5   building material of our age.   Functionality is moving from physical and

6   analog to digital for very good reasons.

7   But software is also the material of cybersecurity, the

8   offensive and defensive weaponry are constructed from it, as are the

9   assets we're trying to protect.   The limits of software capability.   Again

10   as Darren Cofer has noted, derive from mathematical and not physical

11   features.

12   There's a kind of unboundedness, such that as we

13   aspire to greater levels of capability, we're very often able to get there.

14   This up and to the right concept, which looks a lot like Moore's law but is

15   a very different phenomenon, is going to continue through our lifetimes.

16   This is due to powerful languages, models, analysis,

17   tools.   But it's also due to our ability to assemble systems from

18   components.   This is why supply chain is a very important issue.

19   Think about, for example, your mobile device.   There are thousands of

20   suppliers that contribute just to what's on one person's mobile device.

21   But our ability, I should say, also to do the modeling

22   analysis to assure systems is also proceeding at a very rapid pace.   It's

23   just these two things are moving together.   So there are very few

24   categories of systems that are sort of genuinely not buggy.

25   Aerospace, particularly flight controls, is an exception

26   to that because of the success of those standards.   But we hold back

1   on functionality and capability in that context in order to meet those

2   criteria, because software's abstract evaluation is a very different kind

3   of proposition.

4   So I want to mention two other ideas on that first list on

5   that slide.   One is common cause failures.   Of course we want to go

6   after both sides of the risk product, reduce consequences through

7   better modeling and analysis, but also likelihood through diversity and

8   defense in depth.

9   The second point is continuous cyber attack.   We

10   have to recognize that, you know, we kind of focus on the network.

11   That's where the adrenalin is flowing.   It's like fire engines at the fire,

12   fighting the fire.   But really it's the fire codes; it's how we build things.

13   It's the supply chain and insiders in fact as well that we have to focus in.

14   Regarding evaluation, on the slide I inventory some of

15   the challenges of current practices.   A lot of the standards help with

16   quality, but they do not deliver quality, and you can read the list.   You

17   know, informal documents, a lot of reverse engineering, designs that

18   are difficult to evaluate and heuristic practices.

19   But I want to move to the bottom of that slide, the

20   business structures.   There are many structures we've become -- to

21   which we've become habituated in the mainstream practice.   We

22   cannot successfully evaluate a black box executable, you know, and

23   get any kind of an assurance judgment.   We need the transparency.

24   So if we're going to make use of COTS for safety

25   critical, we have to gain that transparency.   Again, this was discussed.

26   And even when we have just the source code, really we're not able to

1   draw conclusions with confidence.

2   So let's go to the next slide, please.   This just

3   mentions some points of experience, related research projects, kind of

4   analogous to Darren Cofer's slide.   My point here is that the research

5   focus is in a sense to push that tradeoff curve out, to get more safety

6   and security with acceptable cost, but also gaining increasing

7   capability.   So this is kind of the long perspective.

8   So now let's move to the next chart.   This is my last

9   chart and my main point.   Software development technology and

10   infrastructure have evolved, I would say, to a point where we can do

11   things in a different way.

12   There's a timeliness argument that I'm going to make.

13   There are a lot of ideas that have been around for a while, but because

14   of the evolution of the technology, including models, analyses, the

15   treatment of data from development practices, we are able to take

16   these ideas seriously.

17   The idea is to contemplate the creation of what we

18   could call chains of evidence to support assurance claims.   What I

19   mean is an explicit linkage of dependencies that connect the models

20   and the analyses and all the various -- the test cases and all the various

21   other artifacts related to a system.

22   This linkage, even back to requirements and the safety

23   and hazard analyses, can help us make that assurance judgment much

24   more efficiently.

25   So as we build the systems, as we advance this

26   development of evidence to the earliest stages of development, we

1   create an opportunity to make the evaluation process much more

2   efficient, and therefore to enable upgrade and evolution, recertification

3   also to be efficient.

4   Really what is contributing in a great way to this is the

5   increasingly expressive models and evaluation methods, analysis

6   methods that focus on software artifacts. Code obviously. The

7   Google repository has a billion lines of code in it, tens of thousands of

8   transactions a day. Virtually every transaction is recorded back

9   through the fullness of time.

10   This is standard practice for the smallest through the

11   largest software development teams. That's code configuration. The

12   opportunity is to link in the models and the analyses that many of us are

13   involved with, that pervade the DO-178 community, and to link those in

14   with hazard and safety models and analytics, and create those

15   dependency linkages and rationale structures.

16   In the past, many of these models and data were lost.

17   They were in people's heads. They were on white boards. We pay a

18   high price in reverse engineering to recover this. The big change is

19   now we can express these efficiently and we can do analyses on that

20   basis. Thank you.

21   CHAIRMAN BURNS: Well thank you all for your

22   presentations. I'll start off with a few questions. I guess in terms I'll

23   put first to 60 percent of the panel I guess, Mr. Coward, Mr. Connelly,

24   Mr. Harmon, I'm trying -- in trying to understand some of the industry

25   concerns, the nuclear industry concerns with where we are or where we

26   might be going with digital requirements, but also it strikes me the

1   concern is not only the potential for a particular rule that we have before

2   us, but it's also a question about disconnects, if you will, between where

3   the existing framework is.

4   For example, and Mr. Coward you talked about the

5   50.59 process, where is that -- how has that divergence come up,

6   because I think you said, talked about in 2010 we thought we were sort

7   of at the same wave length, but that's sort of grown apart.

8   Where are the biggest push points or pressure points

9   in this needing to gain a sort of more common perspective?

10   MR. COWARD: Well I guess what I'm going to do is

11   I'm going to defer to the guy who is nominally responsible for these, to

12   give a better -- I could comment, but I'll let John give a few specific

13   examples.

14   CHAIRMAN BURNS: Okay.

15   MR. CONNELLY: And feel free to jump in any time

16   you'd like.

17   MR. COWARD: I will.

18   MR. CONNELLY: Common cause failure.   That's

19   current, you know, what we're currently working through right now for

20   the NEI-101 task force.

21   You know, trying to understand or getting a common

22   sense of understanding in terms of what are the initiators for common

23   cause failure; what are the appropriate mechanisms for mitigating

24   common cause failure?   How do those translate into the designs that

25   we're implementing?

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

1   for you know, what is the right way to deal with software or all forms

2   of -- including software, all forms of common cause failure.

3   MR. COWARD: And I think a lot of it, Commissioner,

4   Chairman, is there's different ways to look at this.   Part of the challenge

5   is we're talking about the application of -- by our standards new

6   technology into these plants, right?

7   The rest of the world chuckles at us when we say that,

8   but we're talking about the application of new technology and there's

9   always going to be lessons learned and things that come up, where you

10   -- from doing this one, the next one you're smarter and then you're

11   smarter, then you're smarter.

12   I think one of the things that's happened is especially

13   when you look at people considering safety-related projects, as well as

14   some of the bigger non-safety related, all of us together haven't been as

15   good as we could have been, at really, truly understanding those

16   lessons, and quite frankly getting the kind of stream of projects that

17   allows all of us to have some momentum as we're going forward.

18   You know, one of the ones we point to a lot is a plant

19   that decided to do elements of digital upgrade in their feedwater

20   system.   That's not just the software, but some of the components, and

21   through the process someone said hey, we can make this even better

22   and not just control this glass, but we can control this glass and we can

23   control this book.

24   That was a great idea, and they probably did a good

25   project.   But what they missed was they took a glass, a book and

26   whatever my other prop was, the other glass that previously were three

1   independent, separate devices and connected them together in a way

2   that even though it was a non-safety related project, and the --

3   I'll call the posture of the people doing it was to think

4   this is just a balance of point, secondary system, non-safety related

5   project to replace analog controls with digital, they created new

6   potential failure modes that could affect multiple components at one

7   time, and actually introduced some pretty good 50.59 questions, all

8   right.

9   But because we didn't have all of us together, because

10   we haven't had the stream of those projects going to learn together, and

11   to share the lessons and to feed that back collectively together, it was a

12   one-off, as opposed to occurring in a way that we all can embrace it.

13   So there's a lot of factors going on here, if that makes

14   any sense.

15   CHAIRMAN BURNS: The part of it that's curious to

16   me is whether -- and you touched on it -- the artifact in terms of the

17   development over the years.   I'll give you a personal example.

18   A representative, a company that also builds nuclear

19   plants or designs nuclear power plants, but also does refrigerators, and

20   it's not Westinghouse --

21   (Laughter.)

22   CHAIRMAN BURNS: -- basically told us when we

23   were having some issues, they said, well, you don't have a refrigerator.

24   You have a digital device.   And it's very true.   And he says, the

25   problem was the software, it needed a software upgrade whereas you

26   don't have -- and I'm wondering is our -- is the lexicon we use in terms of

1   regulation which was developed in -- I won't call it a pre-digital age, but

2   in an age where it's more analog than it is digital?

3   There's something of how we talk about safety-related,

4   important to safety, other things like that, doesn't quite fit.

5   MR. COWARD: I'm not sure if this is going to

6   specifically answer your question, but I will tell you I do believe that the

7   way we talk is a consideration.   Because there are -- I like to use the

8   phrase we've ended up using some interpretable words and some

9   interpretable phrases.

10   And instead of having -- over the years there's been a

11   number of instances where instead of having crisp, clear, rigorous

12   three-way communication to confirm that what I just said to you, that

13   you have the same exact meaning, understanding of it as me?

14   I say it, you nod your head and say, yeah, I agree with

15   that.   And we walk out of the room.   We're convinced we just agreed,

16   and the reality is we're like this (indicating).

17   And there's a cumulative set of a number of those over

18   the last number of years, the last several years in particular where in the

19   end, you know, people are excited about doing these projects.   I mean,

20   these are great, valuable, important projects that go to the basic

21   infrastructure of our industry, our assets and the ability to continue to

22   generate the important power we need and for this industry to be

23   successful and to do it together.

24   So, people get excited and there's a tendency to just

25   go.   And it isn't, you know, and it isn't until they realize somewhere

26   downstream that, oh, that touch point we thought we had at the

1   beginning, we didn't.

2   And I think -- I'm not sure if it was Darren or Bill, but one

3   of them pointed out when you find those conflicts at the back end,

4   they're a whole lot more disruptive, costly and distracting than they

5   were up front.

6   And what's been happening -- again, I'll go back to my

7   perspective more as the industry leader than the I&C guy trying to

8   implement one of these projects.   If I'm making a decision to do this, it's

9   an expensive project, it's a potentially disruptive project, but very

10   beneficial, you know.

11   When I see the collateral damage that a lot of these

12   projects occur, when I see that, you know, at the, you know, four-lap

13   race and on the third lap all of a sudden you have to add three more

14   laps and the cost goes up and the schedule goes out and the next thing

15   you know we're going back and forth to Rockville left and right, you

16   know, just, you know, I'm not getting, you know, as long as my guys can

17   keep buying stuff on eBay and Craigslist, I'm going to keep doing it.

18   And what I know is I know that we've just about

19   exhausted that.   And I know that, you know, my -- I apologize I got to

20   four, you know, personally speaking one of the things I worry about a lot

21   is the future of this industry is the people.   All right.   We need great,

22   young, strong, technical people coming into this industry.

23   You bring the young people into these plants and they

24   just look at you like what planet are you from?   All right.   You know, it

25   doesn't excite them and they don't even know how to work with the

26   stuff.   The number of people left who can even work with these

1   systems is going down.

2   And I think you put all these things together, you throw

3   them into one salad bowl, the kinds of thinkings or the kinds of attitudes

4   that result all in good conscience, all with good intentions, we've been

5   working in a way together where everybody is trying to do this and we're

6   stubbing our toe enough.

7   And the executives who are watching us see the blood

8   on the floor and they say, I want you to stop bleeding on the floor.   And

9   the best way to stop you from bleeding on the floor is to tell you to stop

10   running.

11   And we need to collectively demonstrate to those

12   decision-makers, all of us together, and I'm sure we can, that we can

13   jog around this room without stubbing our toe and bleeding on the floor,

14   and we can make these assets more valuable and improve safety and

15   improve reliability.   I'll stop.

16   CHAIRMAN BURNS: And sort of in that context, I'm

17   going to turn to Professor Scherlis and Mr. Cofer, you talk a bit in the

18   context of the airline industry and some of the transition there, but the

19   evidence chain, you talk about evidence chains.

20   I   mean,   one   of   the   difficulties   I   think   for   the

21   regulatory -- a regulatory framework, and it's whether it's us, pharma,

22   airlines, et cetera, is regulators to some extent are reactive.   They are

23   pro -- and they are proactive, but oftentimes reactive.

24   So, we're creating frameworks and certainties about a

25   certain -- in some aspects, but what I'm hearing is that you in terms of

26   the development and innovation that's going on and the rapidity with

1   which it occurs, there is somehow the balancing of understood criteria

2   and flexibility for innovation that is good.   The good type, if you will.

3   And I'm trying -- anything else you would like to add in

4   terms of how do you do -- how do you achieve that kind of balance?

5   How is it you are, in effect, allowed that innovation or in terms of doing

6   that kind of testing, that kind of evidence chain building, if you will.

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

8   DR. SCHERLIS: No, I think I understand your

9   question, and there is a kind of a dilemma.   On the one hand we want

10   to avoid framework of standards that is over-prescriptive with respect to

11   either the process that's followed or the structure of designs.   But on

12   the other hand, and, in fact, this goes back to Robert's remark, the

13   earlier we engage with certain issues, the better.

14   And there's data, for example, from NASA some years

15   ago with respect to software defects that shows that the difference -- if

16   you find the defect shortly after it is injected, all right, the difference

17   between that and finding the defect later in the life cycle is orders of

18   magnitude of cost.

19   And when we talk about commercial software, it goes

20   beyond that.   Because once it's deployed, the cost of update is very

21   high just to test.   More than 200.   And there's several studies that

22   were done that kind of reinforce those numbers.

23   So,   on   the   one   hand   we   want   to   avoid

24   over-prescription.   But on the other hand, we want to make sure that in

25   a development process the modeling and analysis and evaluation is

26   done as early as possible.

1   And so, one of the reasons why the idea of evidence is

2   appealing, is that we -- you could say it -- levy on the developer a

3   requirement to produce the evidence along with the artifacts that will

4   actually be executing in situ, but that evidence makes the evaluation job

5   straightforward.

6   So, in a sense, we say to the developer within a very

7   broad framework of criteria, here's a body of evidence and the

8   argumentation to support it.   And then you can come to an evaluation

9   judgment confidently and quickly.

10   And the advantage of that is as systems evolve, the

11   incremental cost to update the system, for example, for changing

12   infrastructure or changing functionality enhancement, whatever it is,

13   that cost goes down, but we still have to live with that dilemma of how

14   much prescription.

15   And I don't think that there's a necessary tradeoff.   I

16   think we can be creative about what's the nature of the framework.

17   This has been done, for example, with respect to security practices.

18   There's a security development life cycle developed by

19   two Microsoft people more than a decade ago.   It's called the SDL.

20   Very widely adopted and it's really a framework of what practices to

21   engage in at what stage of an engineering activity, but it's not

22   prescriptive with how we actually conduct the engineering activity or

23   how we design the systems that are being engineered.

24   DR. COFER: This tension that you mention between

25   innovation and regulation, it was very much in play when we were doing

26   our update to the DO-178 documents.   The previous version of that,

1 version B, was published in something like 1992.

2 So, I mean, between then and when we did the next

3 update starting in 2006, there's a lot of changes in the software industry

4 that had to be addressed.

5 And in that committee involving both industry and

6 regulators from Europe and the United States, FAA and EASA, the folks

7 that have to receive this evidence from applicants and industry are

8 asking how can I possibly review this material, because I haven't been

9 trained to do this.   How am I going to get my head around that?

10 So, one of our jobs in updating these guidance

11 documents was to try to reach a common language for all of the

12 different objectives that needed to be satisfied so that both the regulator

13 and the applicant could point to the same piece of paper and say, okay,

14 I understand that for this new technology, new-ish technology, this is

15 what the evidence in satisfying this objective might look like.

16 And so, again, not being prescriptive, but trying to say

17 this is -- this is what you should expect to see from an applicant if they

18 are using this kind of tool, this kind of technology to claim that they're

19 satisfying this objective.   So, that's one thing we've done.

20 Indeed I think there is going to have to be some

21 amount of education on the part of the regulators to come up to speed

22 on some of these new technologies.   And, again, these pilot studies,

23 case studies that I've mentioned are also helpful.

24 CHAIRMAN BURNS: Okay.   Thank you.   Thanks

25 very much.   I appreciate the indulgence of my colleagues.

26 Commissioner Svinicki.

1   COMMISSIONER SVINICKI: Thank you, Mr.

2   Chairman.   And thank you to all the witnesses for their presentations

3   today.   I find this conversation very valuable.

4   I think it's interesting to reflect on some of the history.

5   I joined this commission in a time in which it had been meeting as

6   frequently as every six months on this topic of digital instrumentation

7   and control.   And it's interesting to look at commission expectation, if

8   you will, and direction to the NRC staff from 2007.

9   This commission said the staff should proceed with the

10   timely implementation of NRC's digital instrumentation and control

11   project plan and the issuance of interim guidance recognizing that the

12   staff will continue to work with the stakeholders to refine the guidance,

13   to address the existing issues within each of the six working groups,

14   and to risk inform the regulatory framework for digital I&C.

15   I'm sure as they issued that direction they felt they had

16   it all tied up in ribbons and bows.   As we wind down to year 2015 and,

17   you know, get close to within 18 months of when -- the ten-year

18   anniversary of that direction to the NRC staff, it's interesting to go back

19   even further to a policy paper written to the Commission in the year

20   1993.

21   So, let's go back 22 years and the staff was talking

22   about an issue we just talked about today.   I'm sure it felt just as

23   contemporary.   Defense against common mode failures in digital I&C.

24   In 1993 the staff wrote recently, so you have to

25   remember again this was 22 years ago, increased attention has been

26   given to detailed assessments of the integrity of software applied to

1   safety-critical functions. These assessments have covered a broad

2   range of applications including computer-based medical treatment

3   facilities, computer-based fly-by-wire aircraft control systems and

4   nuclear power plant protection systems.

5   The staff found a consensus among computer science

6   and software engineering experts that such safety-critical applications

7   should be backed up by some system not based on software.

8   The experts base this opinion on the facts that the

9   quantitative estimate for the reliability of I&C systems based on

10   high-integrity software cannot yet easily be determined.

11   And Professor Scherlis is laughing at this, because it

12   seems in your field 22 years ago it's ancient history.

13   But, you know, as I sit here today and we have

14   representatives who have spoken to aviation, there's been mention of

15   pharma and pharmaceuticals and the medical community, I sit here as

16   a part of the nation's nuclear regulator saying, well, in '93 the staff

17   assessed that all these sectors were in the boat together.

18   It's my observation that these other sectors, medical

19   technology, we may not be in that profession, but we're pretty much all

20   patients. I'm looking at the age demographic in the room. We're all

21   patients now. So, I find -- I don't find a lot of analog anything in a

22   doctor's office or a hospital setting.   So, they passed us by.

23   And as one of millions of Americans who will next week

24   get on an airplane to spend holidays with family and friends and loved

25   ones, the quality of my colleagues' work at the FAA matters a whole lot

26   to me as I enter that small metal tube and get flung through the

1   atmosphere.

2   So, I'm assuming that the quality -- nuclear is special,

3   we say that around here a lot, but it isn't so special that it can just lay

4   itself aside from solving the problem of 1993's paragraph.

5   So, my one question to anyone, any soul brave enough

6   to answer this question is, you are the doctor and we are the nation's

7   nuclear safety and security regulator.   I bring you in.   Diagnose for me

8   why the others, you know, moved past this issue and we have not.

9   And then prescribe the cure for me on that.

10   And I know for those of you in nuclear business, this is

11   touchier for you to be honest about this one, but I'm wondering -- and

12   please opine whether is it fundamentally a mindset and a paradigm

13   shift?   Because I do agree and have had plain talk with the NRC staff

14   that if you view digital's introduction as introducing only vulnerability and

15   no benefit, your inclination as a safety regulator will be to write the most

16   prescriptive regulation.

17   And I would, you know, postulate to you that in the

18   paper that Commissioner Ostendorff and others have talked about on

19   IEEE 603-2009, the conditions in there represent the instinct of safety

20   professionals   to   say   I   prohibit   whole   sets   of   types   of   systems

21   architecture, I prohibit in its entirety two-way communications between

22   certain types of systems.

23   That is my inclination if all I care about is safety and not

24   generating megawatt hours or anything else.   So, but these other

25   groups conquered that instinct somehow.

26   These other regulators conquered it.   What did they

1   do?

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

3   why?

4   COMMISSIONER SVINICKI: Yes.

5   MR. COWARD: At NPR, about seven, you know, I

6   think most people know NPR was founded by the three chief guys

7   working with Rickover. So, we've always been primarily a nuclear

8   energy company. We remain a nuclear energy company. About 70

9   percent of our business is nuclear.

10   About 20 percent of our business is for the medical

11   device community, the medical -- doing medical product development.

12   Some other time I can tell you how we ended up there.

13   But as president of NPR, I have oversight of that as

14   well and I tend to go to some of their industry meetings and meet with

15   other executives. And I tell the story all the time about how if you look

16   at that industry, heavily regulated, heavy quality programs, they put

17   stuff in people, all right.

18   And you go to their meetings and all you feel in the

19   room is a spirit, you feel it, of the innovation, the moving forward

20   perspective. They have figured out within the context of a heavily

21   regulated industry with rigorous and onerous quality programs, they

22   have figured out together how to move forward.

23   We're doing at NPR right now, we are designing for a

24   customer an artificial pancreas. One of the first, all right. It's

25   software-controlled, all right.

26   There are times when it seems like the expectations

1   and the rigor and the requirements and the burden, it's more of a feel

2   than it is the paper, the feel for how to do some non-safety-related MSR

3   controls in a nuclear power plant -- I'm not putting down an MSR, but

4   the non-safety-related MSR controls in a nuclear power plant feel like

5   they carry a heavier burden than doing the software which is going to

6   control this artificial pancreas that if it goes bad for five minutes, it will

7   kill somebody.

8   And I think that my comment to your question is, and

9   it's a place where all of us can work together on the vendor side, the

10   licensee side, the regulator side, the opportunity we all have in front of

11   us is to revisit and work on our culture and to not let the pursuit of

12   perfection prevent us from making progress.

13   Because I personally believe we've wondered into a

14   place where the pursuit of the perfect digital I&C platform and system in

15   a nuclear power plant has led us to leave the existing systems in the

16   plant and actually increase the risk right now.

17   I believe numerous -- I'm not saying unacceptable risk,

18   but I think the overall risk right now is actually higher than it would be if

19   we replaced the systems.

20   And I think we have to overcome together, the leaders

21   of the industry, that cultural barrier that says we have -- we're nuclear, it

22   has to be perfect.

23   And I'm not saying accept less than perfect, but what

24   I'm saying is we have to convince ourselves and those around us that it

25   is okay to move forward if it's going to make us better.

26   COMMISSIONER SVINICKI: Thank you.   Would

1   anyone else like to comment?   Particularly those of you from maybe

2   more outside the nuclear industry.

3   DR. SCHERLIS: So, let me try this.   And I think

4   Darren may have more authoritative comment on the first part of my

5   remark, which is maybe partnering with other safety-critical industries

6   would be helpful.   Aerospace embedded medical devices and NASA,

7   for example, which has similar issues more focused on reliability.

8   The practices that are emerging in those industries, the

9   kinds of models, the kinds of analyses, the technical means, the tooling,

10   all that's to advantage.   And as part of that, promote innovation.

11   That could mean partnering, for example, with some of

12   the NITRD agencies.   NITRD is the Networking and Information

13   Technology Research and Development Coordination Activity out of

14   the National Science and Technology Council, which involves about a

15   dozen agencies who are all involved in investing in technical innovation

16   related to IT and networking.

17   Partnering with them as a kind of a receptor of their

18   technologies to do pilot projects could be very helpful and at least

19   getting an understanding of what's possible and where things might go.

20   But on the other hand, I think it's important to kind of

21   stare down some of the existing industry norms in a COTS world, which

22   are really adverse.

23   If you look at a license for a typical COTS product, it

24   really has two provisions.   One is it does what it does, and it doesn't do

25   what it doesn't do.

26   COMMISSIONER SVINICKI: And it doesn't start on

1   fire like those hoverboards.

2   DR. SCHERLIS: Right. It's as is. It's as is. The

3   license actually has those two words in it, "as is." And the second is

4   don't look, which is to say you may not do penetration testing or any

5   kind of activity that may look like reverse engineering.

6   This is the norm for many licenses in the world of

7   COTS. And that's a challenge if we want to embed those things,

8   because then we have to make special relationships with those

9   vendors.

10   And so, we've become habituated in a sense to

11   accepting the presence of a large number of defects, but that's not a

12   universal fact. There are many systems where we really achieve an

13   extremely high level of quality and we're able to assess that pretty well.

14   And so, I think the idea on the one hand partnering,

15   and the other hand sort of actively engaging with the innovative

16   community as a client. People get excited by the applications and the

17   challenges and create a kind of innovation culture.

18   That doesn't mean that those innovations are going to

19   kind of transition right into the current set of systems, but at least we get

20   a sense of, okay, as we look towards the horizon, what's the right vector

21   for us to be on and how can an understanding of that vector and

22   participation in that process help guide rulemaking in a way that will

23   make more opportunities available to the industry so that the kinds of

24   things that are happening with medical devices that Robert just

25   described are possible for digital I&C.

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

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

2   interested.   Thank you.

3   CHAIRMAN BURNS: Thank you.   Commissioner

4   Ostendorff.

5   COMMISSIONER OSTENDORFF: Thank you,

6   Chairman.   Thank you all for your presentations.   They were very

7   enlightening and extremely helpful for us.

8   About a year and a half ago I went to visit a nuclear

9   power plant in Region II.   I'm not going to mention the plant, but

10   basically the chief nuclear officer for this fleet told me that because of

11   regulatory uncertainty he was directing his staff not to proceed to go

12   from analog to digital automatic voltage regulator for emergency diesel

13   generator.

14   A few months ago I was visiting a plant in Region I and

15   I was dismayed when the -- it's an operating plant and the plant

16   manager told me that, yes, I asked him to show me signs of where

17   you're upgrading your instrumentation.   And he said, well,

18   Commissioner, we're upgrading this.   I've directed my engineering

19   staff to go reverse engineer this existing analog component to build a

20   new analog component.   That was not an encouraging message.

21   Earlier this year in March 2015 during our annual

22   Regulatory Information Conference, I sat on the industry and staff

23   group along with John Thorp over there.   John was in there from NRR.

24   There was about 50 or 60 people in this room.   Steve

25   Arndt was in there from NRC staff and there was others I'm not able to

26   put my eyes on.   And our staff, I think, was pleading for industry to

1   submit some more pilots, examples, upgrade requests to the NRC to

2   give us some more run time to demonstrate success.

3   And it was not a warm and touchy-feely atmosphere on

4   that topic.   And a lot of hesitancy to do that because of prior

5   experiences.

6   And I appreciate, Robert, your comment that, you

7   know, you think some of the misinterpretation and some of the staff

8   versus industry assigning different meanings to the same phrase, et

9   cetera, not assigning blame to anybody, any organization, that's not

10   constructive.

11   I support your comment that, you know, I think I

12   support it where our staff has been.   Send us something to do.   Send

13   us something to look at here.

14   And John Lubinski there who we'll hear in the next

15   panel, is nodding his head.   But I worry that without a commitment to

16   some contextual example, you know, these kinds of components that

17   have some nuclear industry applicability that there's an interest and

18   incentive to move forward on that creates a lot of interest, I don't see us

19   getting any -- making much progress.   So, how can industry and/or

20   staff work together?

21   And I'll also note the -- you got a roadmap, NRC's got a

22   roadmap, they're not the same roadmap.   There needs to be some

23   convergence there to work towards some common outcomes that

24   industry and staff can agree to.   So, I'm going to stop there and let you

25   guys comment.

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

1   I think we have talked a couple times with your staff.   And I think even if

2   we don't end up with one roadmap, I think the vision is to end up with

3   collaborative roadmaps that will feed off of each other and work

4   together.

5   And I think the challenge to us, and this is the

6   challenge to the NEI working group, the challenge to your staff from the

7   chief nuclear officer meetings I've been in, I think there is a long list of

8   people eager to submit the second application.

9   COMMISSIONER OSTENDORFF: Okay.

10   MR.   COWARD: You   know,   they're   waiting   for

11   someone to pay to learn the lessons.   And what we have to figure out

12   together is how can we give someone the comfort that it's not going to

13   be as bad as he thinks and it's worth the investment and that everyone

14   will   be   responsive   together   and   get   it   through   in   a   way   that   it's

15   successful for that plant and the others that will fall in right behind it.

16   And that's part of the theme of our roadmap.

17   COMMISSIONER OSTENDORFF: Well, I sincerely

18   believe NRC staff wants to receive these applications.   I know they do.

19   And so, they're anxious and eager to work on it.   They seem to be

20   given an opportunity.

21   Did you want to say anything, John?

22   MR.   CONNELLY: I   did.   So,   we   have   had

23   discussions about the roadmaps, both the NEI roadmap and the NRC

24   roadmap, and they're not inconsistent with each other.   I mean, there

25   are large degrees of continuity between them and obviously we'll have

26   to -- there will have to do some adjustment or refinement there.

1   You kind of alluded to it earlier that -- I can give a

2   representative example.   So, when faced with -- in the Westinghouse

3   world, the pending obsolescence of solid state protection system circuit

4   cards, okay, there's kind of a fork in the road there.

5   We could go down the path of a full-blown digital

6   upgrade similar to what Oconee did, or we could go with fit, form and

7   function upgraded cards by the OEM.

8   They were -- the initial system or the original

9   construction system was highly reliable, has proven for decades its high

10 reliability, but the newer circuit cards were even better and addressed

11 obsolescence issues.

12   So, to my knowledge every licensee in the United

13 States elected the path of in-kind upgrades versus a large-scale

14 modernization project just because there is very -- it's a very low-risk

15 profile.

16   I think what you're alluding to is, you know, we'd like to

17 see more of Oconee-like projects.   But until we have some run time

18 with the processes and people can feel more comfortable about the risk

19 profile that attaches to that, it's not likely that licensees will be, you

20 know, that we will be submitting projects like that to the staff.   It's

21 just -- it's a -- we're a naturally risk-adverse industry and rightly so.

22   COMMISSIONER OSTENDORFF: Okay.   I'm just

23 going to make a comment with you, John.   Your Slide 2 that shows the

24 historical performance for digital feedwater turbine controls, that was

25 extremely helpful.

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

1   commissioners here in advance of this meeting and I don't think I've

2   ever seen that kind of an articulation of a safety benefit.   And I think it's

3   very helpful for us to be able to see, because it helps put it in the

4   broader context.

5   And I think Commissioner Svinicki hit this point earlier

6   about how do we look at the overall safety benefit, not just is this

7   independence attribute or this common cause failure attribute met in a

8   more compliance method, but what are the benefits of this.   And so,

9   thank you for bringing this to the table.

10   MR. CONNELLY: You're welcome.

11   COMMISSIONER OSTENDORFF: Daryl, I thank you

12   for you presenting dual-hatted Westinghouse and IEEE.   And I've got

13   about eight questions for you all.   I don't have time to deal with all of

14   these, but let me just ask you a couple of them.

15   MR. HARMON: Okay.

16   COMMISSIONER OSTENDORFF: When is the next

17   update due for IEEE 603?

18   MR. HARMON: I think the -- as I mentioned, the

19   working group currently has a PAR.   They started work on it this year.

20   The -- I think the expectation is that it could be issued in early -- or

21   sometime in 2018.   So, that would be the next issuing of the standard.

22   COMMISSIONER   OSTENDORFF: On   your

23   Westinghouse hat --

24   MR. HARMON: Okay.

25   COMMISSIONER OSTENDORFF: -- you obviously

26   do a lot of business overseas.

1   MR. HARMON: I do mostly overseas.

2   COMMISSIONER OSTENDORFF: Yeah.   So, how

3 would you characterize the high level of the different regulatory

4 requirements for digital I&C for existing nuclear power plants or new

5 plants between what you're seeing overseas and what the NRC is being

6 requiring?

7   MR. HARMON: The two -- the experience that I have

8 overseas is primarily in South Korea and now in the United Arab

9 Emirates.   Would say KINS in South Korea quite closely follows what

10 the NRC does, how they use IEEE standards.

11   South Korean regulations are also based on IEEE

12 standards and I would say they relatively closely follow what the NRC

13 does.

14   In the UAE it's a little unique because FANR is a new

15 regulatory organization.   My experience so far with them is that they

16 have regulators from many diverse backgrounds.   It's like the,

17 somewhat, the United Nations in FANR.

18   So, they have some different perspectives.   Some

19 certainly U.S.-based and it's still IEEE-based primarily, but there's other

20 perspectives that are brought to the table.   So, I would say they may be

21 a little more diverse in terms of their regulatory perspectives.

22   We're a little bit, you know, we're still early in the UAE

23 nuclear industry.   So, may be a little hard to tell.

24   COMMISSIONER OSTENDORFF: Okay.

25   MR. HARMON: Does that help?

26   COMMISSIONER OSTENDORFF: It does.   Thank

1 you. Last question for our two final witnesses here. The general

2 context, you know, from your experience in your respective

3 communities and I think really adds a lot of value for us to hear how

4 others look at these issues. So, thank you for doing that.

5   Testing and evidence, how should we as a regulatory

6 body use the existing digital instrumentation control experience, some

7 of which was highlighted on John's slide for feedwater and turbine

8 control, how should we use that as evidence to look at things such as

9 common cause failure or software failure modes?

10   Run time, you know, years of experience,

11 reliability-type studies.

12   DR. COFER: Yeah. So, this is -- it's somewhat of a

13 religious debate in how you assess the reliability of --

14   COMMISSIONER OSTENDORFF: That's why I

15 asked the question.

16   DR. COFER: -- software. And in terms of my

17 denomination in that particular argument, I don't believe in treating

18 software probabilistically, because it's not. It's pure design. It doesn't

19 behave probabilistically.

20   That doesn't mean to the -- it's affected by its

21 underlying hardware, its inputs which are probabilistic. And so, we

22 have -- we can -- if we can, you know, make that distinction between

23 software, which is pure design just analogous to a mechanical design,

24 and then the underlying physical process is that influence, then that

25 gives us a basis for having a proper science of reliability.

26   That being said, there's different approaches to how

1   you deal with software common cause failures.

2   In our industry, we have typically relied on diversity so

3   that it -- but it varies a lot depending on the regulatory organization,

4   even which FAA office is doing the certification, the OEM, the airframer,

5   the manufacturer of the equipment.   Everybody has different ways of

6   doing things to try to show that they're safe, but ultimately they have to

7   perform a safety analysis as you would in your industry to demonstrate

8   the required reliability.

9   But it is very common to if you have two cross-checking

10   channels, to require different microprocessors so that the executable

11   then is different and you have some assurance hopefully that will fail in

12   different ways.

13   That said, there are also studies that show that if you

14   build things from the same set of requirements, you can end up with the

15   same errors being programmed in.   So, it's not a magic silver bullet in

16   any sense.

17   And there's also others that have shown that you would

18   be better off focusing all your attention to develop one piece of

19   software, one common piece of software for redundant channels that

20   you put all of your effort in and you have the highest level of assurance

21   in rather than splitting that effort into multiple development efforts and

22   possibly having errors in those redundant channels.

23   I don't think there is a conclusive answer to that yet.

24   Personally I think because of the tools and methods that we have

25   available to us now, I would lean towards trying to make sure that the

26   software is -- you focus all your attention on the one software, getting

1   the software right and then probably having some degree of

2   architectural dissimilarity where you might have a separate sensor, a

3   separate backup to try to cross-check it.

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

5   COMMISSIONER OSTENDORFF: I appreciate that.

6   Dr. Scherlis, do you want to add anything there?

7   DR. SCHERLIS: I agree with what Darren has said.

8   There's a danger in applying probabilistic models and doing Bayesian

9   arithmetic on software components, but the environment in which the

10   software operates does have physical characteristics.

11   And so, the software is responding to the models -- the

12   software has got to be designed, rather, to respond to the way we

13   understand the models, the environment and, in fact, software is

14   discontinuous.

15   There's a famous old story, an old, old NASA story in a

16   Fortran program, a period which was supposed to be a comma.   And

17   on those old line printer outputs, it's kind of hard to tell the difference

18   and that fundamentally changed everything about how that code

19   operated.

20   So, recognizing that and building the models and then

21   building the software to respond to those models, that's Point 1.

22   Second is with respect to diversity it is a hard problem.

23   I agree with what Darren said.   You can look at lots of different

24   dimensions of diversity, the algorithms, the choice of language, the

25   choice of infrastructure and tooling, the hardware, the people who do

26   the development.

1   But if they're building to the same spec, and this is an

2   old result, then we don't get as much variance as we're looking for.

3   And so, really play to both sides of the risk product, really work hard to

4   get the instance correct.

5   And that may mean pushing simplicity into the design

6   in order to get that and getting enough evidence and doing the

7   mathematical reasoning.   That's kind of where we are, as I understand,

8   with flight controls to a great extent.   But if we do go diverse, let's do

9   that kind of multi-factorial analysis of all the dimensions.   Make sure

10   we understand how to get as much dimensionality as we can and then

11   try to define measures within those dimensions.

12   There's no -- I don' think there's a simple answer to this

13   question of CCF, but I -- it's not an impossible problem either.

14   COMMISSIONER   OSTENDORFF: Thank   you.

15   Thank you all.

16   CHAIRMAN   BURNS: Thank   you,   Commissioner.

17   Commissioner Baran.

18   COMMISSIONER BARAN: Thanks.   I want to start

19   off by thanking Dr. Cofer and Dr. Scherlis for being here.   It's really

20   helpful to get a broader perspective.

21   You know, there are some issues we have here that

22   are   really   truly   exclusive   to   the   nuclear   sector,   but   digital

23   instrumentation control really isn't one of those issues.   And it's

24   something that other industries where safety is critical have grappled

25   with.   So, it's very helpful to get that perspective.

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

1   and ask -- I want to focus a little bit on IEEE 603, the standard and the

2   conditions that the staff has added to the original standard and get a

3   better understanding of the views and concerns about those.

4   So, as Mr. Harmon pointed out, this was an industry

5   consensus standard, the core standard was.   I want to just make sure

6   we're all kind of on the same page in terms of understanding how much

7   of the concern you all have expressed about where that proposal is now

8   is related to the conditions.

9   I guess another way of putting that is does everyone --

10   does NEI, does Exelon, does Westinghouse, would you all support

11   incorporating by reference the standard if their conditions weren't fair?

12   MR. COWARD: I believe the answer is yes.

13   COMMISSIONER BARAN: You   would   support

14   incorporating it without the conditions.

15   MR. HARMON: I would agree with that, too.   What's

16   been expressed to me is most of the concern is with the conditions and

17   going beyond what the standard imposes or has for criteria.

18   MR. CONNELLY: As would we.   The only concern

19   that I would express is that, you know, because there is this large sea of

20   standards, that introducing yet another change into that environment

21   may ultimately be counterproductive, you know.

22   We're probably better served to iron out these major

23   issues, you know, the application of 50.59 dealing with common cause

24   failure and so forth, get those issues ironed out before we introduce yet

25   another variable into it.

26   COMMISSIONER BARAN: Well, let me follow up on

1   that aspect of it, because I was interested in that point when you made it

2   originally in terms of, you know, trying to get our arms around a lot of

3   issues here.   Can't we just hold this constant while we work on these

4   other things?

5   And I'd like to get your thoughts on this, which is, you

6   know, we've talked a lot about innovation, how much things have

7   changed, and those standards are from 1991.   The standard is 25

8   years old.

9   Isn't it outdated?   Don't we need to update the

10   standard?   Can we really -- can we really afford to hold this variable

11   constant and have it use a standard that's 25 years old?

12   MR. HARMON: Well, from the IEEE's perspective,

13   we did approve a standard back in 2009.   And again we're working on

14   it now.   Certainly a 25-year-old standard with the way technology has

15   improved could have some question.

16   Although it is a fairly high-level standard in terms of

17   safety system criteria, it would seem the 2009 standard may be better

18   suited and there's still improvements.

19   Some of the things we've learned from the rulemaking

20   activity that are now being factored back into IEEE 603 that will be the

21   next standard, but it would seem that one might want to move forward.

22   I'm not as familiar with the 50.59 aspects and other

23   possible influences or things that will happen to the overall regulation

24   that --

25   COMMISSIONER BARAN: Well, let me ask about

26   this: In terms of the conditions that the staff have added to this and are

1   proposing, proposing to propose, my understanding is that several of

2   those conditions are currently in existing guidance that we have.

3   So, these aren't, for the most part, new expectations.

4   Some of this is moving things from current regulatory guidance into

5   regulation.

6   First of all, do you think that's an accurate

7   characterization?   And if so, what's the concern about, you know, kind

8   of the same expectations being shifted from guidance to the regulation?

9   MR. COWARD: Let me start and then you please fix

10   me.   I think the spirit of your comment or question is on track.   I think

11   part of it is what is the right place for the existing guidance to land and

12   what is the right forum to put it in, what is the right kind of document,

13   what is the right use?

14   And the potential to set what a number of people in the

15   industry think would be sort of some bad precedent, that they just don'

16   think it belongs where they're trying to put it, you know, that's a big part

17   of it.

18   And I think the other big part of it is the, you know, all of

19   us in nuclear tend to be fairly clear, logical thinkers with a heavy

20   technical bend.   And the idea of ending up with what are essentially

21   different criteria for Byron or the plant that might get built at Turkey

22   Point, just doesn't seem to make sense to us.

23   COMMISSIONER BARAN: Well, let me follow up on

24   that just for a second, because this is one of the points that was made,

25   which is there's a concern about having a different set of requirements

26   for existing plants and new plants.

1   But in our regulatory framework we have several areas

2   where there are requirements that differ for new versus existing plants,

3   probabilistic risk assessment, severe accidents, management

4   guidelines and other things where it's not the same.

5   Are they really similarly situated in this case?   Is there

6   really a problem with having different requirements for existing plants

7   and new plants that you factor in kind of the ability, and maybe this is an

8   oversimplification of, you know, designing around some of these

9   problems for a new plant.

10   MR. COWARD: And I think that our perspective

11   would be along the lines of we agree there's numerous areas where

12   you're going to have different requirements and different processes.

13   This isn't one of them.

14   COMMISSIONER BARAN: Okay.

15   MR. COWARD: This is sort of core, underlying, basic

16   design philosophy that we would expect to be the same everywhere.

17   COMMISSIONER BARAN: Going back to kind of the

18   conditions and whether it's more appropriate to have some of these

19   concepts in regulation, some of the concepts in regulatory guidance, I

20   get the sense, and we'll have a staff on the next panel, we can explore

21   this, that part of this is a disagreement about, well, how do you have

22   greater clarity in the requirements and greater regulatory certainty.

23   And you read the staff paper and their view is, well, you

24   wanted greater clarity.   Here it is.   We're putting conditions in the

25   regulation.   What can be clearer than that?

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

1   level of detail in the regulations isn't -- doesn't result in regulatory

2   stability or certainty.   It's something that would be an obstacle to

3   improving the -- improving the licensing for digital upgrades.

4   Can you talk a little bit about that?   Why is there this

5   disconnect about the level of specificity that should be in the regulation

6   versus in the guidance?   And why is additional specificity in the

7   regulation?

8   If it's performance-based at least, why is that an

9   obstacle to progress in this area?   That's a lot all in one question, but,

10   you know, it's kind of a general theme, I think, here.

11   MR. HARMON: I think one of the things that at least

12   we see is that the Code of Federal Regulations is typically technology

13   neutral.   It doesn't specify implementations.

14   Some of the conditions I think such as hard wiring

15   certain signals, the one-way communication as opposed to defining

16   criteria for data communications and when you could have bidirectional

17   communications as previously specified, I think those are the things

18   that kind of react to and believe that those may limit us and make it

19   more difficult to implement some of the solutions we're trying to

20   implement.

21   COMMISSIONER BARAN: So, from your point of

22   view, and we'll get the staff's view on this, too, some of these conditions

23   aren't really performance-based, they are prescriptive from your point of

24   view and it's going to limit particular technologies.

25   MR. HARMON: Yes.

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

1   This is helpful.   I've gained a better sense of the views and the

2   concerns about this and it's good for kind of starting discussion with the

3   staff on the next panel.   Thanks so much.   Appreciate it.

4   CHAIRMAN   BURNS: Okay.   Thank   you,

5   Commissioner.   I want to thank again the panel for their presentations

6   this afternoon.   It's been very rich discussion.   And with that, we're

7   going to take a break.

8   Let's reconvene at five to 3:00 and we'll hear from the

9   staff panel at that time.   Thank you.

10   (Whereupon, the above-entitled matter went off the

11   record at 2:48 p.m. and resumed at 2:57 p.m.)

12   CHAIRMAN BURNS: We'll come back to order.

13   I would ask folks in the audience, I feel like I'm at the

14   theater, but to silence your cell phones and electronic devices,

15   particularly appropriate since we're talking about digital things today.

16   But, I've heard a couple of them, ring-a-ding-dings today, so if you

17   would do that, I would appreciate it.

18   We'll proceed with the second half of the meeting, the

19   presentation of the staff who will provide background on NRC Digital

20   Instrumentation and Control Activities including recent lessons learned

21   and we'll discuss the proposed rule that's in front of the Commission

22   and incorporate by reference the IEEE 603-2009 Standard and other

23   issues that may be relevant to this topic.

24   So, I'll call on the Executive Director for Operations, Vic

25   McCree to begin.

26   MR.   MCCREE: Good afternoon, Mr. Chairman,

1   Commissioners.

2   We're here this afternoon to discuss our efforts to

3   continue to improve the licensing of digital instrumentation and control

4   systems for commercial nuclear power plants in the United States.

5   We'll discuss the proposed rule currently before the

6   Commission to incorporate by reference the IEEE Standard the

7   603-2009 into the NRC's regulations.

8   We'll also provide the Commission with a summary of

9   other key activities that we are pursuing.

10   The NRC is a learning organization and we're focusing

11   on addressing emergent challenges in the area of instrumentation and

12   control technology.

13   We're committed to ensuring safety while achieving a

14   stable, consistent and predictable regulatory framework consistent with

15   our principles of good regulation for use of digital instrumentation and

16   control systems.

17   With me at the table today are John Lubinski, Acting

18   Deputy Office Director for Engineering, Office of Nuclear Reactor

19   Regulation, to his right, Richard Stattel, Senior Electrical Engineer also

20   from NRR, to our left, John Tappert, the Director of the Division of

21   Engineering, Office of New Reactors and Deanna Zhang, Senior

22   Electronics Engineer, also from the Office of New Reactors.

23   Next slide, please?

24   I'd like to note that our presentation today has a deeper

25   level of detail than our normal presentation at Commission meetings,

26   but it's in an attempt to be responsive to the questions that I know that

1   you're interested in hearing us respond to.

2   We will begin our presentation with a short discussion

3   of the unique issues associated with Digital I&C and a brief history of

4   recent efforts.

5   We'll also discuss lessons learned from other

6   industries from licensing experience in the United States and regulators

7   from other countries.

8   We'll discuss the efforts of the NRC Digital

9   Instrumentation and Control Steering Committee and the industry's

10   Digital Instrumentation and Control Working Group that developed

11   interim guidance for the implementation of digital systems in the late

12   2000s.

13   We'll also discuss our continuing efforts to use the

14   interim guidance to improve the licensing of digital systems.

15   We will then discuss in some detail the proposed

16   rulemaking that's currently before the Commission.

17   And, we will conclude our presentation with a

18   discussion of other key efforts that we're engaged in to continue to

19   improve to improve the licensing of digital system.

20   Digital technology provides significant advantage over

21   earlier analog or relay-based systems as mentioned during the industry

22   panel.

23   However, with these advantages have come new

24   challenges. We recognize that added functional capability of these

25   systems as well as new design development and testing methods have

26   outpaced our regulatory guidance.

1   The use of IEEE 603-2009 is just one aspect of

2   addressing the potential challenges with digital instrumentation and

3   control systems.   We recommended in our SECY 15-0106

4   Commission approval to publish for comment a proposed rule that

5   incorporates the standard.

6   We're also developing an action plan to support the

7   continued improvements and plan to work with key external

8   stakeholders on these activities.

9   The priorities in the action plan include improving the

10   licensing processes based on lessons learned from past and current

11   reviews and working with industry to address concerns with licensee

12   implementation of plant digital modifications using the 10 CFR 50.59

13   process.

14   The significant challenged addressed in the action plan

15   is the use of identical software across redundant safety channels that

16   could potentially defeat this redundancy and lead to common cause

17   failure.

18   As Commissioner Svinicki noted earlier in a 1993 Staff

19   Requirements Memo, the NRC position on software common cause

20   failure was established and it is today still the Agency's policy in this

21   challenging area.

22   However, we do believe it prudent to take a fresh look

23   at the NRC position on needed diversity to address the potential for

24   common cause failure.   And, we plan to coordinate our efforts in this

25   area with our external stakeholders.

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

1   experience with digital system review and efforts to improve the

2   regulatory process.

3   John?

4   MR. TAPPERT: Thank you, Dick.

5   Next slide, please?

6   To begin with, digital technology is unique from analog

7   technology.   Specifically, digital systems involve the execution of

8   application software and instruction are logic to perform system

9   functions.

10   The flexibility of digital technology offers many benefits

11   to address some of the reliability and maintenance issues with analog

12   technology.

13   Although digital technology offers benefits, the unique

14   hazards associated with the use of digital technology should be

15   considered.

16   Examples of such hazards include difficulty in

17   achieving deterministic behavior, inability to fully test the system,

18   difficulty in achieving communications and dependence and potential

19   for latent errors in software that could result in software common cause

20   failures.

21   To utilize this technology, the applicant must

22   demonstrate that these systems will operate reliably to ensure the

23   safety of the plant under normal and accident conditions.

24   This includes ensuring that systems provide a

25   sufficient level of diversity and defense-in-depth, commensurate with

26   the potential consequences of failure.

1   Next slide, please?

2   Digital systems were initially deployed in the nuclear

3   industry in the 1980s.   In response to our early experience, in the late

4   1990s, we issued licensing guidance documents and staff review

5   guidance covering some of the unique aspects of digital system

6   development processes including software development and

7   consideration of diversity and defense-in-depth.

8   Though this new guidance provided additional

9   clarification of our expectations for licensees to adhere to our rigorous

10   digital development process, the industry sought a more predictable

11   and effective regulatory approach.

12   We have looked towards other industries for lessons

13   learned from their experiences with implementation of digital

14   technologies, for example, the military and commercial aviation and the

15   process industries.

16   And, we've evaluated that experience to provide

17   additional insights to our guidance.

18   Next slide, please?

19   In 2007, at the industry's request for additional

20   clarification, the NRC formed the Digital I&C Steering Committee.   And

21   during the 2007 to 2011 time frame, the NRC with participation from

22   stakeholders developed seven Interim Staff Guidance documents, or

23   ISGs, for the evaluation of proposed Digital I&C systems.

24   We intend to incorporate the content of the ISGs into

25   the NRC Standard Review plan during the next update.

26   We used some of the interim guidance in our

1   evaluation of the Oconee reactor protection system upgrade and for a

2   number of Design Certification Application reviews such as the AP1000

3   and US APWR.

4   Based on lessons learned and the Oconee project, we

5   issued ISG 6 regarding the licensing process and used this updated

6   guidance in the performance of the Diablo Canyon process protection

7   system digital upgrade review.

8   Next slide, please?

9   It is likely that more digital safety system upgrades will

10   be needed in the coming years to address operational and

11   obsolescence issues.

12   We have identified that NRC policies and processes

13   can be improved to decrease uncertainty and the cost of licensing

14   digital technologies.

15   In order to improve the Digital I&C licensing process,

16   we are working on the lessons learned from the Diablo Canyon ISG 6

17   pilot review.

18   Some concepts within ISG 6 that have worked well

19   include pre-application meanings, early submittal of certain design

20   documents to support acceptance reviews and guidance on

21   documentation submittal.

22   One concept that has been less successful is the use

23   of a graded or tiered approach to determine the level of NRC review

24   needed.   Since this concept is based solely on the pre-approval status

25   of the I&C platform.

26   We believe additional system aspects should be

1   considered for this determination including scope and type of

2   modification being performed.

3   And, currently, we are focusing on future process

4   improvements to enhance the current digital licensing processes as

5   described in ISG 6.

6   Next slide, please?

7   With regards to new reactors, the new reactors, the

8   new reactor I&C designs use highly integrated Digital I&C systems

9   which may include features such as control of safety-related equipment

10   for non-safety I&C system, bidirectional communication between safety

11   and non-safety systems and a high number of interdivisional data

12   communication links.

13   We have used the current Digital I&C Interim Staff

14   Guidance to review new reactor designs. In several instances, new

15   reactor applicants were challenged in providing sufficient design

16   information, analysis to support the safety demonstration for these

17   integrated systems.

18   In addition, the applicants did not initially provide

19   sufficient analysis to demonstrate that hazards associated with I&C

20   interactions with plant systems were fully analyzed.

21   Further, some designs differed significantly from

22   Interim Staff Guidance. And, as a result, these reviews continued

23   much longer and required significantly more resources than originally

24   planned.

25   To address these issues, some applicants were able to

26   successfully demonstrate safety by modifying the design and

1   addressing NRC requirements at a higher level of the I&C design such

2   as implementing physically limited one-way data communications.

3   And, this approach was found to greatly simplify the safety case.

4   Next slide, please?

5   The current NRC regulation, 10 CFR 50.55(a)

6   incorporates by reference IEEE Standard 603-1991. We believe it is

7   appropriate to update the regulation to incorporate the most recent

8   2009 version in order to capture criteria specific to address digital

9   technology.

10   We believe that this proposed rule will make Digital I&C

11   system licensing more efficient and effective.

12   We have also gained some additional lessons learned

13   from recent licensing experiences. For example, the industry

14   developed NEI 01-01, Guideline on Licensing Digital Upgrades, to

15   provide guidance for performing the 10 CFR 50.59 evaluation for digital

16   upgrades.

17   And the NRC endorsed NEI 01-01 through a regulatory

18   issued summary.

19   Based on recent experience, we have identified some

20   weaknesses and ambiguity in this guidance, particularly in the area of

21   addressing the potential of software common cause failures.

22   These weaknesses in the current guidance have

23   contributed to several licensees improperly performing 50.59 analyses.

24   In addition, the diversity and defense-in-depth criteria

25   provided in the Staff Requirements Memorandum to SECY 93-087

26   need to be reevaluated to determine whether it should be updated to

1   reflect advances in digital technology.

2   We have also sought to stay abreast of Digital I&C

3   developments in the United States and the international nuclear

4   industry as well as other industries where digital technology is used in

5   safety applications.   And, this has included our work with the

6   multinational design evaluation program and various research efforts.

7   An example of this is the documentation of technical

8   approaches used in other industries to determine what is the

9   appropriate level of diversity needed to mitigate software common

10   cause failure.

11   And,   this   assessment   can   be   found   in

12   NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant

13   Instrumentation and Control Systems.

14   And, we will discuss the topic of software common

15   cause failure in more detail later in the presentation.

16   And now, Rich will now provide a discussion of the

17   proposed IEEE 603-2009 rulemaking.

18   Thank you.

19   Next slide, please?

20   MR. STATTEL: Thank you, John.

21   The Standard IEEE 603 is titled Standard Criteria for

22   Safety Systems in Nuclear Power Generating Stations.

23   It's a performance-based standard for the design and

24   development of safety-related instrument and control systems.

25   It is intended to be a technology neutral and its criteria

26   are used by the NRC to determine regulatory conformance for all I&C

1   safety systems.   This standard is incorporated by reference into NRC's

2   regulation 10 CFR 50.55(a).

3   When performing I&C safety evaluations, we use IEEE

4   603 as the principle regulatory basis document.   The criteria of this

5   standard are considered as required means of meeting the general

6   design criteria associated with I&C systems.

7   The 1991 version of IEEE 603 includes a safety system

8   criteria for several topical areas.

9   Next slide, please?

10   An NRC working group was formed to evaluate and

11   compare the new version, 2009 version of the standard with the 1991

12   and 1998 versions of that standard.

13   This slide summarizes the changes that the working

14   group identified.   The new standard addresses potential safety issues

15   that might arise from incorporating advanced technologies and safety

16   systems.

17   It provides added guidance to address electromagnetic

18   compatibility issues.   It adds new criteria to address the potential for

19   common cause failures.   It adds clarification for the requirements for

20   equipment not credited to perform safety functions, but connected to

21   safety systems.   And, it adds a specific requirement for electrical

22   isolation and digital communication independence between safety and

23   non-safety systems.

24   Additionally,   the   standard   contained   updates   to

25   references and eliminates references that were no longer in effect.

26   Next slide?

1   The backfit analysis performed determined that the

2   application of the standard was not mandatory for current license

3   holders.   Instead, new criteria as proposed will be applied to new

4   applications and selectively to license amendments.

5   The previous date base applicability criteria were left in

6   place to maintain existing design basis for those currently licensed

7   plants.

8   A new set of criteria was included in the proposed rule

9   to define applicability for the new standard.

10   The conditions for determination of applicability are

11   functionality, technology, independent strategy and diversity strategy.

12   The proposed rule includes guidance for determining

13   the applicability and tables which provide examples of different types of

14   I&C design changes, some of which would require compliance with the

15   new proposed criteria and some others that would not.

16   Next, I'll discuss each of the conditions for the use of

17   IEEE 603 being proposed.   Many of these conditions have been a part

18   of our regulatory guidance for some time, as was mentioned earlier.

19   We felt that it would be beneficial to provide more

20   specific regulatory basis for those requirements to ensure these

21   important aspects would be addressed.

22   We expect applicants to provide documentation to

23   demonstrate compliance with these conditions when performing Digital

24   I&C system upgrades.

25   The standard already contains clauses to address

26   integrity and independence.   But, the interpretation of these clauses

1   has not always been consistent between the applicants and the NRC

2   staff.

3   The added conditions in the proposed rule are

4   intended to reduce regulatory uncertainty that concerns applicants by

5   elaborating these criteria.

6   Next slide?

7   The first condition I'll discuss regards system integrity.

8   This new clause would require, in order to assure the integrity and

9   reliable operation of safety systems, safety functions shall be designed

10   to operate in a predictable and repeatable manner.

11   The existing integrity criteria in the standard refers to

12   IEEE 7432 which I would characterize that as a companion standard to

13   IEEE 603. But, that standard is not incorporated so it doesn't really

14   have the weight of regulation.

15   We felt that the additional regulatory basis would

16   ensure conformance with those criteria.

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

18   here.

19   Okay, predictable and repeatable operation of the

20   system requires that the results of translating input signals to output

21   signals are determined through known relationships among controlled

22   system states and required responses to those states.

23   It also requires that a given set of input signal produces

24   the same output signals for the full range of applicable conditions to

25   defined in the design basis.

26   All signal processing between sensor, data input and

1   safety control device actuation must be accomplished in a manner that

2   is neither redundant, portions of the safety system, nor other external

3   inputs can affect the system's ability to perform its safety functions.

4   Next slide?

5   In the next set of slides, I'll be discussing a proposed

6   criteria for maintaining communication independence.

7   The figure shown here shows a reactor protection

8   system architecture.   It illustrates three different types of

9   communication interfaces which can exist in these designs.

10   When I refer to communications between safety

11   divisions, I'm referring to the interfaces shown here in the blue and red

12   lines which connect different components of a safety-related system to

13   support safety functions.

14   This includes interfaces between divisional safety

15   processors shown as the blue horizontal lines as well as the red line

16   interfaces to the coincidence voting processors.

17   When I refer to communications between safety

18   systems and non-safety-related systems, I'm referring to the interfaces

19   shown here in the green lines which connect safety system

20   components with external non-safety-related systems such as plant

21   computer systems or maintenance work stations.

22   Next slide, please?

23   So, for independence, this condition adds several new

24   requirements to the existing independence criteria of IEEE 603.

25   Protection systems and safety systems must

26   implement provisions for protection against identified hazards.

1   Next slide?

2   Subparagraph A of the independence clause would

3   clarify that signal processing portions of the safety system shall provide

4   the capability to ensure that degradation or failures of signals

5   exchanged among redundant safety divisions or between safety

6   systems and other systems do not propagate in a manner which results

7   in impairment of the safety functions.

8   For example, safety function processors should not

9   directly exchange information with other processors outside of the

10 division.

11   Separate communication processes, instead, should

12 be used to ensure the data is received, formatted correctly and is

13 properly addressed to the intended destination.

14   Subparagraph B would clarify that safety systems shall

15 be designed with provisions for detecting and mitigating the effects of

16 signal faults or failures received from outside the safety division.

17   Redundant divisions of safety systems should have the

18 capability of tolerating such faults or failures originating from outside

19 that division in a manner that, again, does not degrade the ability of the

20 system to perform safety functions.

21   Next slide?

22   Subparagraph C would clarify the requirements for

23 communications in currently operating nuclear power plant designs.

24   Specifically, it would clarify that communications or

25 signals received by a safety system from outside the division or system

26 should be limited to those that support the accomplishment of a safety

1   function or otherwise benefit safety.

2   In the proposed rule, safety benefit is defined as

3   justification for adding safety system functionality that is not necessarily

4   required for accomplishment of the safety function, but that contributes

5   to safety.

6   Examples would include increasing safe system

7   availability or increasing the safety of a mechanical, nuclear or electrical

8   system design.

9   Next slide?

10   Subparagraph D contains new independence criteria

11   being proposed for new reactors.   This clause would clarify

12   requirements for communication in new reactor designs.

13   The first part of this ensures that data communication

14   from safety systems to non-safety systems is in one direction while the

15   system is in operation and is accomplished through hardware means.

16   The second provision ensures that transfer of signals

17   between redundant portions of safety systems is only permitted when

18   signals transferred is required for the performance of safety-related

19   functions.

20   Next slide?

21   The third criteria ensures that for functions that require

22   safety systems to receive signals from non-safety systems to ensure

23   diversity and defense-in-depth were support automatic anticipatory

24   reactor trip functions.

25   The signal transfer method is restricted to means that

26   do not use data communications.

1   And, finally, the fourth criteria requires that new reactor

2   applicants who propose alternatives to these previous conditions would

3   identify direct and indirect pathways to safety systems from other

4   systems.

5   This additional requirement facilitates the identification

6   of interdependencies and failure modes in alternative designs.

7   These proposed independence criteria would improve

8   evaluation processes for new reactor I&C designs by allowing new

9   reactor applicants to demonstrate communications independence at

10   hardware architectural design level.

11   Establishing communication at the hardware

12   architectural level would also minimize the potential for propagation of

13   design errors.

14   We recognize that there are certain cases where a

15   safety division would need to receive signals from outside the division.

16   For example, voter processors need signals from other

17   systems in order to accomplish the coincidence voting functions.

18   A safety system may also need signals from the

19   non-safety to support diversity functions.

20   Next slide?

21   We believe the proposed rule will have a positive -- the

22   positive impacts on operating plants performing digital safety system

23   upgrades that are shown here on this slide.

24   Applicants will be able to design their digital safety

25   systems to the new improved standard without having to rely on

26   alternatives clause for approval.

1   It's more efficient to perform our evaluations without

2   having to evoke alternative standards clause. This supports a more

3   consistent evaluation with the greater degree of predictability.

4   The NRC already evaluates hazards associated with

5   digital systems per our existing regulatory guidance. And IEEE 603

6   includes a clause which addresses the need for hazard analysis.

7   We believe that adding this as a regulatory

8   requirement would reinforce the importance of this activity.

9   Go to the next slide, please.

10   The benefits of the rule on operating reactors will also

11   apply for new reactors. In addition, for new reactors, we believe the

12   licensing process will be more effective because the proposed

13   independence criteria would allow new reactors to demonstrate

14   communication independence with a higher level of design information

15   at the architectural level.

16   As such, applicants would not need to provide detailed

17   design implementation information.

18   The proposed independence condition incorporate

19   lessons learned from new reactor licensing reviews. These criteria

20   restrict the implementation of communications for safety systems to

21   limit failure modes and unexpected behaviors associated with

22   communications while preserving some of the benefits of digital

23   technology and allowing functionality that improves reliability and

24   availability.

25   Next slide?

26   In reviewing IEEE 603-2009 Standard and developing

1   the proposed rule, we engaged with the industry stakeholders in

2   various forms.   Some of the key interactions are listed on this slide.

3   First, we were actively involved with the NPEC working

4   group throughout the development of IEEE 603.   The NPEC working

5   group, as mentioned before, consists of members from the industry as

6   well as NRC staff with all having expertise in the I&C development area.

7   NRC working group members have discussed and

8   presented plans for incorporating the 2009 rule into our requirements

9   including the additional conditions.

10   In 2014, we gave two presentations to the ACRS on

11   the draft proposed rule language as it existed at that time.   The draft

12   rule was made publically available to support these meetings and

13   highlighted NRC's plans to provide these additional conditions.

14   As documented in letters to the staff, the ACRS has

15   generally agreed with the proposed rule and has provided several

16   recommendations to add conditions to clarify the use of the standard.

17   We accepted some but not all of these conditions in our

18   response to the ACRS.

19   More recently, we conducted a public meeting webinar

20   in August of this year to solicit feedback on the draft rule language.

21   We described our intent to provide the proposed rule to the

22   Commission with recommendation to publish it for stakeholder

23   comment, including specific questions on the key issues in the

24   proposed rulemaking.

25   As noted in the meeting summary, we received a

26   diversity of comments such as the suggestion to include a provision

1   which would allow new reactor applicants to provide a greater level of

2   design detail without having to invoke the alternatives clause.

3   The industry also expressed interest in having an

4   opportunity to participate in workshops.

5   This concludes my discussion of the proposed rule.

6   I'm now going to turn over the presentation to John Lubinski who will

7   discuss key initiatives related to instrumentation and control.

8   MR. LUBINSKI: Thank you, Rich.

9   Rich discussed our evaluation of IEEE 603-2009, the

10   proposed rule and our external stakeholder interactions thus far.   I'd

11   like to highlight a few of the benefits of the proposed rule first.

12   We believe it is appropriate to update the regulations to

13   incorporate the most recent version of IEEE 603 in order to capture

14   criteria specific to digital technology.

15   We believe the 2009 version provides a safety

16   improvement over the '91 version of the standard.   This includes

17   addressing potential safety issues that might arise from incorporating

18   components that use advanced technologies and safety systems,

19   additional guidance to address electromagnetic capability compatibility

20   issues and better classification for equipment not credited to perform a

21   safety function but is connected to safety-related equipment.

22   In most cases, the conditions included in the proposed

23   rule and the regulatory guidance that we have used for some time into

24   the rule.

25   We believe it would be beneficial to provide more

26   specific regulatory basis for those requirements in order to ensure

1   these important aspects would be addressed during licensing.

2   Specifically, the added condition on applicability will

3   provide more specific criteria on what plant modifications will require

4   updating of the licensing basis.

5   Additionally, the added condition on system integrity

6   will ensure better consistency and demonstration of this property for

7   digital system and improve regulatory predictability.

8   We also believe that there will be added regulatory

9   certainty provided by the proposed restriction associated with data

10 communication in the independent section of the rule.

11 We recommend the Commission approve publication

12 of the proposed rule to incorporate by reference the 2009 version for

13 public comment. We believe it is important to obtain formal external

14 stakeholder feedback on the use and incorporation of the standard.

15 Next slide, please?

16 We believe the use of the IEEE standard is only one of

17 the actions needed to address Digital I&C upgrades. We are

18 developing a Digital I&C action plan to review all aspects of our current

19 licensing processes.

20 The plan's objective is to identity where improvements

21 can be made and the effectiveness and efficiency of our regulatory

22 processes for Digital I&C licensing and upgrades.

23 To make most effective use of our resources as well as

24 the industry's resources, the issues will be prioritized based on our

25 belief as to which topics, if resolved quickly, could realize the greatest

26 impact.

1   Where appropriate, the plan identifies specific links to

2   research activities that need to be addressed to support improved

3   technical and regulatory basis for policy or process improvements.

4   We plan to work with external stakeholders to integrate

5   our Digital I&C action plan with the NEI roadmap.   And, we currently

6   have a public meeting planned in January to discuss both our action

7   plan as well as the roadmap.

8   In addition, as we develop our roadmap, we will

9   continue to revise it periodically based on lessons learned as we

10   implement the actions.

11   Next slide, please?

12   The current draft of the Digital I&C action plan includes

13   ten activities related to Digital I&C.   One we've already discussed was

14   the use of the IEEE Standard 603.

15   Next, the Deanna Zhang and I will discuss in more

16   detail four activities which are listed on this slide.

17   These activities have near term milestones or may

18   require Commission engagement which is why we're discussing them

19   in more detail today.

20   The first is revising guidance for 50.59 evaluations for

21   Digital I&C modifications.

22   The second is reevaluating the current process for

23   addressing potential for software common cause failure of digital

24   systems.   It is likely we will engage the Commission regarding this

25   activity.

26   And, the third is identifying the most effective process

1   for staff to perform its evaluation of proposed license amendments and

2   new applications related to Digital I&C.

3   And the fourth is evaluating the process and timing for

4   evaluating applicants compliance with cybersecurity requirements.

5   We plan to provide a vote paper to the Commission on this topic.

6   I will note that while we have not seen the roadmap that

7   NEI has developed nor have they seen our complete Digital I&C action

8   plan, we have coordinated on the major topics and would note that the

9   first two topics, 50.59 evaluations as well as common cause failure are

10   top priorities in both plans and we think that the plans will align on our

11   prioritizations.

12   Next slide, please?

13   During component design basis inspections, NRC

14   inspectors have identified noncompliances with 50.59 reviews

15   performed by licensees for digital systems.   This is one of the reasons

16   that we are reexamining our 50.59 guidance.

17   Current industry guidance for evaluating Digital I&C

18   modifications against 50.59 is included in NEI Guidance NEI 01-01.

19   This guidance was originally endorsed by the NRC through a regulatory

20   issue summary.

21   However, over time, the NRC and industry have found

22   that additional clarity and specificity is needed for this guidance.

23   We understand that NEI has a working group

24   dedicated to enhancing this guidance.   We understand our current

25   plans are to propose its revised guidances and new Appendix D to the

26   implementing guidance which is NEI 96-07.

1   We plan to meet with NEI on January 13th to discuss

2   the revised guidance. We plan to evaluate the new appendix and, if

3   appropriate, we would rescind our current endorsement of NEI 01-01

4   and, instead, endorse the new guidance in Appendix D of NEI 96-07.

5   Any new NRC guidance which endorses guidance

6   development by the industry would become available in the first quarter

7   of 2017.

8   Additionally, two weeks ago on December 2nd, we met

9   with NEI and EPRI to learn about EPRI's new good practices design

10   document which is being developed in parallel to the new NEI

11   guidance.

12   The EPRI guidance will not be submitted for NRC

13   endorsement. However, EPRI has solicited our technical comments

14   on the document and we will work with them to provide those

15   comments.

16   I would now like to turn to Deanna Zhang to discuss the

17   remaining items in the Digital I&C action plan.

18   MS. ZHANG: Thank you, John.

19   Digital technology has the potential to introduce

20   software common cause failures and unwanted system interactions

21   due to undetected systematic faults.

22   The Commission's SRM to SECY-93-087 defines

23   specific criteria for addressing software common cause failures.

24   These criteria are specified the performance of a diverse and

25   defense-in-depth analysis and provisions of a diverse means of

26   accomplishing the safety function.

1   We implemented this direction in Branch Technical

2   Position 7-19 titled, Guidance on Evaluation of Defense-in-Depth and

3   Diversity in Digital Computer-Based Instrumentation Control Systems

4   in Chapter 7 of the Standard Review Plan.

5   This Branch Technical Position provides guidance on

6   diverse means that could be used to mitigate software common cause

7   failures including adoption of internal diversity with the safety system or

8   use of manual operator actions.

9   In addition, this Branch Technical Position allows a 100

10   percent testing of simple systems to address the potential for software

11   common cause failure.

12   This guidance was based on Interim Staff Guidance

13   developed at the request of industry to consider testing as means to

14   address software common cause failures.   Also, guidance for

15   performing the diversity and defense-in-depth analysis of reactor

16   protection systems is provided in NUREG/CR-6303 as endorsed by the

17   Standard Review Plan.

18   This guidance constitutes the implementation of the

19   current NRC policy on software common cause failure.

20   Next slide?

21   The current policy and guidance for addressing the

22   potential for software common cause failures have been challenging for

23   some licensees.

24   For   example,   the   current   guidance   is   a

25   consequence-based approach for addressing software common cause

26   failures and does not directly relate to safety significance.   Thus, the

1   same rigor for treatment of software common cause failures applied to

2   all safety systems without consideration to the significance of the safety

3   function performed by each particular system of the overall plant safety.

4   In addition, even though we have effectively licensed

5   digital systems using this process we believe the assumptions in

6   SECY-93-087 should be reevaluated in light of significant technological

7   advancements.

8   Specifically, over the past 20 years, digital technology

9   and the tools for designing it have changed significantly including

10   advancements in both the use of digital use of field programmable data

11   rates and complex programmable logic devices.

12   The time that the 1993 SRM was issued, few standards

13   and no regulatory guidance documents existed for implementing digital

14   technology in nuclear power plants.

15   Since 1993, there have been significant improvements

16   in the methods used to design and implement digital systems.   There

17   have also been advances in the tools needed to analyze and test these

18   digital systems.

19   This has led to improved quality and reliability of these

20   systems and improved industry standards as well.

21   Some of these changes have also been reflecting our

22   updates to Branch Technical Position 7-19.   But, the basic NRC policy

23   has not been updated.

24   Based on evolution and technology and our lessons

25   learned from digital upgrades, we are evaluating the existing policy on

26   software common cause failure and looking at options to update it.

1   This evaluation will also assess potential ways to

2   achieve a graded approach based on safety significance.

3   We intend to prepare a report and a SECY paper

4   outlining the technical basis for either modifying the existing software

5   common cause failure policy or for establishing a new rule to

6   appropriately apply diversity and defense-in-depth for Digital I&C safety

7   systems.   Our goal is to have a draft SECY paper by the third quarter

8   of 2016.

9   In parallel with this effort, we will maintain appropriate

10   interfaces with industry stakeholders to identify what activities, if any,

11   can be performed to facilitate addressing this particular issue.

12   Next slide, please?

13   As previously highlighted, ISG-06 introduced new

14   concepts to the licensing process.   After the pilot program with Diablo

15   Canyon to upgrade the plant protection system, where plant has the

16   processes described in ISG-06.

17   For example, the level of technical detail and the need

18   for acceptance test reports in the license applications for digital

19   upgrades will be reviewed.

20   In addition, we are considering options to support

21   industry's request to reduce early regulatory uncertainty prior to

22   submittal of the factory acceptance test results.

23   We continue to enhance the guidance for licensing

24   processes for new and operating reactors including improvements to

25   ISG-06 and the issuance of design specific review standards.

26   In particular, to provide additional guidance on

1   addressing safety hazards associated with highly integrated I&C

2   systems.

3   We intend to pilot the use of the design review -- design

4   specific review standard for the NuScale Small Modular Reactor which

5   is anticipated to be submitted in the last quarter of 2016.

6   We also plan to incorporate our lessons learned from

7   ISG-06 into a Branch Technical Position. A draft of this Branch

8   Technical Position is projected to be ready in the third quarter of 2016.

9   We're considering the lessons learned, industry

10   feedback, new concepts for licensing processes along with research

11   activities to support licensing, to develop stable, consistent and

12   predictable licensing guidance.

13   Next slide, please?

14   Finally, we are evaluating the possibility of enhancing

15   the regulatory framework to consider cybersecurity at the design phase.

16   The current cybersecurity regulatory framework is programmatic in

17   nature.

18   As such, we currently do not perform cybersecurity

19   design reviews during licensing. We believe that considering

20   cybersecurity early in the system design process will help avoid designs

21   that may be difficult or impossible to adequately protect after

22   implementation. The ACRS has made similar recommendations.

23   As such, we are developing a SECY paper that

24   considers options for performing licensing reviews of cybersecurity

25   design information and plan to provide that SECY paper for

26   Commission consideration by the second quarter of 2016.

1   Next slide, please?

2   Besides the IEEE 603 proposed rule and the four

3   issues that were discussed in the previous slides, there are five

4   additional topics that the Digital I&C action plan addresses.

5   This includes evaluating new methods for assessing

6   highly integrated systems that focuses on hazards and safety design

7   principles.

8   Improving the regulatory infrastructure to achieve more

9   efficient and effective licensing reviews, developing guidance for

10   evaluating proposed alternatives to NRC requirements and guidance,

11   improving regulatory consistency between licensing and inspection

12   activities and enhancing Digital I&C topical report evaluation and

13   update process.

14   In support of developing new methods for assessing

15   highly integrated systems, we're engaged in research activities that, in

16   the intermediate term, we hope will yield efficiencies and effectiveness

17   improvements to Digital I&C licensing reviews.

18   This includes evaluating techniques for hazard

19   analysis and structure safety arguments, many of which of these

20   techniques you've heard from the other panelists that are being used for

21   other industries.

22   This concludes our discussion of our near term Digital

23   I&C initiatives.   I will now turn it back to Vic for closing remarks.

24   MR. MCCREE: Thank you, Deanna.

25   In summary, we recommend a Commission approval

26   to publish the proposed rule.   And doing so will enable us to obtain

1   formal external stakeholder feedback on the potential use and

2   incorporation of IEEE 603-2009.

3   If approved by the Commission, we will also hold a

4   public workshop during the comment period to seek and understand

5   stakeholder input.

6   As John noted, we will continue to identify and address

7   the other key regulatory initiatives through the development and

8   implementation of the Digital Instrumentation and Control action plan.

9   The actions over the next several months include work

10   on the 10 CFR 50.59 guidance and evaluating the NRC's processes for

11   evaluating software common cause failure.

12   We believe it's important to coordinate with external

13   stakeholders and we will continue to coordinate with the industry's

14   Digital Instrumentation and Control Working Group as well.

15   This concludes our presentation and we'd be happy to

16   address your questions.

17   Thank you.

18   CHAIRMAN BURNS: Thank you all for your

19   presentations.

20   As we hear the discussion, you know, it's a rich field of

21   issues and, you know, actions, potential actions because we're talking

22   not only about a proposed rule on IEEE standards but we're also,

23   particularly, I think Deanna's presentation focused on and some of the

24   others, there is a lot of other stuff going on here.

25   So, I'm going to try to touch a few of these things. I

26   mean, I think the simple, you know, the question that's sort of posed by

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

2   Let's assume there was a consensus just decided to go

3   ahead with approval as we often do with industry standards under

4   50.55(a) and approve IEEE 603-2009 and that's it.   What are we

5   missing doing that?   What is the critical -- convince me what the critical

6   additions in this rulemaking which are different than a lot of, you know,

7   industry standards incorporation by reference I've seen before, what's

8   the critical?

9   MR. LUBINSKI: I think if we were to look at that,

10   there's many options on how you would address the issue.   We chose

11   one option which we thought was the best of incorporating these

12   requirements as conditions in the rule.

13   We could continue to keep them in a guidance and

14   work with the industry as this being companion guidance to the rule if

15   we were to go forward with just an incorporation of the standard with no

16   conditions and address any concerns that the industry has with those

17   conditions through the development of the guidance.

18   We have been effective at using that.   We have

19   performed reviews already using the alternative clause under 50.55(a)

20   to approve applications that have met the 2009 standards and many of

21   those have met the conditions, the additional conditions already.   So

22   we can continue to do that.

23   What do you lose?   I think you lose a little bit of the

24   transparency and clarity of what the requirements are.   And, if there's a

25   concern or a difference among us and the licensee on where we're

26   going, then you may get into a little bit of a debate about whether or not

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

2   And then, finally, in the past, sometimes we've been

3   criticized for including information which we treat as a regulation, if you

4   will, and put it in guidance and, therefore, regulate through guidance.

5   So, that would be the other criticism we may be open to

6   if we do that.

7   CHAIRMAN BURNS: Okay. One of the things, and

8   again, and focusing on the last presentation, you talked about the

9   potential for new licensing processes, new -- other new things is my one

10   concern I would have.   What would be the impact of some of those on

11   the adoption of a rule with these added conditions, if any?

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

13   licensing first.

14   MR. TAPPERT: Okay. So, Deanna was talking

15   about our design specific review standard which is probably our biggest

16   initiative right now to try to streamline and focus the I&C reviews.

17   That's in place for the NuScale application which we're

18   expecting to receive the end of the next calendar year.

19   So, that's baked in so that's almost irrespective of what

20   the 603 rulemaking does.

21   CHAIRMAN BURNS: Okay. One of the other

22   questions, I'm going to turn away from IEEE 603, I think.

23   But, go to the issue that both panels discussed with

24   respect to 50.59 and that over some period here, sort of understandings

25   have diverged with respect to the requirement in 50.59 because is an

26   important control point from the standpoint it allows what we think are

1   safety acceptable changes in operation and in our license so we don't

2   have to review everything.

3   Where would you say, in terms of coming to a greater

4   consensus about where that guidance should be, what are the primary

5   gaps or primary push points?

6   MR. LUBINSKI: In answering that question, let me

7   say I think there's two aspects with the 50.59 guidance.

8   One is the clarity of the application of that guidance.

9   So, we may be aligned with the industry that there were certain 50.59

10   reviews that were performed inadequately and the industry may agree

11   with that in hindsight.

12   There may be other areas where the industry would

13   disagree with our interpretation of 50.59 and its application with respect

14   to whether it is coming up with a, you know, a new scenario that was not

15   previously analyzed by the licensee or come up with a different

16   outcome.   So, there may be differences.

17   We have yet to see the guidance that NEI has

18   developed, so it's too soon to answer what that question would be.

19   And, that's the importance to our January meeting with NEI on that new

20   guidance to see how much of this is clarity and specificity of the

21   guidance and understanding current 50.59 and where are there

22   differences between our interpretation.

23   I will say one of the big -- because it is a link to common

24   cause failure because that's another aspect that feeds into 50.59 which

25   is why I believe both us and the industry have put both of those items as

26   our high priority items to look at.

1   CHAIRMAN BURNS: Okay.   One of the -- you know,

2   we obviously in the first panel we had a couple additional experts

3   outside of our industry.   And, I know during the discussion maybe one

4   of the Johns, I think you mentioned, in terms of our, you know,

5   participation in multinational design evaluation program and I know

6   from, you know, past experience, Digital I&C has been an issue, you

7   know, one of the subcommittee type issues on MDEP for a long time.

8   What do we -- any comments you want to make from

9   what you heard on the first panel about the -- what we might learn from

10   aviation?   And, is that, in terms of approaches that we've seen through

11   MDEP, you know, that the French have done or others, and I know, you

12   know, again, this is from sort of being, you know, the amateur reader, if

13   you will, on some of this that there are some differences.

14   But, any insights we have from MDEP or our

15   interaction on aviation industries or others?

16   MR. STATTEL: I'd like to make an observation with

17   regard to that because I think a lot of the misunderstandings we've had

18   in 50.59 have actually resulted from some of the things that we're

19   hearing from the other industries.

20   So, for example, the challenges that we've all faced

21   involve and the way we respond to those involve not just looking at the

22   end result or the testing but also focusing on processes, the

23   development processes and different aspects of these systems.

24   And, that's why you see these big maps and these

25   complex maps of the different facets of I&C that we all look at.   And, I

26   think that tends to create some misperception so, like one of the

1   statements I've seen in some of these 50.59s that were deemed

2   unacceptable was that, well, we used a really good development

3   process so, therefore, we didn't have to do complete testing.   Right?

4   So, in our interpretation, we wanted basically to

5   address multiple facets of the design and their interpretation was more,

6   well, since I have a good process, then I can basically de-emphasize

7   the end testing results or I don't have to concern myself with the

8   common cause failure aspects because it's -- I've reduced the

9   likelihood of that.

10   CHAIRMAN BURNS: Okay.

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

12   perspective.

13   So, I chaired the Digital I&C Working Group and it's a

14   number of regulators we have and we all have a number of concerns

15   with respect to software common cause failure.

16   We developed a common position for this.   And, what

17   we have come to alignment is that, yes, it is a multifaceted issue.

18   There are many ways to address it, but we definitely have to address it.

19   It's not something we can ignore.

20   And, what we have to come to agreement on is that

21   there are -- you should do analysis.   You should consider different

22   coping measures.   But, the acceptance may be different, the

23   acceptance criteria for applying it may be different.

24   CHAIRMAN BURNS: And, how so?   How are the

25   acceptance criteria different?   What drives that?

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

1   regulators, they look at a lot more in terms of the software. So, they

2   get the actual software code. They evaluate it, they analyze it for the

3   potential software defects that may be in there.

4   So, there's a lot more emphasis on testing, analysis

5   and development than what we would typically look at in our licensing

6   reviews.

7   CHAIRMAN BURNS: Okay, all right.

8   MR. TAPPERT: And, I'd just like to add, you talked

9   about other industries, one of the items in the action plan is dealing with

10   highly integrated systems. And, that's more of an intermediate term

11   thing where we're going to be looking at different opportunities and

12   different paradigms to look at greater reliance of hazard analysis and

13   structured safety arguments to kind of think about different ways of

14   evaluating these systems.

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

16   knowledge.

17   CHAIRMAN BURNS: Okay, thanks.

18   All right, thanks very much.

19   Commissioner Svinicki?

20   COMMISSIONER SVINICKI: Well, I want to thank the

21   staff for the presentations today. But, beyond that, I'd like to thank

22   Richard, John Lubinski and Deanna for, I think at this point, we may be

23   up to close to four hours worth of separate briefing time that I've had an

24   opportunity to talk about the specific IEEE 603-2009, that SECY paper.

25   That's been very helpful in terms of building a

26   foundation to consider the staff's recommendation that's in front of me.

1   Something that's not been mentioned because today's

2 meeting, the topic, when the topic of that paper comes up, the staff has

3 presented on, appropriately so, the staff's recommended position.

4   There are multiple nonconcurrences to that staff

5 recommendation, however, all of which I've reviewed, all of which I

6 found very thoughtful and I do thank the nonconcurring individuals. I

7 don't know if any of them are attending here today.

8   In all cases, those were very thoughtful

9 nonconcurrences and, for me, in terms of my review of the matter,

10 many of them were quite compelling.

11   A number of them originate with NRC reviewers who

12 have, frankly, decades worth of experience on this topic as safety

13 reviewers here at the Nuclear Regulatory Commission. So, the level

14 of experience they have in the operating reactor field carries a lot of

15 weight with me.

16   So, again, I think as we discuss this today, we have

17 discussed the staff's recommendation which was the ultimate decision

18 adjudicated by the staff as they reviewed the nonconcurrences.

19   However, there is other body in the decision record for

20 the Commission's consideration which I think is important.   And, but for

21 its existence, it might be a little more straightforward.   But, you know,

22 candidly put, our experts are not of one mind on the additional

23 conditions, principally, a lot of the nonconcurrence has to do with the

24 addition conditions beyond incorporation by reference, there's not

25 unanimous support for those.

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

1   underlying matter.

2   I think that, at some point, it is difficult as an

3   organization, we do need to find, maybe it will be through the additional

4   work that we continue to engage with external stakeholders.

5   At some point, if we could bring this diversity of position

6   into greater alignment, I think it would strengthen us as a professional

7   organization and the experts for the nation on this topic that we have to

8   be able to auger some competence in our decision making.

9   So, again, I'm fully supportive of the nonconcurrence

10   and differing views process.   I just think that we've got a lot of moving

11   parts here and if there's a fundamental philosophical divide or

12   divergence that's occurring, my general instinct maybe just even as a

13   human being, is that sometimes you want to mend that first and then

14   you want to continue to the detailed technical work.

15   So, I think if you can't get the ideology in alignment, I

16   think we might then -- I might -- my successor in, you know, 2027 won't

17   read an SRM from 2017 and say, gosh, ten years ago it was so quaint

18   that Commission thought that these things were near resolution.

19   But, I think it is something for the senior leadership

20   team here.   I know alignment is tough.   I know the EDO and his direct

21   reports do a lot of alignment meetings.   That's part of being a technical

22   community, a community of professionals and experts is that we need

23   to go through that process.

24   And so, I think it's healthy.   I'm not in any way

25   suggesting that this is deeply irregular, but I do think, you know, before

26   we dot every I and cross ever T, we may want to get to the root cause.

1   That's kind of popular in this business. We might want to get to the

2   root causes of some of that divergence.

3   So, I only had one specific question and it had to do, as

4   the Chairman mentioned, there's other things beyond that SECY paper

5   which Deanna covered.

6   Deanna, you talked about work on highly integrated

7   systems. Do we have a good definition for a nonpractitioner in this

8   field of what differentiates an integrated system from a highly integrated

9   system?

10   MS. ZHANG: I think it's just an upper, but if we look at

11 a lot of the shared resources that are going between the different

12 systems between levels of independent systems.

13   Prior to, you know, use of digital systems and even

14 throughout the upgrades, it's always been a little bit more piecemeal.

15 You get one system that performs one function. Now you have a

16 system that could perform multiple functions.

17   And, that's where the integration comes from is how

18 much functionality are you putting into one resource or how many

19 different systems share the same resource in performing different

20 functions?

21   COMMISSIONER SVINICKI: Okay, thank you.

22 That's helpful and I look forward to learning more about work as the

23 staff moves forward on advancing its work products in that area.

24   I guess I'll just close maybe with a little bit of a pep talk

25 to say that the first panel talked about other industries. I made a

26 comment there that other sectors may be some how overtook us and

1   surpassed us on conquering this issue.

2   You know, I want to say that I come at this sincerely

3   with just so much respect for all the differing views that exist on this, the

4   recommendation and the other views.

5   People have -- our experts have come at this with a lot

6   of conviction.   But, at my level, you know, some of this bubbles up to

7   fundamental determinations of how safe is safe enough?   What is risk

8   tolerance?   What risks can be tolerated?   What level of risk can be

9   tolerated or levels of uncertainty?

10   And, that is a threshold judgment at every level of

11   senior leadership.   We've got to make tougher and tougher decisions

12   about that.   The Commission being the ultimate expression, we often

13   have to make the ultimate judgment call on how safe is safe enough.

14   But, I will say this to you, none of your peers over at

15   FAA or anywhere else are better at this than us, so we absolutely will

16   resolve this.   I know we will conquer it.   It is not, as the first panel said,

17   a question if we can resolve these issues, we will because there is no

18   future for nuclear technology, either for the stuff that's operating now or

19   future stuff if as the nuclear safety regulator for the American public, if

20   we can't solve this, there's no future.   I know we can solve it.   I know

21   we're going to.

22   So, you know, continue, please, no matter the outcome

23   of the Commission's decision on the 603 paper, please continue to work

24   on this with the kind of commitment that you have.

25   Thank you, Mr. Chairman.

26   CHAIRMAN BURNS: Thank you.

1   Commissioner Ostendorff?

2   COMMISSIONER OSTENDORFF: Thank you all for

3   your presentations.

4   I want to start out, and I'll let anybody answer this who

5   wants to.   With the first panel, we clearly heard from industry that, with

6   respect to this piece that deals with IEEE 603-2009 that there is not

7   agreement that we should add these additional requirements above

8   and beyond the industry standards.

9   I just want to provide an opportunity to anybody that

10   wants to speak to address that issue.

11   MR. LUBINSKI: I'll start at a high level and maybe ask

12   others to talk detail.

13   I think what I also heard from the industry this morning

14   as well as hearing in other communications with the industry was, one

15   was a prioritization of resources when they were saying that the IEEE

16   603-2009, they were looking at what's the resources to continue

17   through the rulemaking, go through the comment period, what the

18   concern would be there and trying to address those additional

19   conditions through that process.

20   And, I hear that they're looking from a prioritization

21   standpoint and saying things like 50.59 and common cause failure are

22   more important and should be addressed first and then we can look at

23   the conditions.

24   I think from the standpoint of the additional conditions,

25   what I also heard this morning was a concern of making them

26   regulatory requirements versus the actual technical nature of those

1   requirements and Rich can maybe expand on some of the technical

2   nature of some of those aspects.

3   I think we have been effective across the board as a

4   regulator and an industry in addressing issues associated with those

5   additional conditions through current licensing reviews that have been

6   performed whether they're in the operating reactor or in the new reactor

7   area.

8   So, the conditions have been in guidance, not as

9   conditions, of course, but have been in guidance to address things like

10 the hazard analysis, the independence and the communications. So,

11 we have been able to address those on a case by case basis.

12   But, I think from the standpoint of understanding more

13 of the specific concerns from the industry on those specific items, no,

14 we don't have a clear handle on that.

15   Rich, did you want add?

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

17   The working group did spend a lot of time discussing

18 this. And, virtually every one of the conditions that you see in the

19 proposed rule was originally proposed as guidance, that inclusion into

20 the reg guide that accompanies this rule.

21   There wasn't unanimous agreement, there still isn't

22 among the working group members.

23   The real thing is, at a glance, you might think that

24 taking exactly the same verbiage out of a consensus guide that

25 everyone agrees to and moving that language into a rule, well, why

26 would that be a problem?

1   But it's really a context issue and by putting it in the rule

2   and changing the context of that language, you really make that the

3   only acceptable way, you know, by definition, by putting it in the

4   regulation and it makes it a whole lot more difficult for designers to

5   innovate and to realize some of the safety benefits that could otherwise

6   be realized.

7   So, it really does change the context.   In some cases,

8   like the hazard analysis requirements, I like to call it a strong guidance

9   because, you know, every safety evaluation I've ever done on a digital

10   system, we require them to identify hazards and we require the

11   applicant to address all of the hazards they identify.

12   So, making that a regulation, it's, you know, it kind of

13   emphasizes the importance of it, but I really can't see applicants

14   proposing alternatives to that, like I'm not going to address the hazard

15   that I identified.

16   So, those are not so much controversial.   But other

17   ones, the independence requirements in particular are viewed as being

18   a lot more difficult and problematic.

19   Those requirements in particular, those are where we

20   basically divided the rule into new and operating reactor criteria and,

21   what really drove that was the processes.   We really have -- we really

22   face very different problems when we're reviewing a design certification

23   versus an amendment, a license amendment.

24   So, one of the big differences I'll point out, there's a lot

25   of subtleties to this, but one of the big differences is, with an operating

26   plant, it's operating.   It has a licensing basis.   We have something to

1   compare the new system to. And it's therefore, there is a basis for

2   putting forth your safety conclusions. Right? You're at least as safe

3   or you're improving safety on that system.

4   With the new reactors, you don't have that baseline, so

5   that makes it a lot more difficult for them. And, honestly, you know,

6   we're all engineers here and we do kind of think a lot alike.

7   However, you know, we're really faced with very

8   different problems and I think, you know, if we reverse positions and,

9   you know, I was working on the new reactor side, I would have a lot of

10   the same concerns they have.

11   So, it's really the process that drove those differences

12   in the proposed criteria.

13   COMMISSIONER OSTENDORFF: Okay. John?

14   Or Deanna, yes?

15   MR. TAPPERT: I just wanted to chime in.

16   So, the way I think about it, and I think John talked

17   about this earlier, is there's a lot ways to skin a regulatory cat. And, I

18   think what the proposal before the Commission is really the staff's best

19   proposal to go forward.

20   But, we recognize that there are, you know, good

21   arguments on different approaches as well. And, that's why in addition

22   to the proposed rule before you, we've also proposed an approach

23   where we wanted to have an extended public comment period. We

24   wanted to have public workshops in order to get more stakeholder

25   input.

26   We've   actually   put   a   number   of   --   or

1   suggested -- recommended putting a number of questions in the

2   proposed Federal Register Notice to kind of elicit some of this feedback

3   on, you know, are these too prescriptive? Are there better ways of

4   doing this?   Are there unintended consequences?

5   So, I think what we have is our best thinking, but we

6   recognize that we need other input as well.

7   COMMISSIONER   OSTENDORFF: Thanks.

8   Deanna?

9   MS. ZHANG: Yes, and I would like to just add on a

10   little bit to what Rich was saying which is, you know, we heard from the

11   previous panelists, you know, evidence.   And that's something that we

12   definitely had an issue with with a lot of the new reactor applicants is

13   that they did not provide evidence that the design was safe in terms of

14   communications independence.

15   And with that, you know, are there other means to

16   achieve the same result as limiting the architecture? Yes, there are

17   other means.   And, that's why we do have an alternative process which

18   we have successfully used before.

19   But, when we looked at our previous lessons learned

20   from the recent design certification applications, because of the lack of

21   evidence and because not all the hazards were correctly identified, we

22   had a lot of issues approving and reviewing those designs.

23   COMMISSIONER OSTENDORFF: I'll just make a

24   comment, I'm not going to ask a question of this, but in my vote on the

25   Commission involvement or decisions rulemaking, I did use cite -- a

26   paragraph using this SECY paper as an example.   And, it's quite

1   frankly, not a positive example.

2   Where it took 18 months in concurrence to come to the

3   Commission and there is different -- I respect the fact everybody's

4   engineers and always trying to do things the right thing, but both Rich

5   and Deanna have hit upon there's different ways of looking at this in the

6   organization.

7   So, I just would ask you to look at my vote on that

8   because I think it's highlighting the lack of agility in decision making

9   here which I'm going to make a comment on as I close.

10   I start out by saying I'm struggling with this one. At the

11   conclusion of today's meeting, I'm still struggling.

12   I've heard Deanna talk about well, we need to go back

13   maybe and look at SECY-93-087. We've had -- the SECY paper talks

14   about these other future rulemakings. They are not well defined.

15   John, I appreciate the comment on public, you know,

16   comment and so forth. My personal view as a Commissioner, I don't

17   vote on something that I'm not comfortable putting out there that I would

18   say this proposed rule can be a final.

19   So, I'm very leery to vote on something to say throw it

20   over the transom let public comment on. Is it premature? You know,

21   with all these other moving parts, I can't, you know, we spend a lot of

22   time, as Commissioner Svinicki noted, we've had a lot of different

23   briefings before today from the staff on this exact topic.

24   How should I look at our ability as a Commission to

25   make a decision on this given all these other moving parts?

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

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

2   In addressing the issue with respect to the IEEE 603

3   Standard, there are many options and the way to handling it is was

4   stated, as Commissioner Svinicki said, there were diverse opinions

5   from staff.   And, you could probably go about three or four different

6   options on how to move forward with respect to the standard.

7   We chose what we believed was the best option in

8   moving forward and provided that to the Commission.

9   COMMISSIONER OSTENDORFF: I just want to

10   make sure I'm clear on the record.

11   I do not fault the recommendation that came to the

12   Commission.   My real concern is these other ancillary efforts that are

13   not real clear what they might mean going forward.

14   MR. LUBINSKI: Understood, I appreciate that.

15   And, the reason I brought that up too, my comment is

16   that we think that the public comment period that we would have if this

17   proposed rule is approved is important.

18   We also believe that in going forward, if we had no

19   comments on the proposed rule and it went final, we believe it would be

20   an effective way to regulate.

21   With respect to the other issues, we did take those into

22   consideration and looking at continuing with this rulemaking.

23   In fact, common cause failure was one of the issues

24   that we considered putting into this rulemaking and making part of this

25   rulemaking at that time.

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

1   looking at it as potentially, and that's what's referenced in the rule is the

2   diversity and defense-in-depth rulemaking that's being handled under

3   separate, is we did believe that more work was needed on that.   We

4   believed better regulatory basis was needed.

5   We also believed in going forward that more

6   stakeholder interaction was needed, external stakeholder interaction.

7   We do plan to do that in the coming year to work with the industry to get

8   their issues.

9   We're currently calling it a rulemaking process.

10   Whether it turns into a rule or not is going to be a question.   It could be

11   that we believe that the current policy or say policy position, if you will,

12   on the SRM from 1993 is adequate and we continue to stick to it.   It

13   could be a modification and guidance but we won't know until we do

14   more evaluation.   But, we felt that was necessary.

15   In answering your question why are we comfortable

16   going forward with 603 with these other issues there?   We're not

17   seeing that we need to change 50.59 and we don't see a big connection

18   to 603 with that.

19   For common cause failure, that is one piece of what's

20   being evaluated and if it turns into guidance, why should we hold up this

21   rulemaking When it could just be a change in guidance and moving

22   forward?

23   We would have certainty in the industry from the

24   standpoint as a question you asked the industry earlier about additional

25   applications coming in.   We know that's the goal with the industry.   In

26   their roadmap, we understand that they've put target dates for the next,

1   I'll say, major application to come in and feel that if they can't get to the

2   point of doing that, then that's not success on the roadmap.

3   We believe having some certainty with respect to how

4   you handle 603 will help with the certainty in that application coming in.

5   We believe handling these other issues in parallel, we have looked at

6   the what can be done in parallel and what can be done in series and

7   that's the reason the action plan was put together and we do believe

8   that 603 can and should move forward while we're handling those

9   issues in parallel.

10   COMMISSIONER OSTENDORFF: Okay, thank you.

11   CHAIRMAN BURNS: Thank you, Commissioner.

12   Commissioner Baran?

13   COMMISSIONER BARAN: Thanks.

14   John, let me just pick up right where Commissioner

15   Ostendorff left off on this question of diversity and defense-in-depth and

16   how to approach this.

17   And so, the ultimate recommendation from the staff

18   was don't address that in this IEEE 603 rulemaking. Let's do what's

19   likely going to be a separate rulemaking to address diversity and

20   defense-in-depth.

21   And, I guess my first question on this is, what happens,

22   you know, what happens if we don't include -- we don't address

23   diversity and defense-in-depth in this rulemaking but then we end up

24   not proceeding with a separate rulemaking on those topics?   Where

25   are we going to be at that point if we don't do it here and then, for

26   whatever reason, ultimately, we don't do it separately?

1   MR. LUBINSKI: Okay, I will say from the first point is

2   the IEEE 603 rulemaking is an incorporation by reference rulemaking

3   into 50.55(a).

4   There is a link with common cause failure, diversity and

5   defense-in-depth but it's not an industry standard, if you will, that's been

6   put together that would be incorporated into 50.55(a).   And, there have

7   been questions whether that is the appropriate place for it or does it go

8   in another section of the regulation if it becomes a rule.

9   From the standpoint of not addressing it, I would say

10   that I believe the issue will be addressed.   Whether it's addressed as a

11   rulemaking or not is a separate question and I think that's where you're

12   coming from.

13   If we were to move forward and look, there are a

14   number of outcomes and I don't know what they're going to be.   The

15   outcome could be that our addressing of common cause failure is

16   adequate the way it is, that the SRM that was issued in '93 is adequate

17   and maybe there's only tweaking of the current guidance which

18   incorporates that.

19   All the way to the other end, it says we believe the only

20   way to have certainty is to put it into the rule.

21   We've discussed today some of the conditions that we

22   would include and how important are they to be conditions in the rule for

23   603 versus being handled through a guidance.

24   So, I think if I were to listen to your question of the

25   worst case scenario if rulemaking was turned off in that area, what

26   would happen?   I believe there would be some type of enhancement

1   and guidance that would address this issue and we would go through

2   the process of interacting with external stakeholders on that guidance

3   to assure that it addresses the issues in an adequate manner.

4   COMMISSIONER BARAN: In that eventuality, we

5   would continue to regulate based on this 1993 SRM.   We wouldn't

6   have anything in regulations, we'd have regulatory requirements based

7   on an SRM.

8   MR. LUBINSKI: I would say that if we were doing

9   something different in a guidance that contradicted the SRM in any

10   way, we would not necessarily have to go through a rulemaking, but we

11   would come back to the Commission with a statement of direction from

12   the Commission in 1993 was this in an SRM and get Commission

13   approval to change what was in that SRM.   We would reference that

14   SRM, talk about the merits of why we would change that and, if we were

15   not doing rulemaking, we would say we plan to address this through

16   staff guidance but request Commission endorsement of that new, if you

17   will, standard or policy.

18   COMMISSIONER BARAN: I guess it just strikes me

19   that there's some awkwardness in proceeding that way, right?   I mean

20   normally we have regulatory requirements that are actually enshrined in

21   regulation versus in just a Staff Requirements Memorandum.

22   And so, if it's a very significant issue from the staff point

23   of view, the idea that we'd address it but we'd never address it in actual

24   regulation strikes me as problematic.

25   MR. LUBINSKI: Right, it's not addressed in a

26   regulation at this point, but what we did is put it into durable guidance, if

1   you will, from the standpoint of our standard review plans, our ISGs as

2   well as Branch Technical Position.

3   Branch Technical Position 719, thank you, I'm getting

4   help from the back, thanks.   It is listed in that Branch Technical

5   Position which we use.

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

7   guidance.

8   COMMISSIONER BARAN: Jennifer, did you want

9   to --

10   MS. UHLE: Yes, this is Jennifer Uhle, I'm the Director

11   of the Office of New Reactors.

12   And, I think in part, the Commissioner's question is

13   also asking what are -- where are the regulatory requirements for

14   anything associated with Digital I&C?

15   And so, I&C has been certainly a requirement since the

16   inception of nuclear power.   And it specified in the general design

17   criteria 21, 22, 23.   There's elements in Appendix B, so that's Appendix

18   B to Part 50.

19   And then, of course, there's IEEE 603 which is

20   endorsed by reference under 50.55(a).

21   So, there is no one clear Digital I&C rule.   That's not

22   how it has been put together and it gets confusing because then it's a

23   patchwork and we can talk about this element of IEEE 603 here.   But

24   then there's other issues about common cause failure and the reliability

25   of the system that is discussed in the general design criteria and then

26   the supporting guidance.

1   So, I don't know if that helps at all. The SRM to

2   SECY-93-087 provides direction to the staff on how to implement those

3   regulatory requirements that are in the GDC and that was previously in

4   50.55(a).

5   COMMISSIONER BARAN: But, is there a downside,

6   and this is a question for everyone who wants to answer it. Is there a

7   downside to seeking stakeholder feedback on a potential, you know,

8   provision on diversity and defense-in-depth through this proposed rule,

9   getting that feedback?

10   Now, originally, once upon a time, in the staff process

11   developing this, there was a provision on this. It was taken out in

12   response to a nonconcurrence. Is there an advantage, given that we

13   don't know what the Commission may or may not approve in the future

14   on a separate rulemaking, we don't know even if there would be a

15   separate rulemaking, is there an advantage of to getting public

16   comment on that question now in this proposed rule? Is there any

17   downside to doing that?

18   MR. LUBINSKI: We've already in our current

19   package in response to many of the nonconcurrences and differences

20   of opinion we've had included additional questions in the current

21   rulemaking package of which this is one of those questions how we

22   should address diversity and defense-in-depth common cause failure.

23   It's a specific question, one of many that are listed in

24   the Statements of Consideration seeking feedback.

25   We have also, if we were to move forward, issue the

26   proposed rule and have the workshops John talked about, that would

1   be one of the main topics of discussion along with the other questions

2   that are listed in the rule today.

3   COMMISSIONER BARAN: Okay. Well, and then

4   taking a step back on the -- and obviously, I think it's fair to say there are

5   a wide range of views about how to proceed with this rulemaking, and

6   we've talked a lot about the question of what goes in a regulation and

7   what goes in guidance.

8   And, from your point of view, and this is a question

9   really for either John or the other John, you know, how much of the

10   disagreement about this just boils down to whether we're going to take

11   some of these requirements and put them into a regulation versus keep

12   them in guidance where they are now?

13   Is that really what the disagreement's about,

14   whether -- not what the requirement or expectation would be, but rather

15   does it reside in their regulation or does it reside in the guidance?

16   MR. LUBINSKI: I would say probably that's the

17   majority of it, but that's not all of it. There are some disagreements and

18   I think for the -- where there are technical disagreements even

19   internally, and I know there are externally as well, but even internally

20   where you may have disagreements on the technical requirements,

21   there's a concern that if you do put it into the rule that makes it that

22   much more difficult for the people with the diverse view to have their

23   concerns addressed.

24   When they're in guidance documents, they feel that

25   maybe there's a bit more leeway when they're going through a review

26   process that it's only guidance and, therefore, they don't have to treat it

1   as a regulation when they're implementing it through a licensing

2   process.

3   COMMISSIONER BARAN: Did you want to add

4   anything on that, John?

5   MR. TAPPERT: I would just step it back to your

6   previous question about the common cause failure and the desire to get

7   stakeholder feedback in the context of the rulemaking.

8   So, John referred to the Federal Register Notice,

9   proposed Federal Register Notice which had question in it.

10   We also have in the action plan a separate track to look

11   at that one issue.   And, as part of that, there will be public engagement

12   and feedback.   So, even absent the rule, there'll be activities to engage

13   on that topic.

14   COMMISSIONER BARAN: And one of the issues or

15   questions that came up on the first panel was, well, are these conditions

16   that   the   staff   has   added   to   the   core   standard,   are   they

17   performance-based technology neutral or are they technology specific?

18   Does someone want to respond on that?

19   Is this a situation where we're potentially being overly

20   prescriptive   in   the   regulation   and   allowing   only   one   way   to   do

21   something   or   are   these   performance-based   standards   that   are

22   technology neutral?

23   MR. STATTEL: I would just like to point out, I know

24   the perception might be that we're diametrically opposed on these

25   matters.   But, in actuality, we're a lot closer than you might think.

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

1   requirements that are being proposed here, no one at this table would

2   disagree that that's a safe system, that that's an acceptable system.

3   Where the disagreement is, is that's the only way to

4   achieve a safe system.   So, in a lot of cases, you know, just the same

5   conditions under a regulatory guidance perspective, you know, that

6   would alleviate the difference of opinion.   Right?

7   But, you know, When you start putting those

8   prescriptive type requirements into the regulation, that's, you know,

9   you're really boxing the designs in and that's where it becomes

10   problematic.

11   COMMISSIONER BARAN: And, John and John, I

12   mean are you share that view?   Are these prescriptive requirements

13   that are represented by these conditions that allow for only one way to

14   do it?

15   MR. TAPPERT: And, I think at least some of that is

16   being directed at some of the communications requirements for the new

17   reactors communications provisions.

18   So, and I can't argue that those are anything but very

19   prescriptive.   I mean they are.   And, the reason they are that way in

20   the proposal is based on our experience in trying to review these design

21   certifications.

22   And, it's been a very problematic area and our view is

23   that to get better regulatory surety and have a better path to success on

24   these things, it's appropriate to be that prescriptive, understanding in

25   general that's not how we want to do business.   But, in this particular

26   instance, we think that the evidence supports that proposal.

1   MR. LUBINSKI: And, I would agree with John from

2   the standpoint of that being prescriptive and I would not argue at all.

3   There are others that may be technology neutral and

4   more performance-based such as the performance of a hazard

5   analysis. There's not -- it's not prescriptive in how it's done, what the

6   results need to be, but it's that the hazard analysis is performed.

7   And, I'd say that's more of a level of detail of

8   information that's provided to the NRC for review versus a prescriptive

9   design standard in this.

10   COMMISSIONER BARAN: Is   the   one   way

11   communication, is that the only example of a condition that's

12   prescriptive from your point of view?

13   MR. STATTEL: No, there are three criteria in the new

14   reactors clause.   One is that communications for a diverse control, so

15   basically a non-safety signal to actuate a safety injection pump, for

16   example.   That would have to be transmitted via a non-digital means.

17   So, basically, it would have to be a discrete analog signal essentially.

18   And, of course, the one way communications to

19   non-safety-related systems, that's the other example.

20   MS. ZHANG: So, specific to new reactors, that's the

21   answer   is   the   prescriptiveness   comes   for   the   new   reactor

22   independence clauses.   But, in terms of, you know, are there better

23   ways of doing it?   And this is where we are looking at the highly

24   integrated systems, new methodologies for assessing it as part of our

25   Digital I&C action plan.

26   And, we have active research in this area where we're

1   working with the Carnegie Mellon Institute to look at modeling

2   techniques to bottle some of the design certification applications to

3   have come in.

4   And, based on the results of those studies, we may find

5   that there are better ways to do it.

6   COMMISSIONER BARAN: Okay, thank you.

7   CHAIRMAN BURNS: Thank you.

8   Anything else from my colleagues?

9   Well, again, I appreciate the presentations from the

10   staff today as well as from our first panel.   It's been a good discussion

11   of the issues related to the use of digital technology in the nuclear

12   industry and our associated regulatory activities.

13   Obviously, an area of high interest and today's

14   discussion I think are important input to the Commission's consideration

15   of various matters including the particular paper in front of us.

16   Again, thank you.   And, with that, we'll adjourn.

17   (Whereupon, the above-entitled matter went off the

18   record at 4:23 p.m.)